

# A Gamified Experience: A CTF Approach to Understanding Insider Threats

Nick B. Blume & Nikolaj Jørgensen

June 3, 2025



**AALBORG UNIVERSITY**  
DENMARK



**AALBORG UNIVERSITY**  
STUDENT REPORT

Department of Electronic Systems

Aalborg University

<http://www.aau.dk>

**Title:**

A Gamified Experience:  
A CTF Approach to Understanding  
Insider Threats

**Theme:**

Thesis Project

**Project Period:**

4th Semester

**Project Group:**

1012

**Participant(s):**

Nick Blume  
Nikolaj Jørgensen

**Supervisor:**

Lene Tolstrup Sørensen

**Co-Supervisor:**

Jens Myrup Pedersen

**External Partner and Contact:**

Campfire Security - Kristian Larsen

**Copies:** 1

**Page Numbers:** 146

**Date of Completion:**

June 3, 2025

**Abstract:**

This Thesis Project explores the design and implementation of a Capture the Flag (CTF) module focused on insider threats. In collaboration with Campfire Security, the project creates an insider threat CTF module tailored specifically for cybersecurity novices with limited to no prior experience. Drawing on established cybersecurity frameworks, academic literature, and insights from an interview with a seasoned cybersecurity professional, the project delivers structured, grounded and interactive learning material to cybersecurity novices. The development process was further informed by an analysis of some of the existing educational CTF platforms, including Campfire Security's own platform, which was used to host the CTF module. The resulting module was tested on a small sample group to collect qualitative feedback on its usability and the user's experience and engagement. Findings suggest that participants preferred the interactive, gamified nature of the CTF format over traditional teaching methods. Furthermore, the results showed indications that the CTFs can serve as an effective tool for cybersecurity training and to introduce complex cybersecurity topics such as insider threats to novices.

# Contents

## Preface

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Insider Threats</b>	<b>3</b>
2.1	Defining Insider Threats . . . . .	3
2.2	Frameworks for Insider Threats . . . . .	6
2.2.1	CISA Insider Threat Mitigation Guide . . . . .	7
2.2.2	Critical Pathway to Insider Risk . . . . .	8
2.2.3	MITRE Insider Threat TTP Knowledge Base v2.0 . . . . .	9
2.3	Insider Threat Analysis as a Work Role . . . . .	10
<b>3</b>	<b>What is a CTF?</b>	<b>13</b>
3.1	Gamification . . . . .	14
3.2	Flow . . . . .	15
3.3	Design . . . . .	16
3.4	CTF in an Educational Context . . . . .	17
3.4.1	HTB Academy . . . . .	18
3.4.2	PortSwigger Academy . . . . .	22
3.4.3	Campfire Security's Platform . . . . .	25
<b>4</b>	<b>Method</b>	<b>34</b>
4.1	Semi-structured Interviews . . . . .	34
4.1.1	Analyzing the Interview . . . . .	35
4.2	Course Development . . . . .	36
4.2.1	Operationalizing Frameworks for Training . . . . .	36
4.2.2	The Modules . . . . .	37
4.2.3	The Campfire Platform . . . . .	38
4.3	Testing in a Workshop . . . . .	38
4.3.1	Data Collection Instruments . . . . .	39
4.4	Ethical Considerations . . . . .	40
<b>5</b>	<b>Results: Interview</b>	<b>41</b>
5.1	Interview . . . . .	41
5.1.1	Interview: Thomas Kristmar from Statens It . . . . .	41
5.1.2	The Findings from the Interview . . . . .	42
<b>6</b>	<b>Results: Course material</b>	<b>44</b>
6.1	Module 1: Insider Threat Awareness Quiz . . . . .	46
6.2	Module 2: Insider Threat Types Quiz . . . . .	50

6.3	Module 3: Is This a Phishing Email... ? . . . . .	54
6.4	Module 4: I Didn't Mean to Let Them In . . . . .	60
6.5	Module 5: An Everyday Help Desk, or ? . . . . .	64
6.6	Module 6: MailMole . . . . .	69
<b>7</b>	<b>Results: Testing the Material in a Workshop</b>	<b>74</b>
<b>8</b>	<b>Discussion</b>	<b>81</b>
8.1	Our Contribution . . . . .	81
8.2	Methodological Reflections & Limitations . . . . .	82
8.3	Usability and User Experience . . . . .	84
<b>9</b>	<b>Conclusion</b>	<b>86</b>
<b>A</b>	<b>Appendix</b>	<b>92</b>
A.1	Framework Sections that were Removed . . . . .	92
A.1.1	NIST Cybersecurity Framework v2.0 . . . . .	92
A.1.2	CERT Common Sense Guide 7th Ed. . . . .	93
A.1.3	G-Research Insider Attack Matrix . . . . .	96
A.2	The Green-"seen" Chart . . . . .	100
A.3	Work Role - Insider Threat Analysis . . . . .	101
A.4	Workshop and Debrief Notes . . . . .	107
A.5	Interview transcription with Kristian Larsen (not analyzed or utilized further) . . . . .	108
A.6	Observation Notes from Interview . . . . .	114
A.7	Transcript with Codes . . . . .	114
A.8	Interview Guide . . . . .	134
A.9	Coding Process . . . . .	136
A.10	HTML Emails . . . . .	138
A.11	Other Pages. . . . .	138
A.12	Challenge 6 Emails . . . . .	140
A.13	Questionnaire data . . . . .	143
A.14	Questionnaire graphs . . . . .	145



# Preface

## Use of Generative AI

Generative AI seems to have taken hold of a wide range of industries, including academic pursuits. Debates regarding *how* and to some extent *if* generative AI is to be used in academic work is pertinent to this project. With the goal of following good academic practice and being open and transparent, this section will present how generative AI was utilized. The presentation is shaped by the AAU guidelines presented on their website [1]. Neither the module nor the semester description presents explicit declaring statements regarding the use of AI, therefore the default permissive state is assumed for this project *"At AAU you are permitted to use generative AI on a par with other aids unless your module- or semester description states otherwise."*[1].

The specific model utilized in the project is the OpenAI ChatGPT 04-mini-high model, with the capabilities it had in the spring of 2025. The model is self-proclaimed *"Great at coding and visual reasoning"*[2]. It is deemed out of scope for this paper to explore the capabilities of the given model any further, as it would likely be an extensive task without much added valuable insight.

OpenAI provides a convenient feature to share conversations. Conversations can be inspected by clicking the following links. The contents of each conversation will be unpacked after presenting the links.

- Conversation 1 (Image generation): <https://chatgpt.com/share/681b3f8b-936c-8006-9d15-abc33c860c3b>
- Conversation 2 (Developing HelpDesk browser game): <https://chatgpt.com/share/681b3ffa-fcc8-8006-8fe5-324931127f38>
- Conversation 3 (Developing Zelda-like browser game): <https://chatgpt.com/share/681b4034-db10-8006-aaca-e0e4237383be>

Note that the content of conversation 3 was eventually not included in the report, but is included in the overview above for the sake of transparency.

## Purpose and scenarios for use.

The use of generative AI in this project is limited to; generation of- and feedback on- ideas and structure, and for image generation and scripting help in developing browser based challenges. Each use case will be explained in more detail in the following. For image generation, we decided to utilize the capabilities of the AI to generate images which are used in scenario based learning situations. For example, we desired to have a challenge regarding the issue of an employee being tailgated and used the AI to generate images for us; see Conversation 1 for the specific images and prompts. Image generation is, as with most uses of generative AI, heavily debated with regard to issues such as potential copyright infringements and misusing the intellectual property of artists whose material has been used for training. Our understanding of the debate led us to the conclusion that our non-commercial and academic use case allows us to use generated images in an ethical manner. For scripting help in creating the browser based games, we specifically used the model to get our development started on the games. As neither of the researchers has much training in html based scripting, and the fact that our academic

pursuit here does not entail us learning html scripting, our assessment was that using generative AI for this purpose is both ethically and academically defensible. Regrettably, for the one-off type of feedback prompts, where we prompt the AI for tips on rewriting paragraphs and provide input to structuring the paper, we did not save the conversations, and can therefore not present them here. As a mitigating factor, in order to follow good academic practice, we will present a few examples of how and why the generative model was used for input and feedback. Generative AI was utilized as it can propose different angles on encountered problems, and acted as a cooperative partner in brainstorming sessions with the researchers. Three examples of use: 1. Finding ourselves struggling to formulate a specific paragraph, we would provide the paragraph as-is to the AI model, with a prompt to provide tips and guidance on how to increase the readability and clarity of the text. Example 2., in line with using the AI as a brainstorming partner, we utilized its capabilities when creating scenarios for challenges. Having for example made four scenarios for social engineering, we prompted the model for more ideas and angles which we then used to flesh out additional scenarios. Example 3., with a vague idea on what we wanted to include in our background section, but not feeling confident that the section would feel complete, we provided a prompt with the sub-headlines and a few bullet points of potential content and asked for suggestions for improvement.

The above clearly states that Generative AI was used to generate text. An important distinction is, that none of the generated text was directly inputted in the project. Further, we would like to stress that great consideration was given as to not disclose copyrighted material, personal data, confidential data, nor information or knowledge which could implicate Campfire Security or others.

# 1 Introduction

As cyber threats continue to evolve and become more prevalent in daily life and in modern society, there is a growing need for fundamental cybersecurity knowledge. This report explores the use of Capture The Flag (CTF) exercises as a gamified approach to cybersecurity.

In collaboration with Campfire Security, this project set out to design and develop a CTF module. Campfire Security is a company that in 2023 grew out of research done at Aalborg University on optimizing cybersecurity education [3]. Their goal of pioneering gamified learning experiences and developing cutting-edge platforms is backed by the focus on relevant research in the field, a focus on gamified learning, and the dedication to collaborative growth. Through their course platform[4], see subsection 3.4.3, they aim to deliver hands-on and tailored learning experiences. This partnership has played a key role in shaping the direction of this report and establishing its focus on the development of a CTF module. Campfire Security allowed us to use their learning platform to host our CTF module, and we were given permission to work with the templates designed for Campfire Security's platform. This helped provide a scaffolding for our CTF and also allowed us to test our material in their development environment, and also in their production environment.

Throughout the collaboration both parties emphasized regular meetings with clearly stated objectives that were to be completed for each meeting. Some meetings were physical, most were conducted via Teams and coordinated via Outlook.

The regular meetings allowed for rapid iterative brainstorming and prototyping. Thus minimizing wasted effort, as potential mis-alignment or misunderstandings were quickly corrected in the tight feedback loop. This process helped us narrow our topic and target audience. The topic chosen for the module was insider threats, and the target audience was determined to be cybersecurity novices, people with limited prior knowledge of cybersecurity and insider threats. This focus on novices is grounded in the principle "As weak as the weakest link", or "security is only as strong as its weakest point", which emphasizes the importance of raising baseline within organizations and society. This leads to the following primary objective and research question:

*RQ: How can CTF be leveraged to inform cybersecurity novices about the fundamentals of insider threats*

Alongside the research question, a sub-research question emerges:

*SubRQ: How is CTF a relevant concept for teaching cybersecurity?*

Answering these research questions will result in the development of a CTF course on insider threats. Research is naturally constrained by the context of the project and collaboration with Campfire Security. As such, other pedagogical approaches for teaching cybersecurity to novices will not be explored; this report assumes CTF as the primary method of instruction.

In addition, the report will have the material tested by a small test group to acquire insights and feedback, and reflections on potential points of improvement.

The paper is structured as follows: it begins by exploring the concept of insider threats in section 2. Next, section 3 introduces CTFs as a concept, along with gamification, flow, and design principles that would help in the creation of our course material. The section concludes with three reviews of existing CTF platforms that focus on teaching, including Campfire Security's platform, which is used to host our CTF module. In section 4,

we describe our methodology used to answer the established research question; how we conducted interviews, approached the creation of the CTF module, and planned the testing and feedback process. section 5 presents the results of said interviews, section 6 exhibits the course material we developed, and section 7 reviews the testing process and the feedback received. Finally, in section 8, we share our thoughts and reflections and end with the conclusion in section 9.

## 2 Insider Threats

### 2.1 Defining Insider Threats

#### Definition and taxonomy

Firstly, the term "Insider Threat" needs to be defined and scoped, Microsoft defines an Insider as:

*"An insider is a trusted individual who has been given access to, or has knowledge of, any company resources, data, or system that's not generally available to the public"*[5].

While CISA (Cybersecurity and Infrastructure Security Agency) defines an insider as:

*"An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems."*[6]

Even if they vary a bit, the underlying meaning remains that an insider threat is an insider that poses a threat to their company or organization. According to the definition from CISA[6], there are different types of insider threats. The types are as follows:

- **Unintentional Threat**

- **Negligence:** These threats stem from carelessness, and negligence[6]. A simple example of this could be when an unauthorized person gains access to a company by walking closely behind an authorized individual or group[6]. Inadvertently, the group or individual becomes an unintentional insider of this type. This scenario is often referred to as "piggybacking". In short, piggybacking occurs when an unauthorized individual enters a building or system by exploiting human tendencies, such as being helpful. A 'friendly' gesture, such as holding the door open for someone, can pose as a security risk if the person's authorization is not validated or verified. Another example could be an employee postponing security updates or updates in general because it feels like an inconvenient disruption to their work. Although this may not have been done with the intent to harm the company or create a security risk, but an intent for efficiency, it could still create a security risk for their company.
- **Accidental:** These involve accidents, such as clicking a link in a phishing or spearphishing email, typing the recipient's email incorrectly, etc. It is important to note that these do not include carelessness, but are genuine mistakes or accidents. While the intent is not malicious, and accidents happen, they are still considered a security risk and are qualified as a type of unintentional insider threat. An example of this could be the accidental sending of confidential or sensitive information to an unauthorized individual[6].

- **Intentional Threats:**

These are also known as a "malicious insider"[5]. Intentional threats involve actions that are deliberately intended to harm the organization, at some level[6]. They are often driven by personal gain, grievance, or other personal reasons, such as ethics or moral beliefs. An example could be an employee taking a client list and using it to gain leverage for a new position at another company, which harms the current employer but benefits the individual. Another example might be a terminated employee who feels dissatisfied and seeks revenge by leaking sensitive information, sabotaging company equipment, harassing coworkers, stealing data or intellectual property from the company. Lastly, it is worth noting that espionage is also contained

within this "Intentional Insider Threat"[6].

- **Other Threats**

- **Collusive Threats:** Collusive threats are described as a subset of malicious insider threats, where one or more insiders work with an external threat actor to compromise an organization[6]. These are often where the threat actor "Cybercriminals" recruit insiders, to enable fraud, theft, or/and espionage[6].
- **Third-Party Threats:** involve third-parties, like vendors or contractors who are not formal employees of the organization but have been given some level of access to company resources, such as its facilities, systems, network or people to complete their work[6].

While Microsoft defines four types of insider threats, "Accident", "Negligence", "Malicious", and "Collusion"[5], these can align well with CISA's insider threat types. To elaborate "Accident" and "Negligence" correlate with "Accidental" and "Negligence" under the "Unintentional Threats". Microsoft's "Malicious" correlates with CISA's "Intentional Threats" and Microsoft's "Collusion" fits with "Collusive Threats" under "Other Threats" in CISA's definition. However, "Third-Party Threats" are present in the definition from CISA, but it does not appear in the Microsoft's four types of insider threats. This might be due to differences in scope, as the "Third-Party Threats" could be considered a form of supply-chain attack. A supply chain attack occurs when an adversary uses a third party to gain access to the systems, data, networks, etc. of a target organization. The attacker compromises a trusted third party, which has legitimate access to the organization's infrastructure or software, and exploits this access to disrupt or attack the target company. While this is purely speculative, it would explain why a type correlating to "Third-Party Threats" is not present in Microsoft's definition of insider threat.

Interestingly, the Ponemon Institute and DTEX's "2025 Cost of Insider Risks Global Report"[7] have another type of insider threat, "Outsmarted", as seen in Figure 1, while the other types look similar, "Mistaken" being "Accidental", the "Outsmarted", arguably would fall under the "Accidental" or "Negligence" type in the CISA and Microsoft definition. However, in this definition an "Outsmarted" Insider threat is an unintentional insider, who causes harm by being reasonably outmaneuvered by an attack or adversary[7]. This seems reasonable because it does not fall under the carelessness of negligence, nor would it be considered accidental(mistaken). This potentially introduces more nuance into the data, as it can account for something different, such as new attacks, strategies, and technologies that could be considered novel, or even the "first" of their kind. Such scenarios could potentially provide a false representation of Insider threats, since they would be considered an unintentional(Non-malicious), but would neither be "negligence" nor "accidental". Therefore, having an "Outsmarted" category seems reasonable, since it could help provide more detail, and the data and information would be more reliable.



Figure 1: From the "2025 Cost of Insider Risks Global Report" by Ponemon institute and DTEX [7, p. 5].

### Empirical ramification of Insider Threats

In the "2025 Cost of Insider Risks Global Report"[7], a total of 8,306 IT and IT security practitioners were interviewed[7]. The report presents some key findings. A total of 7,868 insider incidents were reported, an average of 23 insider incidents per company. 57% of the companies experiencing between 21 and more than 40 (21-40+) incidents per year. However, this is still an improvement compared to previous years. In 2023, 71% of the companies experienced between 21 and more than 40 incidents per year, and in 2022 it was 67% of the companies[7]. In the 2025 report, 45% of the interviewed reported that they felt the funding allocated to insider risk management was inadequate[7]. The 2025 report also presents an overview of the average annual cost of insider security incidents, which is \$17.4 million (USD), with the previous years averages being, \$16.2 million in 2023, \$15.4 million in 2022, and \$11.6 million in 2019[7]. The average time to contain an insider incident has been reduced to 81 days in 2025, from the previous 86 days in 2023, this is a good sign since the longer it takes to resolve an insider incident, the more it will cost. The average cost if an insider incident takes less than 31 days to contain is \$10.6 million, and \$18.7 million if it takes more than 91 days[7].

The "Verizon 2024 Data Breach Investigations Report", or DBIR, by Verizon[8] consists of 30,458 real security incidents, where 10,626 were confirmed data breaches, with victims from 94 different countries[8]. The 2024 DBIR report, reports that 68% of all the breaches were caused from a non-malicious "human element"[8], meaning unintentional insiders, this is more than 2/3 of all breaches represented. Out of all the breaches 28% of them involved errors, 15% involved a third-party (including software vulnerabilities), and out of the 3,661 social engineering breaches in the report, 73% were from phishing, or pretexting via email[8].

Pretexting involves creating a false story or scenario to gain the trust of the victim, with the goal of manipulating them to reveal confidential information, download malware, transfer money to criminals, or cause harm to themselves or their organization[9]. These reports and their statistics provide a solid overview of the importance, impact, and cost of insider incidents and threats. Companies also spend more on insider risk management than previously[7], and 81% of the companies now have an insider risk management program[7], which is great, but

also indicates just how impactful insider threats are on organizations.

## 2.2 Frameworks for Insider Threats

From the previous presentation on defining insider threats, see subsection 2.1 - it is clear that no single discipline or approach will ever fully encompass the risks posed by insiders.

CISA's definition of an insider is: *"[...] any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems."* [6] exemplifies that insider threat risk management exists in an intersection of governance, technical controls, and even behavioral science. With such a diverse intersection of responsibilities and perspectives, it is unlikely that a single standard or framework can encompass all relevant factors. Depending on the stakeholder and their responsibilities, a framework designed to capture their specific slice of the problem space is likely to be optimal. For executive level decision makers, a macro view and framework, which links insider risk to enterprise wide governance structures, is more relevant than concrete tactics, techniques, and procedures (TTPs) that might be the focus of the blue team security analysts. Accepting this plurality when designing learning material on the topic is a prerequisite for an academically rigorous and practically useful treatment of the topic.

Therefore, this section presents various industry recognized ways of conceptualizing insider threats. The order of the frameworks is not random; rather, they are presented such that the section moves from the strategic minded frameworks to more and more tactical framings of insider threats. For the sake of readability, a high-level overview of the section will be presented in the following bullet points, after which the reasoning for each framework is presented.

1. **NIST Cybersecurity Framework 2.0** – Provides an enterprise level governance framework. Note: Was eventually removed from the paper; see reasoning below.
2. **CISA Insider Threat Mitigation Guide** – Provides a program level blueprint and introduction to the **Critical Pathway to Insider Risk**
3. **CERT Common Sense Guide (7th Ed.)** – Provides 22 evidence based best practices for combating insider threats. Note: Was eventually removed from the paper; see reasoning below.
4. **G-Research Insider Attack Matrix** – Provides a kill chain for insider threat incidents. Note: Was eventually removed from the paper; see reasoning below.
5. **MITRE Insider Threat TTP KB v2.0** - Provides tactics, techniques, and procedures known to be used by insiders

The removed sections can be seen in Appendix A.1.

First of the **NIST Cybersecurity Framework 2.0** (CSF)[10] was intended to be used as it would provide an enterprise level framing of insider threats, recognizing the importance of effective governance structures for any successful cybersecurity program. The framework was eventually removed from the CTF modules due to a partial overlap with CISA Insider Threat Mitigation Guide and a realization that if our course were to speak to a broad spectrum of novices, the amount of detail we could use from NISTs Framework would be very little and only touch on the elements on a high level. From there, the **CISA Insider Threat Mitigation Guide**[11]



will be presented, as it adds program level depth to the governance considerations. Next, the **Critical Pathway to Insider Risk** (CPIR)[12] brings a behavioral perspective to bear, describing personal predispositions past insiders have demonstrated and how triggers and stressors increase insider risk. Progressing steadily toward a more tactical perspective, the **CERT Common Sense Guide 7th Ed.**[13] was intended to present 22 best practices for mitigating insider threat based on research and analysis of more than 3000 insider threat instances. It was eventually removed from the paper and CTF modules as the best practice recommendation overlaps with some of the recommendations from CISA Insider Threat Mitigation Guide, at least to the extent we would use them. Second to last, the **G-Research Insider Attack Matrix**[14] would have been used to present a modified Lockheed Martin Cyber Kill Chain which presents a way to conceptualize critical points and opportunities to mitigate insider threats. Due to the frameworks focus on intercepting or disrupting a kill chain, it was removed, as it presents a perspective on insider threats which was deemed out of scope. Lastly, **MITRE Insider Threat TTP Knowledge Base v2.0.0**[15] provides specific TTPs used by insider threats, which defenders can use to simulate insider scenarios and install adequate defenses.

The goal of the following section is not a full encyclopedic coverage of each of the frameworks. Rather, the objective is to illuminate each perspective provided by the individual framework and how that informs the creation of learning material on Campfire Security's platform.

### 2.2.1 CISA Insider Threat Mitigation Guide

Published in November 2020, CISA's Insider Threat Mitigation Guide (henceforth; the Guide)[11] is a comprehensive document which aims to provide an actionable framework for the establishment and maintenance of an insider threat mitigation program. The Guide defines four specific phases for such a program: **Defining the Threat**, **Detecting and Identifying the Threat**, **Assessing the Threat**, and **Managing the Threat**. The objective of these established program are to: *"understand the insider's interaction within an organization, monitor that interaction as appropriate, and intervene to manage that interaction when it poses a threat to the organization"*[11, p. 23, emphasis added]. Notably, the Guide stress that the objective is to be accomplished while addressing three core principles:

- Promote a protective and supportive culture within the organization
- Safeguard organizational valuables, including privacy, rights and liberties
- Remaining adaptive to organizational changes including risk tolerance levels

The three core principles are symptomatic for the approach taken toward insider threat mitigation program management in the guide. It stresses the importance of shaping culture and highlights how the well-being of organizations' employees or members should be a consideration. This is echoed in principle two, where organizational valuables is not limited to intellectual property and assets, but include privacy, rights and liberties. Lastly, but perhaps most critically, its highlighted that insider threat mitigation programs are in constant flux and should be adapted to the changing circumstances, including organizational changes and development in insider threat attack vectors. Crucially, CISA frames the program as a mechanism to **help people** avoid mistakes: *"not an aggressive enforcement or 'gotcha' programme."* [11, p. 5].

A distinctive feature of the guide's *Detect & Identify* phase is its adoption of the **Critical Pathway to Insider Risk (CPIR)** model as a behavioral lens, shown in Figure 2.

### 2.2.2 Critical Pathway to Insider Risk

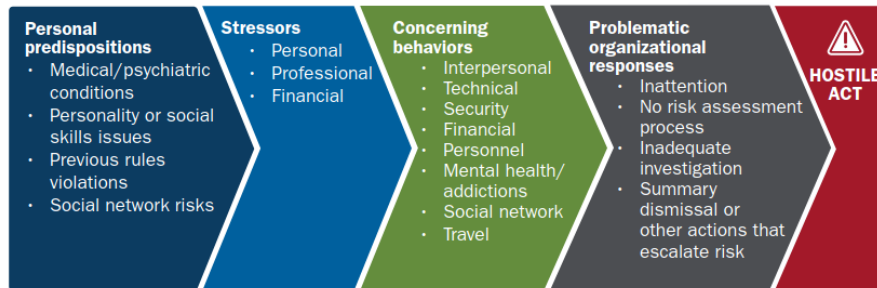


Figure 2: CISA's adaptation of CPIR[11]

Originally by Shaw & Sellers (2015), and more recently retouched by Lezenweger & Shaw (2022), the CPIR model views insider risk as an accumulation and development of four factors that lead to the hostile act: **personal predispositions** (psychiatric conditions, personality, social issues etc.), **stressors** (personal, financial etc.), **concerning behavior** (interpersonal, travel, etc.) and **problematic organizational responses** (inattention, inadequate risk assessment, etc.)[11, p. 42].

The guide expresses the pathway with concrete example like; *"financial need"*, *"Demotion or failure to achieve anticipated advancement/promotion"*, *"Involvement with individuals or groups who oppose core beliefs or values of the organization"*. An important qualification for the examples and the model itself, can be found in Lezenweger & Shaws 2022 revisits to CPIR where it is stressed that while the model seems linear, each step interacts with one another. Particular focus is placed on the organizations response, i.e. the **problematic organizational responses** (named "maladaptive organization response" in the 2022 article). It is made clear that at any point in the CPIR, the organizations actions can either alleviate or exacerbate an insider risk[12].

In terms of technical indicators, the guide provides high level generic indicators, such as *"Direct correspondence with competitors"* or *"Unauthorized configuration file changes or permission changes"*. The technical indicators are explicitly stated as to be a generic structure and a starting point for an organization's construction of actual technical implementations.

From the guide it becomes abundantly clear that managing insider threats is a vast sociotechnical undertaking which has interaction with a wide range of organizational structures, from HR, legal, management and security teams monitoring for specific indicators.

### 2.2.3 MITRE Insider Threat TTP Knowledge Base v2.0

The final step in the presented strategic to tactical continuum is the **Insider Threat TTP Knowledge Base** [15]. Version 2.0 was released in March of 2024, and is maintained by MITRE Engenuity's Center for Threat-Informed Defense. The knowledge base is explicitly presented as an emerging and developing resource aiming to advance the understanding of the technical mechanisms that insider threats employ. It does so through the MITRE vernacular of **Tactics**, **Techniques** and **Procedures** (TTP) mapped to the **ATT&CK** matrix. The TTPs presented in the knowledge base are all based on documentation of actions that insiders actually did in insider incidents. Tactics refers to the overarching goal or behavior of a threat actor. As an example of the vernacular; the tactic *Persistence* has (at the time of writing) 23 techniques associated, including *Account manipulation*, as that is a technique which can achieve the tactical goal of *Persistence*. When investigating the technique, the ATT&CK matrix shows procedure examples, mitigation strategies (eg. M1032 Multi-factor Authentication) and relevant datasources and components (Active Directory Object Modification) for detection of said technique. When these are mapped, a so called "green = seen"-chart can be produced [16] - see Figure 3. This figure shows all the TTPs currently in the Insider Threat TTP Knowledge Base and, as such, demonstrates all the known technical indicators used by insiders, based on the work done by MITRE.

TA0043 Reconnaissance 2 techniques	TA0042 Resource Development 3 techniques	TA0001 Initial Access 3 techniques	TA0002 Execution 1 techniques	TA0003 Persistence 5 techniques	TA0004 Privilege Escalation 2 techniques	TA0005 Defense Evasion 6 techniques	TA0006 Credential Access 2 techniques	TA0007 Discovery 3 techniques	TA0008 Lateral Movement 2 techniques	TA0009 Collection 8 techniques	TA0011 Command and Control 1 techniques	TA0010 Exfiltration 5 techniques	TA0040 Impact 6 techniques
T1595 Active Scanning (r/n)	T1550 Acquire Access	T1133 External Remote Services	T1106 Native API	T1098 Account Manipulation (r/n)	T1548 Abuse Elevation Control Mechanism	T1548 Abuse Elevation Control Mechanism	T1555 Credentials from Password Stores (r/n)	T1046 Network Service Discovery	T1210 Exploitation of Remote Services	T1560 Archive Collected Data (r/n)	T1219 Remote Access Software	T1048 Exfiltration Over Alternative Protocol (p/z)	T1485 Data Destruction
T1595.001 Scanning IP Blocks	T1585 Establish Accounts	T1139 Trusted Relationship		T1098.005 Device Registration	T1546 Event Triggered Execution (r/n)	T1562 Impair Defenses	T1555.005 Password Managers	T1135 Network Share Discovery	T1021 Remote Services	T1560.001 Archive via Utility		T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	T1565 Data Manipulation (r/n)
T1589 Gather Victim Identity Information	T1588 Obtain Capabilities (r/n)	T1078 Valid Accounts		T1136 Create Account (r/n)	T1546.002 Windows Management Instrumentation Event Subscription	T1562.001 Disable or Modify Tools	T1552 Unsecured Credentials (r/n)	T1016 System Network Configuration Discovery (r/n)	T1021.001 Remote Desktop Protocol	T1119 Automated Collection		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1565.001 Stored Data Manipulation
	T1588.002 Tool	T1078.004 Cloud Accounts		T1136.001 Local Account	T1546.003 Event Triggered Execution (r/n)	T1562.011 Spoof Security Alerting	T1552.008 Chat Messages	T1016.001 Internet Connection Discovery	T1021.004 SSH	T1213 Data from Information Repositories (p/z)		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561 Disk Wipe (r/n)
		T1078.002 Domain Accounts		T1546.009 Windows Management Instrumentation Event Subscription		T1070 Indicator Removal (p/z)				T1213.003 Code Repositories		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
				T1133 External Remote Services		T1070.001 Clear Windows Event Logs				T1213.002 Sharepoint		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
				T1078 Valid Accounts (p/z)		T1070.004 File Deletion				T1005 Data from Local System		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
				T1036 Masquerading		T1027 Obfuscated Files or Information				T1039 Data from Network Shared Drive		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
				T1078.004 Cloud Accounts		T1078 Valid Accounts (p/z)				T1074 Data Staged (r/n)		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
				T1078.002 Domain Accounts		T1078.004 Cloud Accounts				T1074.001 Local Data Staging		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
						T1078 Valid Accounts (p/z)				T1114 Email Collection (r/n)		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
						T1078.001 Default Accounts				T1114.001 Local Email Collection		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)
						T1078.002 Domain Accounts				T1113 Screen Capture		T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1561.001 Disk Wipe (r/n)

Figure 3: The green = "seen"-chart for insiders [16]. For larger image see Appendix A.2

Further, for each of the techniques, it is possible to extract specific guidance on how to both mitigate and detect the technique. Beyond the green = seen"-chart, the information used to generate it can be extracted as JSON (and other formats), which makes the data easily ingestible in other tools and workflows. For an organization, it also gives the possibility of mapping their known mitigations and detections against the known insider threat TTPs, allowing for the creation of a heat map indicating where the organization might be lacking in detection capabilities or conversely where they are particularly strong.

The knowledge base is, of course, not without limitations. They openly acknowledge that some information might get lost in translation when they analyze the submitted events which feed their TTP mapping. Further, the *human factor* as they call it, is an area for growth [17].

The human factor is scoped into what MITRE calls **Observable Human Indicators (OHI)**, which is their attempt of creating objective or quantifiable facts about an insider. The OHIs include factors such as; did the subject have elevated privileges, the subjects' time at company, the subjects' government security clearance level and others.

With the open acknowledge of its limitations, it is clear that while enormously tactical in nature, the Insider Threat TTP Knowledge Base is not an one-stop-shop for insider threat mitigation. Combating insider threats is an exercise done at multiple strategic and tactical levels, and across functions from management, HR, legal, security and others. The following section will briefly summarize how we envision these frameworks to inform our approach to teaching the very complex and diverse subject of Insider Threats.

### 2.3 Insider Threat Analysis as a Work Role

In this section, the **NICE Workforce Framework for Cybersecurity** will be presented[18]. The framework provides a standardized way to describe the work being done when performing insider threat analysis. It will provide the nomenclature of **Knowledge**, **Tasks** and **Skills** associated with insider threat analysis, and will be used as a guide for when we design the course material.

The "NICE Workforce Framework for Cybersecurity" is developed the National Institute of Standards and Technology (NIST) [18]. The framework presents a standardized approach to describing cybersecurity work and workers, across both public, private and academic sectors. By its standardized approach and common taxonomy, the NICE framework enables stakeholders like employers, educators and policymakers to have a common language when describing the tasks, skills and knowledge required by the cybersecurity practitioner.

The framework is structured into five overarching **Work Role Categories** which each represents a distinct aspect of cybersecurity work. The Work Role Categories are presented in Figure 4.



Figure 4: **Work Role Categories** as per the NICE framework [19]

The work role categories are further sub-categorized into 52 **Work Roles**, which are groupings of work which an individual might be responsible for. To demonstrate the types of work roles, the following list contains an example work role for each of the work role categories, presented in the format [Work Role Category]:[Work

Role].

- Oversight and Governance (OG): Cybersecurity Policy and Planning
- Design and Development (DD): Enterprise Architecture
- Implementation and Operation (IO): Systems Security Analysis
- Protection and Defense (PD): Insider Threat Analysis
- Investigation (IN): Digital Evidence Analysis

For each of the defined work roles, the framework presents a unique set of **Task**, **Knowledge** and **Skill** statements (TKS statements) which are associated with the effective performance of said work role [20]. Currently, the framework has 2,200+ TKS statements, and as such only a choice few will be presented here as examples. Both Tasks, Knowledge and Skill statements share a format consisting of a unique identifier in bold and descriptive name; [**identifier**]:[descriptive name].

The relation between TKS statements is that while the Tasks describes the work needed to be done, the Knowledge and Skill statements represents an individuals potential to perform said Task. Figure 5 represents the relationship between the three statement types visually.

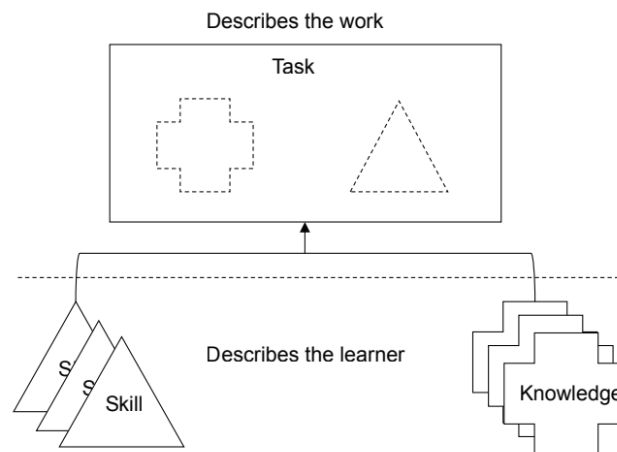


Figure 5: Relation between TKS statements

A Task is to be understood as an activity which has the aim of achieving an organizations objectives. For the work role "Insider Threat Analysis" an example Task could be *T1974: Conduct insider threat risk assessments*. In order to conduct such a Task, a practitioner requires both Knowledge and Skill. A Knowledge statement within the nomenclature of the NICE framework represents a retrievable set of concepts from memory, ie. it is knowledge you know and can remember. An example Knowledge statement could be *K0678: Knowledge of privacy laws and regulations*. Lastly, Skill statements represent the ability to perform a given action, as an example: *S0890: Skill in performing threat analysis* demonstrates a relevant Skill statement.

To demonstrate the relations between TKS statements, consider the following example. An organization wishes to actively develop an insider threat investigation process. Using the NICE framework and its components,

retrievable from the website <sup>1</sup>, the organization identifies the Task *T1997: Develop insider threat investigation plans*, correspondingly they identify the Knowledge and Skills needed to perform said Task;

- K0909: Knowledge of abnormal physical and physiological behaviors
- K1257: Knowledge of insider threat policies and procedures
- K1270: Knowledge of suspicious activity response processes
- K1273: Knowledge of threat investigation policies and procedures
- S0477: Skill in identifying anomalous activity

With all three statements clearly defined, communication between relevant stakeholders can align, allowing for development of appropriate training programs or indeed a targeted hiring process.

---

<sup>1</sup><https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions>

### 3 What is a CTF?

Having looked at the complexities of insider threats, including definitions, and established frameworks such as the NICE framework, the NIST Cybersecurity Framework v2.0 and the CISA Insider Threat Mitigation Guide. To shift the focus towards educational strategies, this section will delve into the concept of CTFs and its potential for gamified learning within the cybersecurity context.

CTF is a well known concept, traditionally originating from games, but has been widely adopted in the field of cybersecurity. In cybersecurity, a CTF is a hands-on challenge, where the goal is to solve a specific task and obtain the flag. Usually, the flag is a unique string of text that serves as proof of the successfully completing the challenge. CTF is a gamified way to learn and test security skills. CTFs come in various formats, but for explanatory purposes, the focus will be on the two broad categories, competitions or events, and platforms. Within CTF competitions, Jeopardy and Attack-Defense are two common types of CTF[21].

**Jeopardy-style** CTFs present participants with multiple challenges, often across different categories such as Web, Crypto(Cryptography) and Forensics. Participants work individually or in small teams, depending on the event. Each solved challenge awards a certain amount of points. At the end of the event, the participant or team with the highest total score is declared the winner[21].

**Attack-defense** involves teams competing in both offensive and defensive cybersecurity tasks. Each team is assigned a vulnerable service that they must protect while they also attempting to exploit the other teams' services. Points are awarded for both defending their own service and successfully attacking opponents[21]. By the end of the event, the team with the most points accumulated is the winner. A well known example of this format is the DEF CON CTF[21]. Competitions are time-limited, meaning that they have a clear start and end date and are inherently competitive. Competitions also usually only use new CTF challenges, to ensure fair competition. While CTF platforms can include competitive elements, like leaderboards and ranking systems, they do not necessarily impose strict time constraints. CTF platforms offer their challenges and services to users to continue testing, learning, and practicing their knowledge and skills at their own pace. They vary in structure and purpose, so offer different experiences. Rules such as "No solution sharing" can foster a more competitive environment, where users are challenged to find solutions independently. Successfully completing a challenge in such a setting can be seen as an achievement and a demonstration of skill. An example of such a platform is HTB(Hack The Box). HTB's 6th rule "Content Sharing and Publication Guidelines"[22], restricts the sharing of solutions for certain challenges, and if violated is a breach of their terms of service[22]. However, other CTF platforms provide solutions, step-by-step guides, or links to write-ups that explain and go through the thought process behind solving each challenge. These platforms serve a different purpose; these often have a more educational focus. Platforms with a heavier focus on teaching and developing knowledge and skills usually presents the user with information on the given topic, and the knowledge needed to complete the challenge, or where to get it, so the user will have an idea of how they can proceed with the challenge. For example, a challenge might require the user to scan a network. Before starting, the user would be given a brief introduction to Nmap, a popular network scanning tool. These platforms encourage learning by presenting the information and allowing users to attempt the challenges at their own pace, and if they get stuck, offers the user guidance

to help solve and overcome the challenge, this can help reduce frustration when not being able to complete the objective. The main focus of these platforms is not necessarily the display of skill, but rather the learning and development of skill.

### 3.1 Gamification

Beyond the basic structure of CTFs, a key element contributing to the effectiveness of CTFs as a learning tool is gamification.

Gamification is the method of using game elements, in a non-game context. Various fields and systems, such as CTF, leverage gamification for different reasons, motivation, engagement, enjoyment are some of the things that gamification can influence and improve[23]. In gamification, some of the common game design elements are:

- **Goals/Objectives:** Clearly defined objectives give the user direction and purpose[23]. Clear, defined goals also help with motivation and maintaining it[23]. In gamification, both short- and long-term goals should be incorporated, to facilitate the potential of flow.
- **Points:** Points are used to reward user actions and quantify performance[23]. They provide immediate feedback, encourage repetition, and can serve as a basis for competition[23]. Points are typically automatically assigned after completion of predefined objectives, with all users receiving the same number of points for the same task[23]. In CTFs, for example, points are awarded after completing a challenge by retrieving the flag and submitting it.
- **Leaderboards:** enables users to compare their performance with others. Leaderboards are an element of competitive game design[23]. The ranking within a group of peers can strongly motivate participants to increase their activity to earn more points and improve their ranking. However, while leaderboards can boost engagement and motivation, their design must be carefully considered, as they can also be discouraging for users[23].
- **Redeemable points:** act as a currency within the game or system and can be used to purchase virtual or real goods[23]. For example, in the HTB Academy, the points earned from completing modules also serve as the currency to unlock modules.
- **Rewards:** Reinforces user behavior by providing compensation for completing actions and reaching goals. Examples include badges and points. Badges appeal to the user's desire for collection and completion. Rewards may be fixed, progressive, or randomly assigned[23].
- **Feedback:** continuous and timely feedback plays a critical role in gamified systems[23]. It often appears as visual signals and cues, such as earning points, unlocking badges, or displaying progress bars[23].
- **Narrative/Story:** Adding a storyline or thematic context can enrich the user experience by providing meaning and emotional engagement. Narratives can help frame goals, connect users to the experience and increase motivation and engagement[23].

Gamification offers a valuable framework for boosting motivation, engagement, enjoyment, involvement, and user experience[23]. Building upon this, the concept of 'flow' represents a further step in optimizing the learning



experience within CTFs, as it is a highly desired outcome in gamification in general[23].

### 3.2 Flow

Flow is defined as the state of optimal experience in positive psychology[24]. Flow is a psychological state of mind in which a person is fully absorbed in an activity, loses track of time, and experiences a deep sense of enjoyment, focus, and energy[24]. It is as if time flies while engaged in the task, leaving the individual completely immersed in the experience. The concept of flow was introduced by the psychologist Mihály Csikszentmihályi, who describes flow as *"There is a common experiential state which is present in various forms of play, and also under certain conditions in other activities which are not normally thought of as play. For lack of a better term, I will refer to this experience as "flow." Flow denotes the holistic sensation present when we act with total involvement. It is the kind of feeling after which one nostalgically says: "that was fun," or "that was enjoyable." It is the state in which action follows upon action according to an internal logic which seems to need no conscious intervention on our part. We experience it as a unified flowing from one moment to the next, in which we feel in control of our actions, and in which there is little distinction between self and environment; between stimulus and response; or between past, present, and future [...]"* from "Flow and the Foundations of Positive Psychology"[24, pp. 136, 137].

Hence, the state of flow is a desired outcome in games, and in gamified systems like CTF. There are certain conditions to enable a potential flow experience [24].

- A challenge with a demand for action, the challenge has to be an active activity, challenging and demand the user to use their skills
- The challenges difficulty has to match the users skill(see Figure 6), if difficulty and users skill does not align either the user moves into boredom or anxious, and out of the space flow can exist.
- Clear, well defined goal(s) - knowing exactly what needs to be achieved is essential to give purpose and direction.
- Feedback - Receiving immediate and unambiguous information about the performance. Both positive and negative feedback can be useful.
- Focus of Attention - The user has to be focused on the challenge, it is important in both entering and maintaining flow.

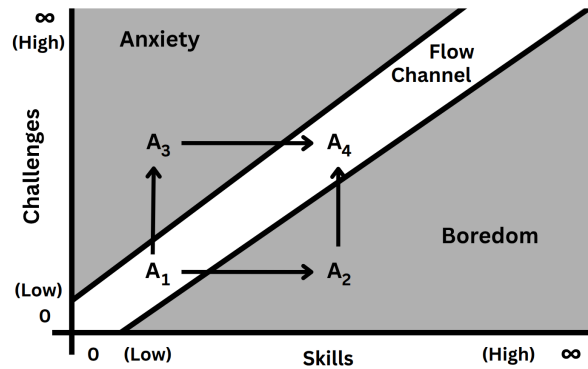


Figure 6: Flow Chart, a recreation of the original from "Flow: The Psychology of Optimal Experience"[25, p. 74]

When in flow people feel enjoyment, a sense of control, and the experience/activity is enjoyed intrinsically, meaning they enjoy the activity for its own sake. They become fully absorbed and involved with the activity, to the point of forgetting time, fatigue, and everything else except for the activity itself, to the point things outside the interaction fails to enter awareness. They are in deep concentration, and can become oblivious to their surroundings. There is an experience of having action and awareness merge, meaning there is little, if any delay from thought to action. These are some of the common sensations associated with being in flow. CTF, events and platform can facilitate flow. Having a challenge presented that is challenging and correlates with the users skill, is exactly also what a CTF can do. CTFs can fulfill every criteria presented to reach flow. If a challenge is neither too easy, or difficult, the is exactly a place where flow exist(see Figure 6). While being presented with too easy or difficult challenge can push result in boredom or anxiety as seen in Figure 6.

### 3.3 Design

Having discussed the concepts of gamification and flow, the next topic focuses on the underlying design principles that contribute to creating an intuitive user experience. Since the objective is to create a CTF module about insider threats, it is appropriate to consider some basic design principles. These can help facilitate a better user experience and offer guidance on how to create the CTFs visually.

The design principles are: Visibility, Feedback, Constraints, Consistency and Affordance. **Visibility** refers to how easily users can perceive available functions or actions within an interface[26]. Functional elements should be clearly visible and indicate what actions can be taken[26]. If a function is not intended for use, it should be less prominent or hidden altogether[26]. Buttons are a good example of visible functions, they signal to the users that an action is possible. **Feedback** refers to providing users with information that reflects what they have done or can do within a system[26]. For example, when a user hovers over a button, it may change color or size slightly to indicate that it is interactive. Similarly, there should be clear visual, auditory etc. feedback after the button is clicked to confirm that an action has been performed. **Constraints** refer to limiting the ways in which interactions can happen, helping to guide the correct actions and prevent potential errors[26]. By reducing the number of possible actions and options at any given moment, constraints help minimize confusion and prevent mistakes[26]. For example a button turning gray indicates that the functionality is currently unavailable. Another example is how flags in CTFs are handled in Campfire's platform. The flags must follow

the format "FIRExxx", where xxx is the unique flag. These are both examples of constraints, and can reduce the likelihood of errors.

**Consistency** refers to keeping things similar[26]. Operations and elements are uniform across a system or multiple systems, allowing users to predict and learn how things work more quickly[26]. An example is when looking at files in a file archive on the computer, every file is shown similarly but might be of a different file type. Another example is the flags format, such as always following the FIRExxx format when handed in. It also lowers the cognitive load by allowing users to apply what they have learned in one part of the system to other parts, or even to different systems. **Affordance** refers to the attributes or properties of an object that suggests how it can be used[26]. In interaction design affordance specifically refers to the visual or physical attributes that indicates how a user can interact with an object[26]. It helps users understand possible actions without needing instructions[26]. For example a button affords clicking. When it looks raised or has a shadow, it implies it can be pressed, these are some visual cues that signals the button's affordance.

These principles will help guide the development of our CTF module, particularly the interactive, hands-on challenges, by making the design and interaction more intuitive to enhancing the overall user experience.

### 3.4 CTF in an Educational Context

With a better understanding of the fundamentals of CTFs and gamification, and how design principles can help create a better user experience this section now explores the use of CTFs in an educational context.

The paper "Advantages and challenges of using capture-the-flag games in cyber security education"[27] is a narrative literature review that explores the viability of using CTFs as a method for teaching cybersecurity[27]. By analyzing various research papers on the topic, the paper presents an overview of the advantages and disadvantages of using CTFs in an educational context[27].

The possible advantages includes:

- CTFs significantly increased participants motivation and engagement[27].
- CTFs game like format makes learning more enjoyable and interactive[27].
- CTFs can potentially lead to statistically better learning results and a deeper understanding of cybersecurity concepts[27].
- CTFs provide hands-on experience, resulting in better practical skills within cybersecurity[27].
- CTFs can potentially increase student's confidence in their cybersecurity abilities[27].
- CTFs can increase interest in cybersecurity[27].

While the possible disadvantages includes:

- A high knowledge requirement, meaning that a certain level of cybersecurity expertise is required from both participants and organizers[27].
- Creating and organizing CTFs can be a complex and demanding task in terms of knowledge, effort, and resources[27].
- Sharing flags[27]. In CTF the flag is a proof, but these can, and has been observed to be shared between participants. which defeats the purpose of CTF.

- Designing CTFs is difficult, particularly in designing challenges to an appropriate level of difficulty and designing effective hints for the challenges[27].
- Quality assurance is often overlooked, which can result in instances like unsolvable challenges or broken websites, which is also described, as a common problem in the paper[27].

However the paper also raises some important points on the current state of existing literature: 1. There is a lack of a strong quantitative approach in papers, in general, regarding the effectiveness of CTF, including many of the studies reviewed[27]. 2. There is a need for future research to use quantitative methods in order to provide stronger evidence of the effectiveness of CTFs[27].

### CTF Platforms

Building upon the discussion of CTFs within an educational context, the focus will now shift to examining specific CTF platforms and how they are actively being utilized for teaching cybersecurity. Various CTF platforms aim to teach topics such as hacking, cybersecurity principles, and the tools commonly used in the field. Platforms for teaching cybersecurity in a gamified way include but is not limited to: Tryhackme[28], Root Me[29], picoCTF[30], ctfLearn[31], HackThisSite[32], HTB(Hack The Box) Academy[33] and PortSwigger Academy[34].

This report will explore both HTB Academy and PortSwigger Academy to review and evaluate how they use gamification and how it is incorporated into their platforms. Then the report proceeds to a review of Campfire Security's platform, focusing on how gamification is applied and integrated. Since the module created for this project will run on Campfire Security's platform, since its structure, features and will play a key role in shaping our module and the overall experience.

#### 3.4.1 HTB Academy

HTB Academy is a platform designed to facilitate learning and teaching in cybersecurity[33][35]. In their own words, *"HTB Academy's goal is to provide a highly interactive and streamlined learning process to allow users to have fun while learning."* from HTB Academy[35]. HTB Academy aims to deliver the knowledge and skills necessary to build a strong foundation in cybersecurity, and help develop a users hacking skills. It offers learning materials on a wide range of topics and has integrated exams and certifications into its platform. HTB Academy is a paid platform. When a new user signs up, they gain access to the introductory module called "Intro to Academy". Completing this module rewards them with **Cubes**, which is the platform's currency[35]. Cubes can also be purchased with real money, and are earned by progressing through modules. Alternatively, users can subscribe to unlock content that would otherwise require cubes.

In HTB Academy the largest structure for organizing learning material is called a **Path**[36]. There are two types of paths **Job-Role Path** and **Skill Path**. A path is a collection of **Modules**. A Module is viewed as a single course, that covers a specific topic. Modules are categorized into three types: **Offensive**, **Defensive**, and **General**. Each module is also assigned a **Tier**, which determines its pricing, tier 0 is free, while Tier 5 is the most expensive. Both paths and modules are assigned a difficulty level, ranging from least to most difficult, these difficulty levels are: **Fundamental**, **Easy**, **Medium**, and **Hard**. A module is a collection of **Sections**, which serve as the smallest

building blocks within the HTB Academy structure. A section is a single page of content, typically focused on one specific topic or theme. There are two types on sections[36]. **Theory sections** are pages with text, that provide the foundational and essential knowledge of the module. They establish the core concepts needed to understand the module as a whole, as well as to prepare for the upcoming hands-on sections. The hands-on sections are called **Interactive Sections**, they allow the user to actively learn, apply, and develop their skills. Interactive sections typically involve working within a VM(Virtual Machine) called PwnBox. The user is given an objective that must be completed within the VM, to get the flag, and to finish the section. Sometimes, additional questions are presented in both types of sections. These must be answered as well to complete the section. In interactive sections questions often require the use of the VM to find the answers. Answering the questions resemble the typical CTF format, where a flag(answer) is the proof of completing the challenge. While in the theory sections question's answer relates to the text material read.

To provide an overview of the HTB Academy structure, and example of the skill path called "Basic Toolset"[37] see Figure 7 will be presented. The "Basic Toolset" is a **Skill Path**, it is of **Medium** difficulty, and contains a total of 7 **Modules**. These modules contains a total 93 **Sections**. Upon completion a total of 110 **cubes** is rewarded, and the total cost of the whole material in "Basic Toolset" costs 470 **cubes**. Upon enrolling the list of the 7 modules will be added to the user's dashboard, each module needs to be unlocked independently, but sums up to the 470 Cubes cost.

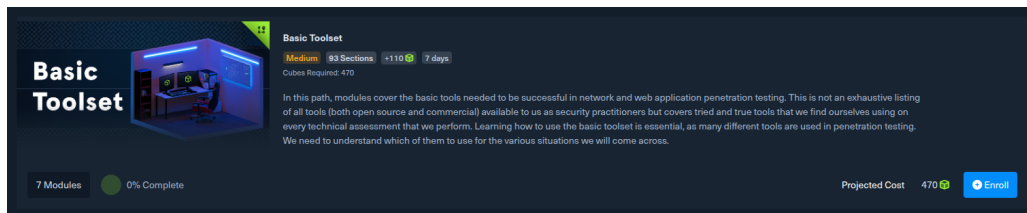


Figure 7: The "Basic Toolset" Skill Path from HTB Academy[37].

The first module in this list of modules is the "Network Enumeration with Nmap"[38](see Figure 8). This **Module** is classified as an **Easy**, **Offensive**, **Tier 1** module. An estimation of 7 hours to complete this module(see Figure 8). On the page of "Network Enumeration with Nmap", users are presented with a description and the overview of the module and its sections(seeFigure 8). In this module there is a total of 12 sections, 4 **Theory sections** and 8 **Interactive sections**. Additionally, users can see which learning paths this module is included in, in this particular case, the module is part of 6 different learning paths. The last thing the "Network Enumeration with Nmap" module page contains is a review section, containing participants thoughts on the module and a 1-5 star rating of it.

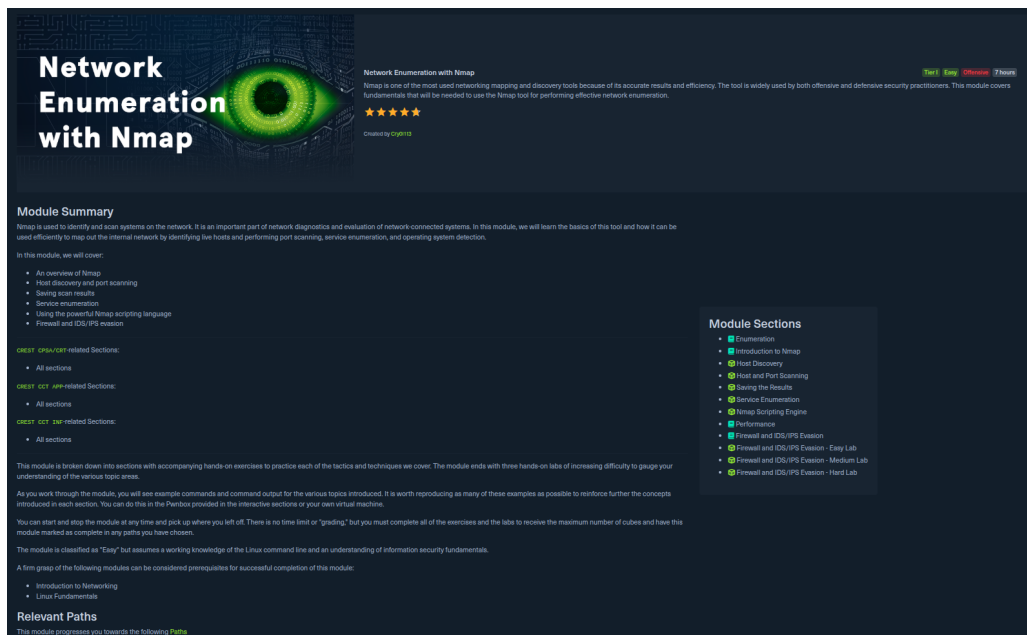


Figure 8: The "Network Enumeration with Nmap" Module[38]. The module summary on the right, and overview of module sections in the left side, from HTB Academy.

HTB Academy's learning material structure in general seems to facilitate "Clear goals", from gamification and flow. Both short term and long term goals seems supported. Sections, modules, and paths are all goals, or objectives to complete. Arguably a path can be seen as a long term goal, while a module may represent a short or long term goal depending on its length. Sections, being the smallest unit, would serve as a short term goal that provide a sense of immediate progress.

HTB Academy use different gamification elements on their platform. When looking at the user's dashboard, see Figure 9, which serve as the "home" page and provides an overview of their progress, streak, and enrolled and completed modules. The dashboard offers valuable feedback which can help reinforce motivation. Another notable element is the current "streak"(see Figure 9). streak is a gamification element designed to encourage daily engagement by rewarding users for daily and consistent activity on their platform. This incentive is used by a variety of systems, such as **Duolingo** a language learning application and **Reddit** a social media platform. Additionally HTB academy also rewards the user with badges and certifications. To the left in the dashboard is a side bar containing an overview of the HTB Academy content, facilitates some of the actions the user can do from this point. This includes the "My Achievements" where the user can review their badges and certifications. It is important to note certifications are given after exams, and needs to be purchased with cubes.

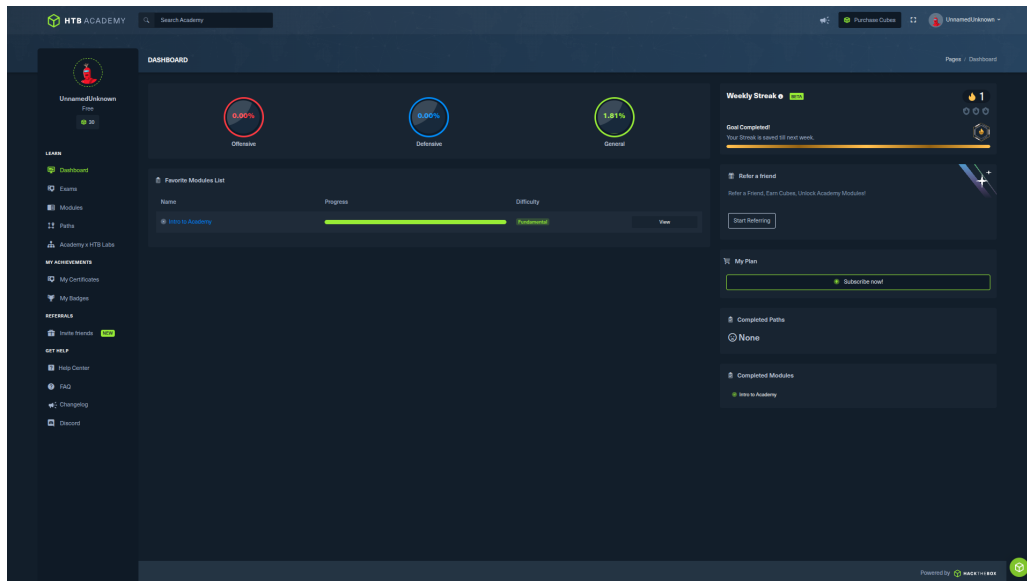


Figure 9: The user's Dashboard

The dashboard also contains the username and a picture of their avatar on the dashboard. An avatar is a gamification element, a visual representation of the user, which can enable individuality and differentiation between users[23].

In general HTB academy seem to incorporate various different gamification elements, and arguably facilitates the requirements needed for a person to reach flow. To review some of the reasons:

- Clear goals are established through the structured hierarchy of their learning material, paths, modules, and sections. Each path and module includes a summary, paths include a list of its modules and modules a list of all its sections, helping users understand their objectives.
- Difficulty matching skills - Is supported by the step by step structure, theory sections provide the necessary knowledge, while questions and interactive challenges test that knowledge and skill. Each module also includes a difficulty rating, guiding users to choose appropriately challenging content, if they wish to be challenged.
- Demand for action is present in all sections. Theory sections require active reading comprehension and answering questions, while interactive sections require user input, interaction and answering questions.
- Feedback is provided at multiple levels. On the dashboard, users can track their overall progress. During modules, correct or incorrect answers prompt immediate responses. During the module a sidebar to the left is always present, which highlights the current section, marks completed ones, and leaves unfinished or skipped sections unmarked. This offers a clear visual indication, and feedback of the progress within the module.

The design is also visually appealing, with a coherent and consistent aesthetic throughout the platform. Constraints are applied thoughtfully in various parts of the experience, including the left side bar in the dashboard. Their use of consistency is particularly evident throughout the platform, and is especially helpful during module completion, where the list of sections on the right provides users with clear and continuous visual feedback on

their progress. Overall, HTB Academy incorporates numerous visual cues and use the design principles well to make their design more intuitive, user friendly and easy to use.

A search on "insider" and "insider threat" in HTB Academy's search function, revealed two modules containing sections dedicated to insider threats:

- **"Supply Chain Attacks"** [39]- In the module's summary: *"Insider Threats are another critical aspect, covering types of insider threats, their impact on supply chain security, and mitigation strategies."*. The module also contains a Theory section called "Insider Threats", and an Interactive section called "Insider Threat Attack". The module contains several sections that may be relevant to insider threats, although it is unclear whether the sections address the topic specifically.
- **"Introduction to Information Security"**[40] - Contains two Theory section "Insider Threat" and "Social Engineering". But no other mentioning of "insider threats" in the sections

These two modules seem to be the only modules having "insider threat" or "insider threats" as part of a sections name in their module. While not having a dedicated section, other modules showed up in the search, but "insider threat" is neither mentioned in the modules descriptions or section lists. An example of this is the module "Introduction to Red Teaming AI"[41]. This module mentions "insider threat" in their "Attacking Data Components" section, this is revealed in the search. But "insider threat" is neither a dedicated section or mentioned in the description. This provides no real value, however, the main take away is there are 3 sections which a specific focuses on insider threats, 1 of which is an interactive section. Otherwise Insider threat is mentioned in relation to other sections.

Having gained access to the "Introduction to Information Security" by purchasing it with cubes generated, a review of the content revealed some interesting insights. Firstly the modules definition of insider threat types are, "Malicious Insiders", "Negligent Insiders" and "Compromised Insiders". These types are not coherent with the definitions this report found, but rather seem as the authors own definitions. Secondly in general for all modules are a lack of references, which could prove useful for transparency and credibility. The section "insider threats" do relay the main takeaways about insider threats in their explanations. It does also mention a "insider threat kill chain" which could be the one described in Appendix A.1.3. However without references there is no way to be completely sure. For an example there is also an insider threat kill chain from DTEX, which is called "The DTEX Insider Threat Kill Chain" <sup>2</sup>.

### 3.4.2 PortSwigger Academy

Having looked at HTB Academy, the next platform to review is PortSwigger Academy[34]. PortSwigger Academy is a platform focused on teaching web security, where users solve challenges using PortSwigger's tool **Burp Suite**. One of the main reasons users engage with the platform is to prepare for the Burp Suite Certified Practitioner (BSCP) exam and earn the certification. This certification demonstrates a strong understanding of web security vulnerabilities and the practical skills required to identify and exploit them using Burp Suite. This certification can be a valuable asset for professionals, especially penetration testers. The PortSwigger Academy

---

<sup>2</sup>Link to it: [https://www.dtexsystems.com/wp-content/uploads/2024/08/DTEX\\_Guide\\_Threat-Kill-Chain.pdf](https://www.dtexsystems.com/wp-content/uploads/2024/08/DTEX_Guide_Threat-Kill-Chain.pdf)



is organized into learning paths, an initiative to make their content more user friendly, and three main topics. The main topics are **Server-side topics**, **Client-side topics**, and **Advanced topics**[42]. Each of these topics include several subtopics, which each contains a number of labs. For example the Server-side topic contains the "SQL Injection" subtopic, which contains 18 labs in total[42]. Labs are the interactive challenges presented to the user. This is equivalent to a CTF challenge in some aspects. However they differ by not requiring users to submit flags. Instead their system automatically verifies whether the objective has been achieved and provides feedback upon completion. Whether these labs qualify as CTFs is outside the scope of this project, what matters is that they offer a gamified approach to learning web security, and the tool Burp Suite. The user can choose between multiple learning path, topics, or labs. A learning path is a *"[...] structured approach to learning web security, empowering you to advance at your own pace while ensuring a deep understanding of the subject matter."*[43]. A learning path contains a page total, these pages can either be text which provides the knowledge on the given theme, or labs. Each lab has a difficulty level, **Apprentice**, **Practitioner** or **Expert** and the user needs to use Burp Suite<sup>3</sup> to complete it. The presentation of labs follow a consistent design. As seen in Figure 10 the labs begins with their title and lab's difficulty level, "Apprentice", in this instance, along with the user's progress status "Solved" or "Not Solved"[44]. A brief description outlines the challenge and its objective. A "Access The Lab" button allows the user to launch the lab environment. Additionally the labs contains Hints, Solutions and Community Solution. Hints offer subtle guidance, not every lab has these. The Solution provides a concise, step-by-step guide written by PortSwigger Academy. Lastly the Community Solution features YouTube videos from users demonstrating how to solve the lab. The lab in Figure 10 is part of the labs in the "SQL Injection" topic[44]. On the left hand side, an overview of the topic is shown. Each section consists of explanatory text, may include multiple labs and can be quite a long page. Meaning the page's content can be quite long and require multiple scrolls to reach the ending.

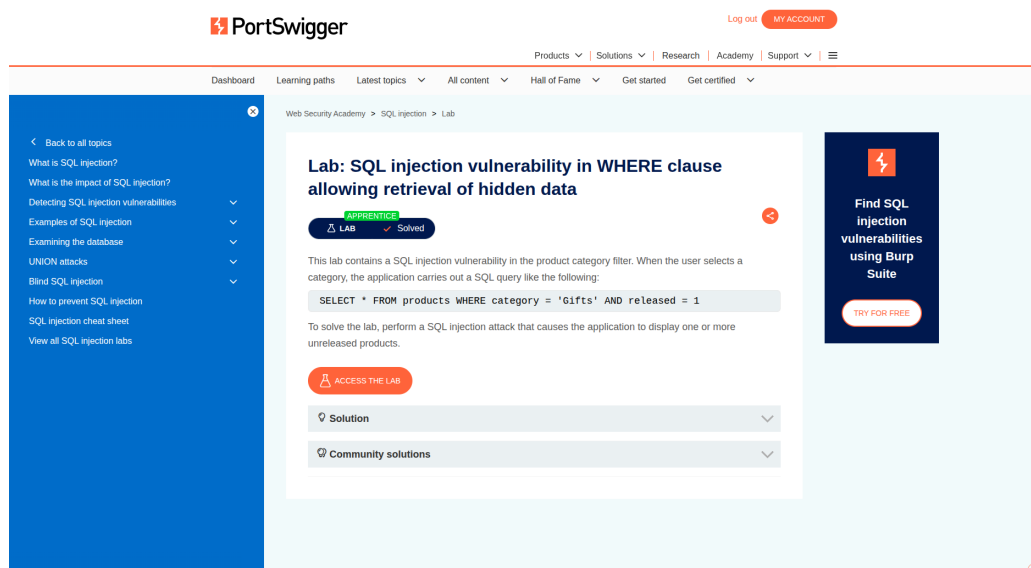


Figure 10: The "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data" from PortSwigger Academy[44].

<sup>3</sup>Or an alternative, however using Burp Suite seems appropriate

← PRACTITIONER SQL Injection 6 of 51

WebSecurity Academy

**My progress**

- What is SQL injection?
- How to detect SQL injection vulnerabilities
- Retrieving hidden data (3 of 3)**
  - Subverting application logic
  - SQL injection UNION attacks
  - Determining the number of columns required
  - Finding columns with a useful data type
  - Using a SQL injection UNION attack to retrieve interesting data
  - Retrieving multiple values within a single column
  - Examining the database
  - Blind SQL injection
  - Exploiting blind SQL injection by triggering conditional responses
  - Error-based SQL injection
  - Exploiting blind SQL injection by triggering time delays

**Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data**

APPRENTICE Solved

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

ACCESS THE LAB

Solution

Community solutions

BACK CONTINUE →

Up next: Subverting application logic

Figure 11: The "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data" from PortSwigger Academy, but accessed through Learning Path[45].

In Figure 11 is the learning path "SQL injection"[44]. In the learning path information is presented in a more segmented format, making each page smaller, typically fitting within a single visible frame or just slightly more. This design choice allows each page to focus on a specific point or step, making the material easier to digest and is therefore more user friendly. The side bar to the left is different than the one previously viewed. This side bar provides additional visual cues about the user's current location within the content. In Figure 11 it is third section from the top, and includes 3 subsections, this currently being the last of the 3. At the top left in the, there is an "6 of 51", which is a general overview of how far the user is to completing the learning path.

Another feature on PortSwigger Academy, is the user's dashboard. The dashboard contains general feedback, an overview of the user's current progress, and also has a "Exam preparation steps" section, which does help keeping track and facilitate the long term goal of getting the certificate.

While the learning path's design is more user friendly, some aspects could be improved upon in terms of the gamification and flow theory. The general overview, such as "6 of 51" (in Figure 11) provides a clear indication of overall progress in completing the learning path. This can be seen as a way to present a the long term goal clearly. However, the section overview on the left, lacks some transparency. Each of the sections can contain multiple subsection, but the user will first know, how many, or how big the section is, when entering. Improving the visibility of this information before would provide the users a better understanding of the scope and effort required before starting a section or short term goal. Another example is their "Hall of Fame"[46] leaderboard displaying the top 50 users, this is measured by how many labs the user has completed. All of them have completed every lab, and with the limited labs and release of new labs. The leaderboard does not reflect overall engagement or skill, but rather who was first to finish the new content, which as mentioned is released rarely. While the "Hall of Fame" display the top 50 users, every users can view their own ranking, they cannot view their position in relation to others[46]. As a result, progressing in rank lacks a sense of context or meaningful

competition, which could reduce the motivational value usually associated with leaderboards.

PortSwigger Academy is primarily aimed at teaching web security, with a strong emphasis on mastering Burp Suite. As the creators of Burp Suite, PortSwigger provides an ideal platform for learning how to use Burp Suite, particularly for those preparing for the BSCP exam. However, the educational content is limited to this focus on web security and the use of Burp Suite, while the content is excellent, it is limited to about 269 labs. This focus also limits the platforms to a specific audience, namely, users who are actively using Burp Suite, intend to use Burp Suite or wants to get the BSCP certification. <sup>3</sup>

One of the most impressive features of PortSwigger Academy is their labs. These hands-on, interactive challenges are really well designed. Each lab includes clear objectives and is supported by solutions, community solutions and potentially hints. This helps ensure that, even if users get stuck they have access to a wide range of helpful resources to continue learning effectively. The platform is entirely free to use, with no cost associated with accessing the learning content and is an excellent place to learn Burp Suite and web security. However, both the exam and full access to the Burp Suite software requires payment. While there is a free version of Burp Suite available, it comes with limits to its functionality, which the paid one does not. To take the certification exam, users must have access to the paid version, as it provides the full set of features required to complete the exam tasks. Additionally, several labs on PortSwigger Academy also rely on features exclusive to the paid version, making it necessary for users to upgrade if they wish to complete all content and prepare effectively for the exam<sup>4</sup>.

### 3.4.3 Campfire Security's Platform

As mentioned earlier, this project is working in collaboration with Campfire Security and has been granted permission to use their platform to host the course CTF its learning material and the challenges[4]. Therefore, this section will examine and review Campfire Security's platform, as it will be an integral part of the user's experience and interaction with the module.

#### The Dashboard

The first thing the user encounters is the user dashboard (see Figure 12)[4]. Similar to the previous platforms, this serves as a collection of information and feedback to the user.

---

<sup>4</sup>While alternatives exist which could compensate for features missing in the free version, using them feels counterintuitive given one of the platform's goals is teaching Burp Suite.

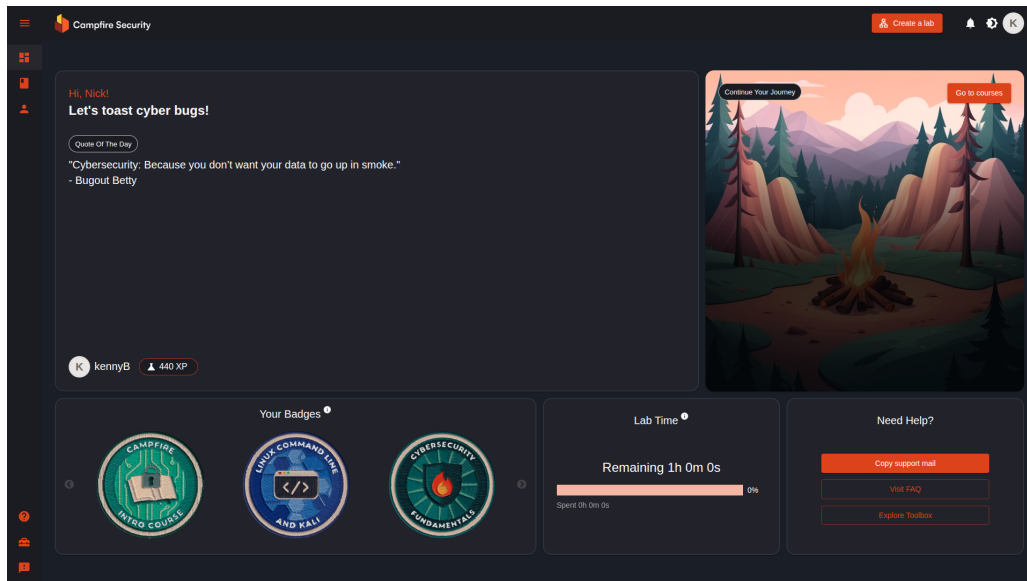


Figure 12: The users' dashboard, on the Campfire platform[4].

The dashboard is clearly designed to fit neatly within the browser window, allowing the entire content to be visible in a single frame. As mentioned previously this is a user friendly design, by having all the content presented to the user without anything hidden or a need to scroll to review content, this makes it easier to get a clear overview of the content. In the top of the dashboard is a header bar, with the company's name and some functionality. In the right side of the header bar, from the left, is an orange button with an icon and the text "Create a lab". Clicking this will open a pop up prompt with the text "Choose lab type", which is seen in Figure 13. The pop up contains the two options the user can access the lab, "VPN lab" and "Browser Lab", both with a small description of what the option encompass. Lab is the VM environment where the interactive CTF challenges are completed. Next to the "Create a Lab" button is a bell icon which opens a drop down with the users notifications. The bell icon indicating notifications are used in various systems to illustrate notifications, which provides some consistency between systems and an expectation of it being used for notifications.

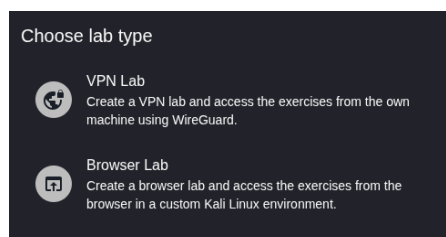


Figure 13: The "Choose lab type" Pop up from clicking "Create a Lab"

The next item in the header bar, is another icon<sup>5</sup> which is a "Toggle theme" functionality, which allows the user to choose between a light or dark theme for the visual presentation of the layout. In Figure 12 and the other figures presented in this section are the dark theme. Lastly a circle with a letter, the first letter of the user's username. The circle is clickable, when clicked a drop down menu appears with 4 sections or choices. Each

<sup>5</sup>In the Dark theme the icon is a moon, while in light theme it is a sun

option with a matching icon are: Account, Plans, Settings and Logout.

On the left side of the dashboard is a side bar, which visually matches the header bar, making them blend in with each other. The first option, from the top, expands the side bar, revealing descriptive text next to each icon. This functionality appears to be well thought out, since it compresses the remaining content to make space for the sidebar(see Figure 14). Keeping everything, all content, visible within a single frame.

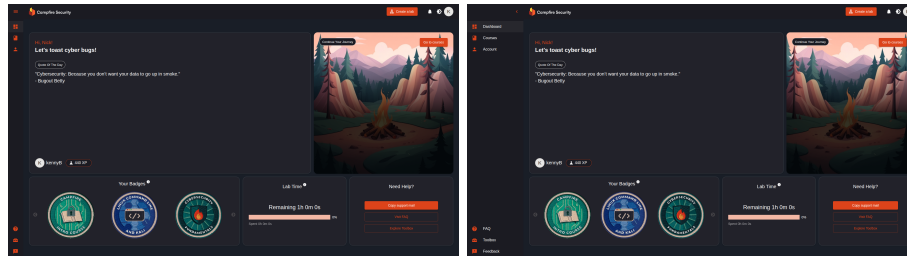


Figure 14: A comparison and visualization of the sidebars expansion impact on the visual

The sidebar contains the Dashboard, Courses, and Account, and further down, FAQ, Toolbox, and Feedback, along with their icons.

Turning the attention from the side bar. The next section, to the right of the side bar. This section contains a greeting to the users registered name and a quote of the day. In the bottom left corner is the user's username, together with the users current XP(Experience points). Experience points or xp, is a gamification element, and is used to express experience and progress. It is often used in relation to levels, and "leveling up". In Campfire Security it is used as Points, mentioned in subsection 3.1, and is one of the Rewards Campfire implements. In Campfire Security's platform, XP is given by completing tasks from courses, and from completing a course. The amount of XP gained depends on the difficulty of the task, or course. The amount is a fixed size, each task gives a fixed amount depending on their difficulty. Completing a course provides extra points, which are also a fixed size. These extra points serve as extra incentive for users to finish courses. Moving along, to the right is an image of a campfire with text "Continue Your Journey", and "go to courses", which is a button and will redirect the user to the Course page. Next is the bottom section of the page, this includes 3 containers or sections. First from the left, is the badge section, the text "Your Badges" presented with the users obtained badges. The badge section shows the badges obtained. Badges are another use of rewards and are obtained from completing courses or exercises. There are two small circles with an arrows one on each side. When hovered over, the cursor changes to a hand, providing visual feedback that they are clickable. The buttons are subtly colored and blending in, in Figure 12, which suggest the functionality is currently unavailable. These design elements serve as visual cues to guide user expectations and interaction with the buttons. They indicate that a scrolling functionality is possible by clicking, although currently disabled, suggesting that if there were more, hidden badges, they could be accessed by clicking. However this is the only section that displays the user's badges, and only displays the ones already obtained. Badges that have not yet been earned are not visible, which might influence the incentive to collect them. Without knowing what is missing, the user's motivation or desire to collect could be affected, as they might be unaware of missing badges.

Next section is the "Lab Time" section, which illustrate the current time left for the user to use the labs. There is a time limit with the free account and "Hacker Club Member" subscription plan, which resets daily. The

"Remaining Xh Xm Xs"<sup>6</sup> will count down the time left, while the bar beneath will slowly be filled from left to right, giving a more visual representation. To the right of the bar is a percentage of the time used in relation to the total time limit. Beneath the bar, "Spent Xh Xm Xs" counting up, this display counts the time used. All these are different ways to present feedback and in some essence the same information, in presented differently. This can make it clearer, but could potentially also make it more complex and complicated for the user, since it is a lot of visual feedback, with the the same information just presented in different ways.

The last container contains an additional way to access the FAQ and toolbox. The Support however is a new functionality not mentioned before. When clicking the "Support" button, the email for support will get copied into the clipboard, allowing the user to reach out to support by sending an email. Lastly something worth mentioning is the small white circles with a "i" in them, they are next to "Your Badges" and "Lab Time" text in Figure 12. These provide additional information when hovered, such as how to obtain the badges, or when the lab time resets. This helps with minimizing the amount of content presented to the user, which can improve the user experience. By reducing the amount of content displayed on the dashboard, it helps decrease the likelihood users will get overwhelmed by being presented too much information at a time. It also helps give a cleaner design which can help with maintaining an overview, but still provide easily access to additional information about the content.

In general a well structured dashboard encompassing useful information and feedback to the user. The design follows a pattern of having functionalities, or interactive objects presented in the same orange color. This helps the user with mapping functionalities and helps in guiding their next course of action.

## The Course Library

This section, the course library page, contains all the available course the user can partake and complete[47]. The header bad and side bar are a consistent element through out each page's layout. This sections content is beyond a single visual frame, and does allow scrolling.

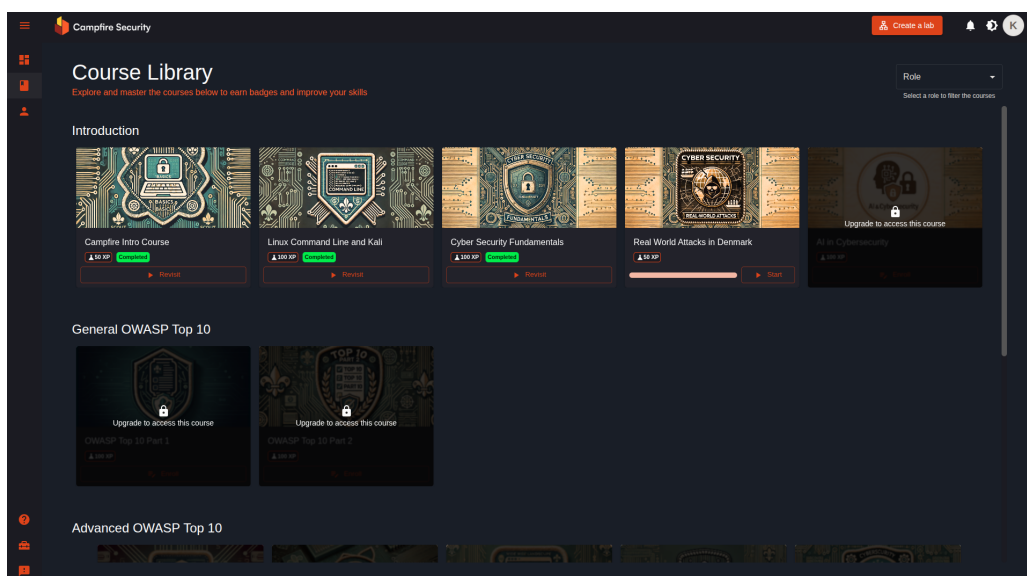


Figure 15: The Course Library section[47].

<sup>6</sup>In "Xh Xm Xs", X is a numerical value. h is hours, m minutes and s seconds.

The courses as seen in Figure 15 are in a grouping, and each course are a visually represented with an image, and under it the course's name. The image is course specific and is also used in the certification. After finishing a course the user will have the option to get the certification, another use of rewards. This reward is, however, used outside the platform, and is a downloadable, printable certification. Each course had a certain amount of xp given when completed, which is displayed under the course's name. Beneath the xp is a progression bar accompanied with an "Enroll" button, if the course has not been started. If the course has been completed a "Revisit" button replaces the progression bar and the enroll button. The progression bar gives a visual representation, and feedback of how far along the user is with completing the course. This concludes the overview of the course's visual appearance, but there is still some functionality remaining. Upon hovering the course name and image, the cursor changes to a hand, suggesting interactivity. Upon clicking the user will be presented with a pop up, as seen in Figure 16. This pop up contains a description of the course, the related themes or tags, and the xp. As seen in Figure 16, the course "Campfire Intro Course" contains 3 themes/tags: "The platform", "Flags" and "Virtual laboratory".

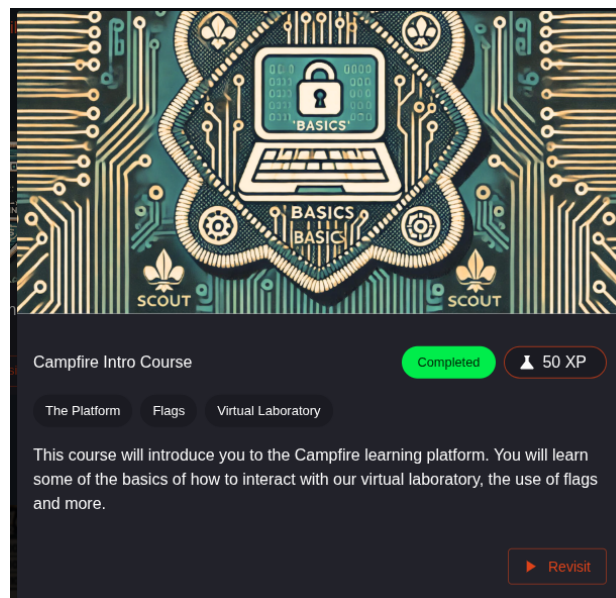


Figure 16: The Campfire Intro course's Pop up.

Returning to the course library. The course library page contains a total of 4 "Main topics" or areas: "Introduction", "General OWASP Top 10", "Advanced OWASP Top 10", and "Open Source Intelligence". These cannot be seen in Figure 15, but are accessible by scrolling. In Figure 15 the first three courses under "Introduction" are completed, which is illustrated with the "Completed" text inside a green box. While the fourth course is yet to "Enroll" and complete. The fifth course has a dark layer on top of it, and a lock icon with the text "Upgrade to access this course". The design choice of adding a dark layer on top resembles that of changing colors slightly to illustrate, that there is a functionality, but is currently unavailable. While the lock and explanatory text tells the user why. The lock icon again is an icon used by many systems to illustrate unavailable content. Therefore it offers some consistency between systems, but the lock icon also gives clear feedback, and affordance, making a connection between a real world use and a virtual one. The physical purpose being keeping unwanted/unauthorized entities out, by requiring some form of key to gain entry. In this context the



user can click the course and be presented with a "Upgrade Now" option. Meaning, upgrading to or being on a subscription plan serve as the virtual key user to get access.

Lastly in the top right corner of the page, is the text "Role" in a box. This is a drop down menu, upon clicking the user will be presented with some options: "Access Controls", "Cryptography", "Cyber Security Fundamentals", and "Operational Technology (OT) Security". Clicking any of these will hide irrelevant topics, while displaying the relevant courses, making it easier for the user to filter out unrelated topics. This can help maintain or give an overview when the amount of main topics and courses increase. However currently this function suggest it's a work in progress since the connection between "Role" and the options seems to be missing. This is purely speculative, but it could either be intended for work roles categorization, enabling filtering relevant courses for a given role. Or it is a way to categorize or filter specific topic, across the main topics. For example when clicking the option "Cryptography", hides some but there are still multiple courses presented across the main topics.

The course library page's design is mostly consistent with that observed before, on the dashboard page. The exception being the "Role" drop down. It is displayed without any orange, which was observed previously to indicate some sort of functionality or interactivity, this does break with the consistency. Upon hovering it, it's border do turn orange, which provides some visual feedback suggesting functionality, and the border turning orange remains consistent with the theme. However, previously the orange color also helped the user with navigating, visually guiding the user to what the available functionalities were. Choosing not to have orange associated, reduces the chances the user will see or noticed it, and therefor also its use.

## The Course

When the user has enrolled and is starting the course the user is presented with the learning material for the first section, as seen in Figure 17.

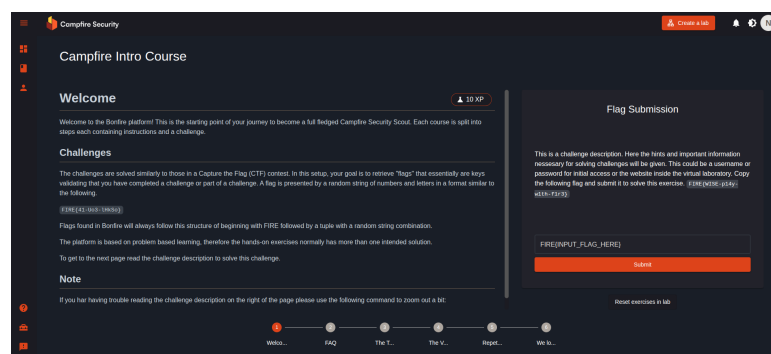


Figure 17: This is the first section or page of the course "Campfire Intro Course"[48]

To help with the description see Figure 18. The image is similar to that of Figure 17. However Figure 18 contains three boxes, numbered 1, 2 and 3, to help simplify the process. Just above box nr.1 is the course's name, in this example it is "Campfire Intro Course"[48].



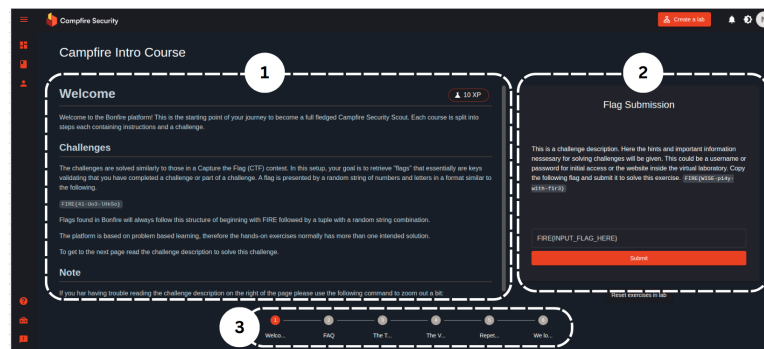


Figure 18: Same image as Figure 17, but with visuals

Box nr.1 contains the learning material for the current challenge, which is the written information the user should read before doing the challenge presented in Box nr.2. Box nr.1 has some limitations in size, which means if the learning material exceeds the height of that boundary, a scrolling bar will appear to enable scrolling, as seen in both Figure 17 and Figure 18. This restriction on Box nr.1 enables the layout to remain inside a single visual frame. In box nr.1, in the top right corner, is the xp awarded for clearing the current section's challenge. As mentioned earlier, completing single tasks within a course award points as well as completing a whole course. Inside Box nr.2 is the summary of the challenge. Beneath that is the input field for the flag, which is already containing "FIRE{INPUT\_FLAG\_HERE}" in Figure 18, and underneath the input field is the "Submit" button, to hand the flag in. The "FIRE{INPUT\_FLAG\_HERE}" is a placeholder, and an illustration of the flag format, to present visually how the flag should be entered. When hovering the input field the white border turns orange, and when clicking stays orange, and the placeholder moves up to the border, and becomes part of the border. When the placeholder moves, it leaving the input field empty, to let the user type in the flag. However the placeholder text remains a part of the input fields border, and is written in orange. The placeholder text constantly provides the user with a visual cue, of where the flag should be entered, how the flag format is, and what the input field is used for<sup>7</sup>. The placeholder is implemented well, both the animation of it moving, how it becomes part of the border, and its functionality of providing the user with guidance on entering the flag. The submit button again making a connection between orange and interactivity and functionality. Just beneath Box nr.2 is a "Reset exercises in lab" button, currently blending in with the background, to show the user that the functionality is not currently available. Upon hovering the button, some additional information is displayed, in Figure 18 the information was the reason why it was not functional<sup>8</sup>. In Box nr.3 there is an overview of the course. For example in Figure 18 it is the first challenge out of a total of 6. Each circle has the correlating section's header text, displayed beneath the circle. The first circle is orange with the number 1, indicating this is the current challenge, while the rest are gray. When completing the challenge, the next circle will turn orange, while the previous circle will remain orange and the number, will change to a check mark. Indicating the challenge has been completed. This visual representation provides the user with feedback and a clear overview of the course's content. The circles also work as the way to navigate the course material, clicking a circle changes the content to that correlating with that circle. When submitting the flag a feedback prompt

<sup>7</sup>If the user leaves for a while and comes back, the input field would have some text associated with its purpose

<sup>8</sup>The information was "You do not have an active lab session"

will appear inside the area of box nr.3. In Figure 19 is how the feedback is visually presented.

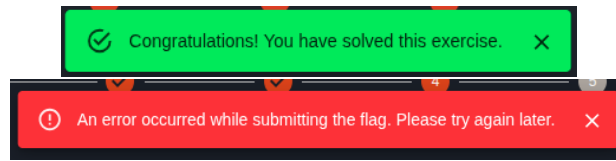


Figure 19: The feedback submitting flag. Top being feedback on correct flag submitted, and the bottom an incorrect flag submitted.

The green box, and first from the top in Figure 19 is the feedback when submitting the correct flag. If this prompts the page will also change automatically to the next challenge. The second one, from the top, in Figure 19 is the feedback from submitting an incorrect flag, which is instead inside a red box. However the incorrect feedback does not provide clear enough feedback, *"An error occurred while submitting the flag. Please try again later."*, does not acknowledge it was the wrong submitted, but instead tells an error has occurred. In general Another potential thing to mention is in Box nr.3, if the user has completed the whole course and revisits it. The user will not have the orange visual cue to help anymore, but will have to rely on the text underneath the circles to navigate, and which of the sections they currently are in.

### Virtual Hacker Lab

Lastly, the Virtual Hacker Lab can be seen in Figure 20. The Virtual Hacker Lab in Figure 20 was run in the browser, one of the options available to users. The Virtual Hacker Lab is a VM with Kali Linux installed. Kali Linux is an open source Debian based Linux distribution. Kali Linux is designed with a focus on penetration testing and hacking, by having multiple useful tools pre-installed and ready to use. Tools such as Nmap, Metasploit, Burp Suite and John the Ripper.

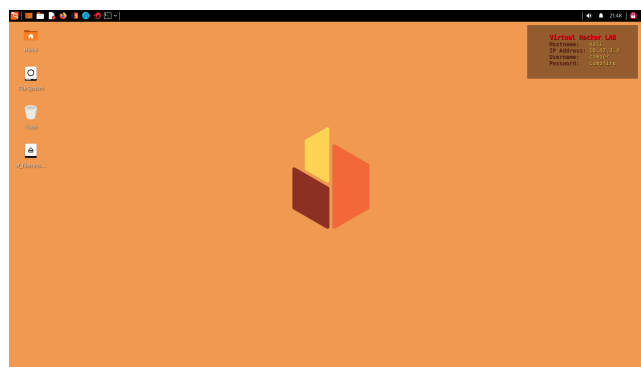


Figure 20: The Virtual Hacker Lab.

The Virtual Hacker Lab is the environment in which the user will solve the challenges of the courses. This is where our CTF challenge will run and where the users will solve them and find their flags.

Reviewing the three platforms provides a good overview of the subtle differences, but also highlights the many similarities. They each follow the CTF like format, incorporating gamification elements to help enhance the user

experience, and can help facilitate additional motivation and engagement in users. They each also facilitate some of the main requirements for reaching flow. This includes providing clear goals and feedback. While providing a clear distinction in difficulty levels for users to choose between and assess the difficulty of an objective and goal, not necessarily matches the difficulty of a challenge with the users' skill, it enables user to determine which challenge to choose depending on their own estimation of skill. Each platform also provides feedback to the user while working on their chosen challenge, but also in the form of a user dashboard containing general overview of their progress, and current situation on the platform. Each platform additionally shares similarities in their design. Color choice might differ, but the overall structure of what and how things are presented is similar. For example each has a dashboard; they might visually be different but encompass similar design elements and functionalities, such as an overview of the user's progress. Another example is the way the learning material is presented, in challenge or learning material section there is an overview of the current course or module throughout its completion, allowing a clear overview of both the short-term goal, and the long-term goal of completing the whole course or module. Lastly, they differ in some aspects like PortSwigger Academy being web security focused, but in general the themes and modules on the platforms touch the same topics. There is a clear overlap on each platform, having similar themes, modules and containing similar topics. However, none of the platforms reviewed has a dedicated Insider Threat module. Insider threats might be part of a larger topic or module, but in general there seems to be a lack of dedicated focus on this particular topic. While it is part of larger topics or themes, like threat actors, the content and information about insider threats are limited and usually just a "reading" experience, leaving out the interactivity. When reviewing HTB Academy one of the modules had an insider threat section and an interactive challenge, which is a good initiative to create some interaction. However, insider threats were still a fraction of the complete module and course. This highlights a potential need for a dedicated focus on insider threats. A module where the vast information and material about insider threats can be unfolded and enables interactivity to let the user use and apply knowledge about insider threats in hands-on exercises like CTFs instead of it being a reading experience.

This was the summary of the review of the three platforms from HTB, PortSwigger and Campfire Security.

Having reviewed its similarities, appealing aesthetics, core functionalities, and the integration of gamification, subsubsection 4.2.3 will elaborate on how this project created its CTF module about insider threats, and used Campfire Security's platform to support the CTF module.

## 4 Method

This section will present the methodological approaches used throughout this project. The methods utilized are in the service of answering both the research and the sub-research questions:

*RQ: How can CTF be leveraged to inform cybersecurity novices about the fundamentals of insider threats*

*SubRQ: How is CTF a relevant concept for teaching cybersecurity?"*

### 4.1 Semi-structured Interviews

From the context of qualitative research methods, we intend to utilize semi-structured interviews as a means of exploring our subject matter. This is done with a relevant expert, as it can be an important step in gathering insights on our field, especially since the field is relatively underrepresented in academic research. We chose to rely on semi-structured interviews as we seek to combine both structure and flexibility. Unlike structured interviews, which follow a strict script, semi-structured interviews have an "incomplete script" comprised of themes or subjects to be approached in the interview. These allow interviewers to adapt their questions based on the participant's responses and thus open the possibility for new topics to emerge [49]. The intention of using semi-structured interviews is to extract the lived experience of our participants. The format is intended to allow participants to feel at ease in elaborating on topics that genuinely matter to them, thus generating richer and more authentic data. However, the interview format will of course introduce drawbacks as well. The most pertinent to our circumstances is the inability to reproduce the interviews, which scientifically is a noteworthy issue. In addition, time and resource demands can be significant for this style of interviews, as the openness that generates the rich details also risks resulting in longer interviews and a more extensive transcription and analysis phase.

To provide a semistructured interview with as much structure and direction as possible, while still allowing for improvisation and curious exploration of the subject matter, Myers and Newman (2007) suggested treating the interview situation as a drama with a stage, props, actors, an audience, a script, and a performance. Each component of the drama has to be involved in preparation or during the interview situation itself.

As a **drama** the interviewer has to carefully manage impressions, this entails showing empathy and allowing space to upon for the interviewee to reveal their personality and identity. However, equally perhaps equally important, it also entails navigating the social interplay between interviewer and interviewee and steer the conversation without being domineering. The **stage** of the interview is the location in which the interview is conducted. This entails considering where the interview takes place and what that particular setting can impose on the interview situation, i.e., an interviewee might be more comfortable doing the interview somewhere private as opposed to in an open office environment, etc. Although such considerations are important, they can be difficult to control, as they require knowledge of the preferences and temperament of the interviewee. Further, when conducting an interview with busy people, the interview situation might be through a phone call while the participant is on commute, or similar, despite potentially being outside of the interviewers' control,

the potential influence on the interview is something worthwhile reflecting on. The **actors** of the drama or interview, are both the interviewer and interviewee. For Myers and Newman (2007) considering both parties as actors, involve given consideration as to how to foster the appropriate level of seriousness to the situation, both in how we as interviewers conduct ourselves and how we dress for the situation. The **audience** is to be understood as a multifaceted term, it can be used to mean either the interviewer or the interviewee depending on who is talking. But the term also refers to the audience at a larger scale, underlining considerations such as giving consideration to who might read the paper being published and evaluating whether special care should be given to anonymize the interviewee or even form explicit nondisclosure agreements if appropriate. The **script** is the questions prepared to guide the conversation. Preparation includes, but is not limited to, having an opening introduction of the researchers and their intention with the interview academically. Crucially of course, preparation also entails having key questions formulated. Lastly, how to end the interview should also be prepared, which include asking permission to follow-up, or asking who else the interviewee recommends might be interviewed. Preparing the script is essentially a balancing act, with the goal of having the preparation aid the interview process in its active curious exploration of the subject, while not being overly cumbersome or too loose. The **performance** is the culmination of all of the above and is paramount: *"The quality of the performance affects the quality of the disclosure which in turn affects the quality of the data."* [49].

#### 4.1.1 Analyzing the Interview

In order to extract the most analytical insight possible from the interview situation, we approached the analysis in a structured and thorough manner. As per Lichtman's (2013) three C's of data analysis, we analyzed both transcript and observation notes for codes, categories and concepts [50]. Figure 21 visually demonstrates the approach taken in the analysis.

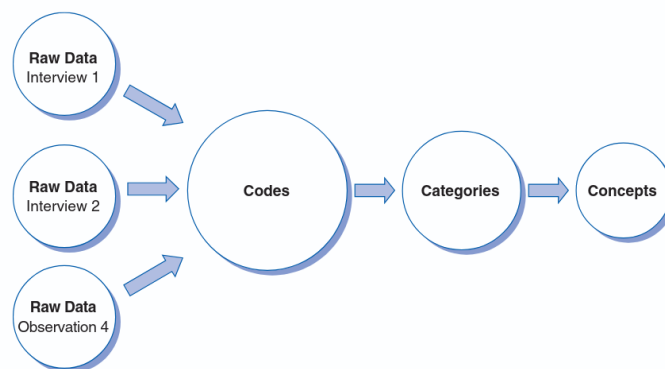


Figure 21: The three C's[50, p. 252]

The analysis process then; starts with initial coding or labeling of the particular meaning bearing segments, to developing categories or what can be thought of as major topics that emerge from the coding process. These categories are then condensed into fewer, but well-supported concepts, as doing so makes *"[...] for much richer analysis than many loosely framed ideas"* [50, p.254]. Both the interview transcript, and the notes taken by the observer, were analyzed.

A note on the implementation: this process will be done on only one of the two interviews, see reasoning later

in section 5.

## 4.2 Course Development

### 4.2.1 Operationalizing Frameworks for Training

The frameworks reviewed in section 2 serve as the conceptual guardrails for the course material we design for the Campfire Security platform. As such, each framework is used to offer a different vantage point or perspective which shape the content, tone, and learning objectives of the material. The following will present the broad strokes of what each framework provided in our course material. A more detailed explanation of the implementations of the frameworks in the course material is presented in section 6 in the subsections for each module.

As the initial step, from the NICE Workforce Framework for Cybersecurity [18], the definition and TKS statements for the Work Role of Insider Threat Analysis was analyzed. This particular Work Role is defined as being:

*"Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations."*[51]

The stated Work Role area of responsibility is broad, and bundles detection, technical forensics and legal duties. This area of responsibility is extensive, and too extensive to be covered in a course designed to cover the fundamentals of the insider threat concept. Therefore, it is necessary not to just blindly use the presented definition of the Work Role. Rather, we create and present a version inspired by the definition, but geared to our audience and research question - *How can CTF be leveraged to inform cybersecurity novices about the fundamentals of insider threats*. A cybersecurity novice, who is informed of the fundamentals of insider threats is to be able to:

#### **Recognize common indicators, understand basic preventive controls, and know when to escalate**

This statement was refined through iterations and in collaboration with Campfire Security. The statement leaves out areas such as advanced forensics and considerations, legal considerations and counterintelligence activities from the definition of the initial Work Role, which presumably could be flagged as next stage competencies in a potential follow-on course.

In order to identify which TKS statements are relevant for our participants, we take outset from the TKS statements which are related to the Insider Threat Analysis Work Role, see Appendix A.3 for the complete TKS statements. The original contains 58 Task statements, 75 Knowledge statements, 36 Skill statements. Any TKS statements that exceeded the scope of what a cybersecurity novice, who is informed of the fundamentals of insider threats is to be able to was excluded. Thus leaving us with 2 Task, 12 Knowledge, and 12 Skill statements (see table 1). The statements retained still map cleanly onto the original role, preserving face validity while aligning with realistic expectations for our target audience.

Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
T1983	Identify potential insider threats	S0913	Skill in performing link analysis	K1261	Knowledge of known insider attacks
T1974	Conduct insider threat risk assessments	S0910	Skill in performing cyberintelligence data analysis	K1258	Knowledge of insider threat tactics
		S0908	Skill in determining the importance of assets	K1257	Knowledge of insider threat policies and procedures
		S0907	Skill in identifying insider threats	K1256	Knowledge of insider threat operational indicators
		S0896	Skill in recognizing behavioral patterns	K1249	Knowledge of digital and physical security vulnerability remediation principles and practices
		S0890	Skill in performing threat analysis	K1248	Knowledge of digital and physical security vulnerabilities
		S0866	Skill in performing log file analysis	K0785	Knowledge of insider threat tools and techniques
		S0854	Skill in performing data analysis	K0784	Knowledge of insider threat laws and regulations
		S0848	Skill in performing behavioral analysis	K0721	Knowledge of risk management principles and practices
		S0690	Skill in performing midpoint collection data analysis	K0684	Knowledge of cybersecurity threat characteristics
		S0540	Skill in identifying network threats	K0683	Knowledge of cybersecurity vulnerabilities
		S0477	Skill in identifying anomalous activity	K0682	Knowledge of cybersecurity threats

Table 1: Chosen TKS statements

The presentation of when which TKS statements was included in the course material is presented in section 6 Figure 22.

The remainder of the presented frameworks from subsection 2.2 each contribute in their unique way a perspective or approach to the development of the course material. The goal of including perspectives from this range of frameworks is to be able to cover as much as possible of the Insider Threat topic. Balanced of course, with the needs of the targeted audience group.

- **Strategic perspective:** The enterprise level language of the *NIST CSF 2.0* and the program blueprint in CISA's *Insider Threat Mitigation Guide* should set the frame for exercises with a governance and cultural approach. Note, that NIST CSF 2.0 was removed as per reasoning described in subsection 2.2.
- **Behavioral lens:** The *Critical Pathway to Insider Risk* encourages story lines that acknowledge human stressors and organizational responses, ensuring that technical clues appear in a plausible narrative rather than in isolation.
- **Practical themes:** CERTs 22 best practices act as a menu of topics like; privileged access hygiene, separation of duties, exit process controls, from which we can draw learning objectives and narratives. Note, that CERTs contribution was removed as per reasoning described in subsection 2.2.
- **Actionable TTPs:** The *Insider Attack Matrix* and MITRE's *Insider Threat TTP Knowledge Base* supply ample inspiration for the creation of realistic and data-driven exercises, which mimic TTPs actually used by insiders. Note, that the Insider Attack Matrix was removed as per reasoning described in subsection 2.2.

The sections can be seen in Appendix A.1.

As with TKS statements, how and where each framework influenced the course material is presented in section 6.

#### 4.2.2 The Modules

The development of the CTF and the associated learning material was guided by the principles of gamification, flow, and effective design, as detailed in section 3. The process involved incorporating gamification elements to enhance user engagement and motivation. This included creating a narrative, provide clear goals and objectives for each challenge, deliver continuous and clear feedback, and ensure that the learning material prepared the user for each challenge. The challenges were designed to increase in difficulty, trying to follow a correlating with

knowledge and skill development. In addition the material was created with an intent of matching difficulty with skill, starting from scratch, but attempting to increase in difficulty as the user's understanding and skills progressed, while avoiding abrupt difficulty spikes. These criteria were intended to facilitate the potential for users to reach a state of flow, characterized by a deep concentration and an intrinsic enjoyment. The design principles was used to create an intuitive layout for each challenge. This involved using visual cues, providing clear visual feedback, and maintaining consistency in layouts throughout the course to guide the user experience and reduce confusion. However variations in the feedback presentation were intentionally introduced to provide some diversity across challenges. While a recurring visual cue in the feedback was color; correct answers would consistently be associated with green, and incorrect answers with red, providing consistency while changing how the feedback was presented.

The CTF hands-on challenges will primarily be created using HTML, complemented by CSS and JavaScript. The accompanying learning material will be written in Markdown to properly fit the format already used on Campfire's platform.

### 4.2.3 The Campfire Platform

Campfire Security's platform facilitates our CTF module, which makes the platform a part of the experience. This means that while we did not create the functionality, it is still a part of the complete package. For example, the platform facilitates gamification elements, such as rewards as points (xp), certificates, and badges. The module will have a certificate and points, xp, facilitated through the platform, which enable some gamification aspects from the platform to be a related part of our module.

Therefore, the course material and module will try to enhance the experience and fit well with the already established platform- For example, the module will not use points as rewards, but be using the established point system, xp, which campfire security already has. Another aspect is how their platform appears and works which will also play a major role in the module. Therefore, through iterations the material was uploaded to the test environment and changed and tweaked until it was a desirable outcome.

## 4.3 Testing in a Workshop

This section details the methodological approach employed to test the developed CTF modules and gather feedback with the aim to engage in iterative refinement. The primary aim of the testing was twofold: firstly, to ascertain the understandability and feasibility of the CTF course for individuals considered cybersecurity novices, and secondly, to collect qualitative feedback to guide improvements to the course material and challenges. The testing was conducted as a workshop involving employees from Statens It.

During an one-hour workshop followed by 30min evaluation, we invited four employees from Statens It to test our course. The contact and booking of the workshop was facilitated and arranged by one of the researchers, who has a professional connection to Statens It. The workshop was held during business hours, which posed the risk that participants were called away for other tasks. One participant was unable to complete the workshop synchronously due to external commitments and instead completed the course materials and questionnaire asynchronously at a later time (this will be discussed further in section 8).



The initial approach for the workshop, was to emphasize the collaborative and learning nature of our particular CTF. We wanted to make sure to align the participants expectations with ours, and had prepared a short list of bullet points which was used as a talking paper for the introduction. This introduction lasted the first 5 minutes of the workshop. It included a presentation of who we are, the estimated timeframe for the CTF, and by the end would like to collect some feedback. We also emphasized the workshop was meant as a "team game", elaborating talking, collaboration and helping each other was encouraged.

The notes for the talking paper, and the notes taken during both the workshop and a subsequent debrief are appended as Appendix A.4.

### The setting of the workshop

The workshop took place in a meeting room designed for eight people, with eight chairs arranged around a round table placed in the center of the room. The room was well lit and had two large windows that let plenty of sunlight in. The room had a TV mounted on the wall, which the participants all sat facing. The TV was connected to one of the researchers laptop, which allowed us to demonstrate and guide the participants through the initial steps, such as setting up accounts on the Campfire platform. Each participant was to bring their own work laptop on which they engaged with the course individually.

### The participants

There were four participants in the workshop. Three were so-called "graduates" in Statens It, meaning they *typically* have little or no IT background nor cybersecurity knowledge. In contrast, one of the participants is a security analyst, who has years of experience and cybersecurity specific knowledge, see Table 2.

Participant ID	Job role	Cybersecurity experience level
<i>P1</i>	Graduate	Basic awareness
<i>P2</i>	Graduate (IT)	None
<i>P3</i>	Graduate	Other
<i>P4</i>	Security Analyst	Intermediate/hands-on

Table 2: The participants

Table 2 shows the participants' own answers regarding prior cybersecurity experience; it is evident the group has a self-reported diverse level of experience from "None" to "Intermediate/hands-on". The "Other" answer is clarified as the individual haven taken a 15ECTS course in network security as a part of their education.

#### 4.3.1 Data Collection Instruments

Multiple methods were employed to gather data on the participants' experience and the usability of the CTF module.

**Observation:**

The researchers took systematic observational notes throughout the workshop. Aiming a level 3 or 4 degree of observation, in which we seek to limit our interaction and intervention, but also allowing for the opportunity to use active control over the situation in order to elicit specific information should we deem it beneficial [52]. Using observation notes as data points aims to capture participants' engagement, points of confusion, collaboration instances, and overall interaction with the CTF. Observation is a recognized method for gathering data on usability in naturalistic settings (ibid.).

**Questionnaire:**

Immediately following the workshop, participants completed a questionnaire designed to elicit feedback on various aspects of the CTF module. The questionnaire included the User Engagement Scale-Short Form (UES-SF) to measure **Focused Attention**, **Perceived Usability**, **Aesthetic Elements**, and **Reward Factor** [53]. The UES-SFs consists of 12 questions (three for each of the categories).

One of the three questions related to Focused Attention is *I lost myself in this experience* and the rest follow the same theme. In broad terms the questions relate to how absorbed and concentrated participants were during the experience. One of the three questions related to Perceived Usability is *I felt frustrated while using this Application X* and the rest follow the same theme. In broad terms the questions attempts to understand the ease of use and the level of frustration experienced by participants while interacting with the course.

One of the three questions related to Aesthetic Elements is *This Application X was attractive* and the rest follow the same theme. In broad terms the questions are focused on the visual appeal of the course.

One of the three questions related to Reward Factor is *Using Application X was worthwhile* and the rest follow the same theme. In broad terms the questions are focused on the perceived value of the experience with the course. Additional questions covered the perceived overall difficulty of the challenges, preference for the CTF learning style compared to traditional methods, the influence of storytelling on their experience and engagement, and their confidence in explaining a learned concept to a colleague.

**Qualitative Feedback:**

Beyond structured questionnaire responses, open-ended qualitative feedback was encouraged to allow participants to elaborate on their experiences and provide specific suggestions for improvement. This was collected through written comments in the questionnaire and informal discussion during the debriefing session, post workshop.

**4.4 Ethical Considerations**

For the workshop we ensured participant confidentiality by making all data collected through questionnaires and observational notes anonymized. Participants were informed about the purpose of the study and how their data would be used. Participation was voluntary.

For the interviews, explicit permission was given to include the interviewees names and personage in the report. For both interviews the participation was voluntary and the participants had to option to have potentially confidential information withdrawn from transcript and report.

## 5 Results: Interview

### 5.1 Interview

In the project we conducted the following expert interviews as seen in Table 3. Both interviewees gave explicit permission to be referred to by name in the project.

Date	Interviewee	Interviewer	Topic
30-04-2025	Thomas Kristmar	Nick Blume	Cybersecurity Training
23-05-2025	Kristian Larsen	Nikolaj Jørgensen	Teaching novices within a CTF framework

Table 3: Table of conducted interviews

Thomas Kristmar is one of two Heads of the Center for Security and Compliance in Statens It and leader of the Danish Foreign Ministry’s Operations team, a more detailed expounding of Kristmars profile is presented in subsubsection 5.1.1.

Kristian Larsen is the CEO of Campfire Security and our main point of contact for the external collaboration. Kristian provided many valuable inputs throughout the process as detailed in section 1 and his contributions are implicitly present in the project, regrettably we did not further analyze or utilize the interview we did, see section 8 for the reasoning behind this decision. The full (Teams generated) transcript of the interview with Kristian is available as Appendix A.5.

As such, the following sections will limit itself to engage with *an* interview - singular, that being the interview conducted with Thomas Kristmar.

The interview was done in person and recorded and transcribed manually as per a modified *intelligent verbatim* approach [54]. This approach removes unnecessary filler-words or other partly pronounced words and sentences, however laughter was included in the transcript. In addendum to the transcript, thorough notes were taken by the observer, see Appendix A.6. The transcript was sent to the interviewee for confirmation, and the final and approved version can be seen in Appendix A.7 - note, the version in Appendix also includes our coding of the interview (see section 5.1.2 for more on coding). The interview was conducted in Danish. Quotes presented in the paper have been translated by the researchers.

#### 5.1.1 Interview: Thomas Kristmar from Statens It

Aligning with Myers and Newman (2007) the following considerations were done pre-interview. In order to situate ourselves as researchers and interviewers we familiarized ourselves with Thomas’ professional background (e.g., LinkedIn bio, known publications). Further, as one of our group members (Nikolaj) has a professional relationship with Thomas we had to consider how that would affect the interview process. There are both positive and negative aspect of a previously established relationship. As a positive the existing relationship makes it easier to establish initial contact and allowed for an easier scheduling of the interview. This, as we could make use of the local meeting facilities as Statens It, and contact could be established face-to-face in

Thomas' familiar work setting. However, the pre-established relationship implies also existing shared experiences and perhaps a common language and way of communicating. In order to avoid the negative aspects, the group decided to delegate the interview process such:

- Nikolaj existing relationship to handle initial setup and booking of meeting
- Nick will do the actual interviewing and have a leading role in the interview situation
- Nikolaj will during the interview take notes and intervene as little as possible during the interview

Based on prior knowledge and our short research in Thomas' professional profile, we learned that he has a significant professional and academic background. His professional background entails both private security consulting and a leading role within the national cybersecurity center (Center for cybersikkerhed - CFCS). Academically his pedigree is equally robust, and he is currently a reviewer for the international publication "Computers & Security" <sup>9</sup>. With this in mind, we shaped our interview guide to best utilize him as a resource. Also it informed our decision to introduce ourselves in a less casual and more professional way than we initially had planned. It also informed our decision to forego control of where the interview would be conducted (setting the stage), as we deemed it necessary to be flexible in planning, due to Thomas presumably having a busy calendar. Further, it informed our decision to dress business casually and not shy away from technical language. In order to both be transparent with our intentions and following the advice of Myers and Newman (2007) we made sure to stress in our initial communication with Thomas, that if he preferred we would be willing to sign non-disclosure agreements. The following interview guide was developed leading up to the interview:

Theme/Focus	Rationale	Sample questions
1. Introduction & building rapport	Opening the "drama" and setting the stage. Establish interviewee as the knowledgeable 'actor'	- What is your current role and responsibilities?  - Why is Insider Threats an important topic?
2. Defining Insider Threats	Explore the interviewee's frame and vocabulary for Insider Threats	- How do you personally define Insider Threat?  - Is there anything lacking in the common conceptualization of the term?  - What sorts of indicators/behaviors do you associate with Insider Threats?  - What would you have liked an earlier version of yourself to know about Insider Threats?
3. Cybersecurity training in general	Open the 'stage' and allow interviewee to 'perform'	- How do you conduct cybersecurity training in Statens It?  - How do you feel good cybersecurity training looks like?
4. Cybersecurity training in practice	Steer the 'performance' towards challenges identified	- When conducting cybersecurity training, who are the most likely target audience?  - From your experience, what makes good cybersecurity training? what makes the knowledge stick?
5. Future needs	Open the 'stage' once more and allow for interviewee to give advice	- How do you envision the future of cybersecurity training to look like? What would have the most impact?  - Which emerging tools or methods (AI-based analytics, user behavior monitoring) might transform insider threat detection?
6. Closing	Exit from the "stage" and explain next steps. Ask for follow-up and snowball	- Is there anything crucial about insider threats we haven't covered?  - Would it be okay to reach out if we have additional clarifications?

Table 4: Interview guide for interview A.

A larger and more easily readable version of the table is available as Appendix A.8.

### 5.1.2 The Findings from the Interview

Both the interview transcript and the notes taken by the observer were analyzed with the goal of extracting supported concepts. The transcript of the interview, including initial codes, is available as Appendix A.7. The

<sup>9</sup><https://juc.dk/undervisere/thomas-kristmar>

observation notes are available as Appendix A.6 - note, codes are marked with blue writing. The mapping of codes to categories and onto concepts is available as Appendix A.9.

From the transcript, 55 codes were gathered. From the observation notes, 19 codes were gathered. Combining the codes, the categories were narrowed down to four, which led to the four condensed concepts.

1. Insider risk = motivation + opportunity phenomenon
2. Security is an organizational obligation operationalized through governance rituals
3. Behavior changing training hinges on: relevance, interactivity and contextual fit
4. Trust culture and emerging technologies create a double-edged landscape

These four concepts influenced our own conceptualization of insider threats and the way we approached the effective formulation of said concept to a target audience. Concept 1 *"Insider risk = motivation + opportunity phenomenon"* reinforced the need for our CTF scenarios to not only present a technical vulnerability (the opportunity) but also to incorporate plausible motivations, making the threats and concept more realistic. Further, Concept 3 *"Behavior changing training hinges on: relevance, interactivity and contextual fit"* directly validated our use of the CTF format. The interviewee's perspective underscored the importance of hands-on, engaging content that learners can relate to their own environment. Concept 2 *"Security is an organizational obligation operationalized through governance rituals"* highlighted that while our CTF focuses on individual learning, for an organization it is critically important to embed such training within broader organizational security practices if it is to have real world impact. Lastly, Concept 4 *"Trust culture and emerging technologies create a double-edged landscape"* prompted us to consider scenarios that reflect modern technological environments and the nuanced ways trust can be exploited, even in introductory material.

A range of codes and subsequent categories from the interview pertained to *espionage* and four motivation types (MICE - Money, Ideology, Compromise and Ego, from Appendix A.7) which can be exploited to lead a person to become an insider threat. This subject and theme was prevalent in the interview, but not to an extent where it qualified as its own concept. It is mentioned here despite this, as it while not immediately relevant for the project, it did spark many subsequent reflections for the researchers about possible pivoting the course to include espionage as a theme. It was evidently not included, as it shifted the course to a more organization centric focus, and thus potentially losing some of the courses ability to be used on a broad audience of novices.

## 6 Results: Course material

This result section is dedicated to the course material. Each module developed will be presented with both the learning material and the associated challenge explained. The versions used are the compiled versions, the files (html, markdown etc.) are added to this project in a separate zip archive. Before engaging in the presentation itself, the following will firstly present some of the findings "at a glance" and then present the structure that the reader can expect from the course material presentation sections.

### Results: Course material at a glance

This results section utilize **four** distinct frameworks, for each module the frameworks utilized are shown in Table 5.

Framework	Integrated in Module 1	Integrated in Module 2	Integrated in Module 3	Integrated in Module 4	Integrated in Module 5	Integrated in Module 6
<i>NICE Workforce Framework for Cybersecurity</i>	✓	✓	✓	✓	✓	✓
<i>CISA Insider Threat Mitigation Guide</i>	✓	✓	-	-	✓	-
<i>Critical Pathway to Insider Risk</i>	✓	✓	-	-	✓	✓
<i>MITRE Insider Threat TTP KB v2.0</i>	-	✓	✓	✓	✓	✓

Table 5: Framework integration in modules

The integration of each framework is rarely made explicit to the user. Rather, the integration of a framework entail its insights and scaffolding permeating through the material and challenges as opposed to direct exposition of the framework content to the user. This is done as the researchers deemed it for the target audience only would add unnecessary cognitive load if the frameworks themselves became explicit, instead we focused on bringing forth the points from said frameworks that we saw as essential for the users to know in order to:

#### **Recognize common indicators, understand basic preventive controls, and know when to escalate**

Following that logic; on Table 1 in section 4 we defined the desired TKS statements our course should touch upon. The wording "touch upon" is used here to demonstrate there is a difference in rigor and "depth" in how a TKS statements is approached, some are approached from multiple angles and fleshed out, others are addressed with fewer detail.

The comprehensive coverage of TKS statements within the course is illustrated in Figure 22, which indicates the specific modules addressing each statement.

Task ID	Included in modules	Skill ID	Included in modules	Knowledge ID	Included in modules
T1983	1, 2, 3, 4, 5, 6	S0913	3, 6	K1261	1, 2, 3, 4, 5, 6
T1974	5, 6	S0910	-	K1258	1, 2, 3, 4, 5, 6
		S0908	-	K1257	1, 2, 4, 5
		S0907	1, 2, 4, 5, 6	K1256	1, 2, 3, 5, 6
		S0896	1, 2, 4, 5, 6	K1249	2, 3, 4
		S0890	1, 2, 3, 4, 5, 6	K1248	2, 4, 6
		S0866	6	K0785	2, 3, 6
		S0854	6	K0784	-
		S0848	2, 3, 4, 5, 6	K0721	2, 3, 4, 5
		S0690	-	K0684	2, 4, 6
		S0540	3	K0683	3, 4, 6
		S0477	3, 5, 6	K0682	2, 3, 4, 6

Figure 22: TKS statement representation in each module

Notably, four TKS statements, despite being part of the initial scope, were ultimately excluded during the course development process: *"Skill in performing cyberintelligence data analysis" (S0910)*, *"Skill in determining the importance of assets" (S0908)*, *"Skill in performing midpoint-collection data analysis" (S0690)*, and *"Knowledge of insider-threat laws and regulations" (K0784)*. This decision was based on the assessment that these particular skills and knowledge areas would introduce a level of depth and complexity beyond what is essential for achieving the course's primary goal of imparting fundamental insider threat awareness to novices. Furthermore, this scoping aimed to prevent cognitive overload, ensuring the material remained accessible and focused for an introductory-level audience.

### Course material

Each module presented in the following will be done so in a subsection dedicated to each specific module. The subsections will be following the naming standard: "Module [enumerator]: [Title]".

For each module, its corresponding section will first present the TKS statements that the module touches upon. Afterwhich the learning material and challenge will be further unpacked. Note, the application of frameworks for each module will be presented in the overview, and subsequent only elaborated upon with relevant examples as opposed to a full breakdown - this is done for the sake of conciseness and enables the paper to focus on the highlights and most valuable insights.

### Learning material

The learning material is written in Markdown. The presentation in the paper will be the compiled versions - this is the version that the participants in our CTF see. The Markdown versions can be seen in the zip archive attached to the project.

The presentation of the learning material in the paper will serve two purposes: 1. It should provide a reasonable representation of the result of our work without necessarily including all the material - see the Appendices for the full version. 2. The presented learning material should demonstrate where and how a framework (see subsection 2.2 or insight from the interviews (see section 5 was utilized. Note, as stated in "Course material at a glance" that it does not mean the users themselves are introduced to the specifics of the frameworks, rather,

the concepts and insights from the framework are permeating the material presented to the user.

## Challenges

Each challenge will be described and explained in its corresponding module. The challenges each have some thought process behind it, which will be elaborated on under each module. In general the idea and desire was to create a good user experience and let the user use the knowledge gained from the learning material in an interactive way, informed by the interview finding training should be relevant, interactive and have a contextual fit (Concept 3: "Behavior changing training hinges on: relevance, interactivity and contextual fit", see section 5). The challenges are created using the design principles mentioned in subsection 3.3, gamification mentioned in subsection 3.1, with the added capabilities of using the Campfire platform, from subsection 3.4.3, and using the CTF format explained in the section 3. These criteria and an increasing difficulty, should help facilitate the potential for flow from Figure 6. Each challenge was created in HTML with CSS, and with JS(JavaScript) for additional functionality. The exception being the challenge in module 6. Each module follows some patterns of having a blue header bar in the top section containing "Skybound Technologies", "Home" and "Challenge Overview". The Home redirects the user to the index.html and is where the user will first arrive. While the Challenge Overview is where the redirection to challenges are contained, a page containing a link to each html.

## 6.1 Module 1: Insider Threat Awareness Quiz

Module 1 is designed to lay out the conceptual groundwork; it provides the definition of insider threats, demonstrates the rudimentary difference between intentional and unintentional insider threats, and touches on common behavioral and technical indicators. The module ends with a quiz designed to allow the user to practice differentiating between intentional and unintentional insiders while being informed of common insider scenarios.

The module touches on the following frameworks as demonstrated in Table 6.

Framework	Inclusion status for current module	Notes on status for inclusion
<i>NICE Workforce Framework for Cybersecurity</i>	✓	The module touches on several TKS statements
<i>CISA Insider Threat Mitigation Guide</i>	✓	The learning material draws on the definitions provided by the Guide
<i>Critical Pathway to Insider Risk</i>	✓	The characters designed, all exemplify early phases of CPIR
<i>MITRE Insider Threat TTP KB v2.0</i>	-	No TTP's were introduced in a meaningful way in module 1

Table 6: Frameworks inclusions status, module 1

As shown above, module 1 touches on key TKS statements from the NICE Workforce Framework for Cybersecurity. The main focus for module 1 is to provide the user with knowledge and skills that make them ready to start engaging with the task: "*Identify potential insider threats*" (*T1983*). Figure 23 shows the TKS statements that Module 1 aims to address. The full list of in-scope TKS statements for the course can be seen in Table 1 in subsection 4.2.1 where a short descriptive text expands on the contents of each statement. Figure 22 shows the TKS statements actually implemented in the course.



Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
T1983	Identify potential insider threats	S0907	Skill in identifying insider threats	K1261	Knowledge of known insider attacks
		S0896	Skill in recognizing behavioral patterns	K1258	Knowledge of insider threat tactics
		S0890	Skill in performing threat analysis	K1257	Knowledge of insider threat policies and procedures
				K1256	Knowledge of insider threat operational indicators

Figure 23: Module 1. TKS Statements

A more granular demonstration of how each of these TKS statements are covered in module 1 will be presented in both the following learning material and challenge sections.

### Learning material

In the learning material for module 1, the user is introduced to Skybound Technologies, a mid-sized software company that will serve as the running narrative throughout the course. A narrative is utilized as a gamification element which can potentially help increase motivation, engagement, and user experience [23]. Included in the narrative is a set of distinct characters which likewise are introduced: **Dana** the over-stretched IT manager, **Carl** the resourceful but convenience-seeking systems administrator, **Lori** the hurried HR assistant, and **Jordan** the disgruntled employee. All characters are present and used consistently throughout the course, from start to finish, further the character archetypes and their narratives were designed to reflect the interview finding that insider risk is a combination of both motivation and opportunity (Concept 1: "Insider risk = motivation + opportunity phenomenon", see section 5). For instance, Jordan's disgruntlement provides a plausible motivation, while Carl's system administrator role provides opportunity. Emphasizing a running narrative and relatable characters within Skybound Technologies, was deliberately chosen to enhance relevance and contextual fit, key elements for effective security training as highlighted in our expert interview (Concept 3: "Behavior changing training hinges on: relevance, interactivity and contextual fit", see section 5).

After the introduction of the narrative, the learning material proceeds by presenting the theoretical elements. The material then defines "insider" and "insider threat" using CISA definitions. It clearly distinguishes between intentional and unintentional insider threats with illustrative examples (e.g., a disgruntled admin stealing data, an HR assistant accidentally emailing confidential information). Further, the material briefly touches upon the real-world impact (financial, reputational, operational) of such threats and links the key characters' behaviors or situations to these potential risks. Finally, it sets up the subsequent challenge (the quiz) as a way to apply what the learning material goes through.

In Figure 24 is shown a snippet of the theory presented. In an attempt to pursue conciseness, when presenting the following modules they will not contain an image of the learning material, as the layout follow the same

structure for all of them.

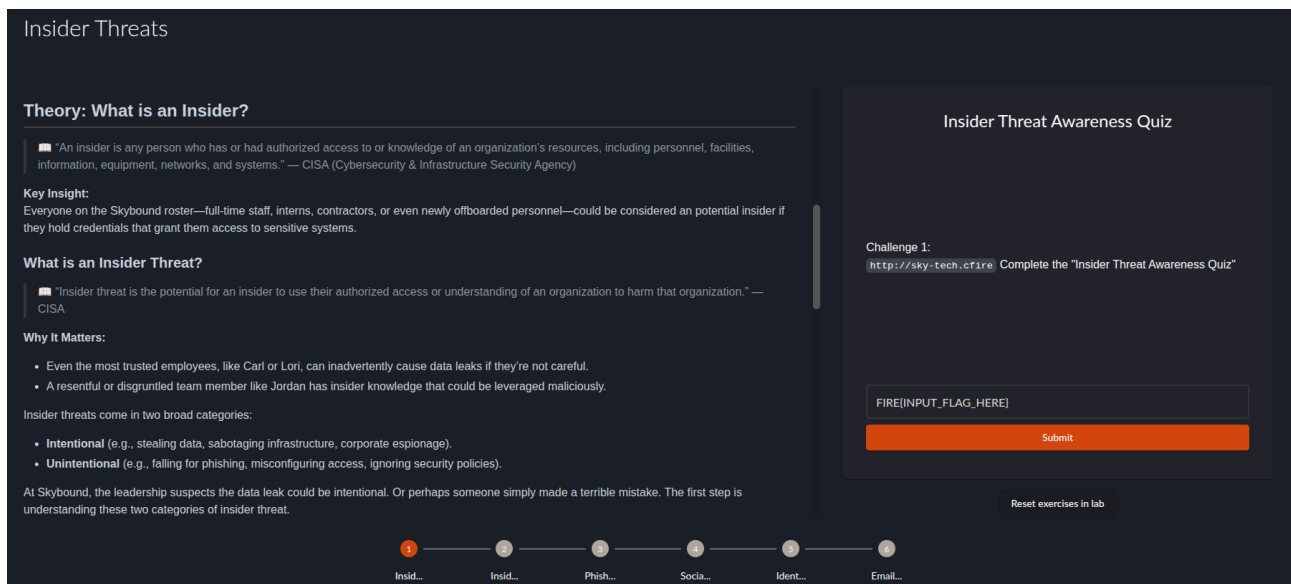


Figure 24: A snippet of some of the theory in Module 1.

#### *Alignment with NICE Workforce Framework for Cybersecurity*

The learning material introduces several NICE Framework Knowledge statements (K-statements) through its narrative and examples. For instance, it presents scenarios like a system admin copying a client database or an HR assistant mistakenly emailing a confidential spreadsheet, which directly illustrate *"Knowledge of known insider attacks"* (K1261). The distinction between intentional and unintentional actions, along with character motivations such as Jordan's disgruntlement or Carl's policy bending, aligns with *"Knowledge of insider threat tactics"* (K1258). Furthermore, descriptions of "odd after-hours database access", files surfacing at a competitor, Carl's late-night sessions, Jordan leaving late, and Lori's accidental document sharing aim to provide knowledge of *"insider threat operational indicators"* (K1256). While not detailing specific policies, the material underscores their importance by mentioning security protocols, characters' policy deviations, and by providing a resource link to CISA's mitigation guidance, thereby touching upon *"Knowledge of insider threat policies and procedures"* (K1257).

#### *Alignment with CISA Insider Threat Mitigation Guide*

As stated above, the definitions provided in the module are verbatim from the Guide, and the influence of said guide is evident in the learning material. The inclusion of real world impacts like financial, reputational, and operational also is inspired by CISA's emphasis on the comprehensive damage from such threats.

#### *Alignment with Critical Pathway to Insider Risk*

Lastly, the direct link provided to the Guide further solidifies its role as a foundational source. Regarding CPIR, the characters introduced in the narrative all exemplify elements from the framework. See Table 7 for a mapping of the characters to the relevant pathway stage.

Pathway stage	How it is represented in the story
<i>Personal predisposition</i>	Low morale after a missed promotion (Jordan)
<i>Stressors</i>	Over-work (Dana), anxiety after mistakes (Lori)
<i>Concerning behaviors</i>	Late-night system access (Carl), accidental data sharing (Lori), open resentment (Jordan)

Table 7: Mapping characters to Critical Pathway to Insider Risk

## Challenge

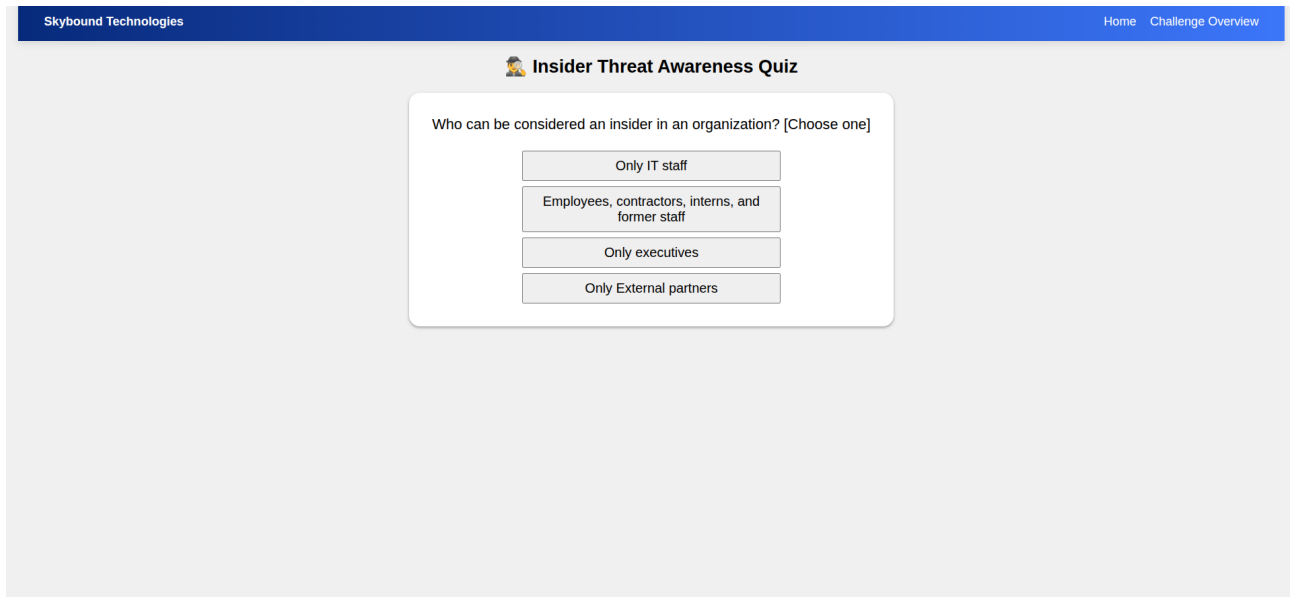
The user is introduced to the concept of insider threats through the learning material in module 1. This challenge is intended to let the user apply the information interactively by answering a short quiz.

### *Alignment with NICE Workforce Framework for Cybersecurity*

There was created 3 questions for this quiz, which combined with the learning material allows the users to practice three skill as per the TKS nomenclature, namely "*Skill in identifying insider threats*" (S0907), "*Skill in recognizing behavioral patterns*" (S0896), "*Skill in performing threat analysis*" (S0890).

### *Description of the challenge*

The layout of the challenge 1 quiz can be seen in Figure 25.



The screenshot shows a web interface for a quiz. At the top is a blue header bar with 'Skybound Technologies' on the left and 'Home Challenge Overview' on the right. Below the header, the title 'Insider Threat Awareness Quiz' is displayed with a detective emoji. The main content area contains a question: 'Who can be considered an insider in an organization? [Choose one]'. Below the question are four buttons: 'Only IT staff', 'Employees, contractors, interns, and former staff', 'Only executives', and 'Only External partners'.

Figure 25: The first task in the first challenge.

Below the header bar, is the challenge's name, "Insider Threat Awareness Quiz", accompanied by an emoji resembling a detective. Beneath the text and the emoji is a white box. The white box contains the current question's text, followed by 4 buttons displaying the different choices available for the user to answer. The buttons have some visual cues, like changing the cursor to a hand, and the color of the button changes slightly, when the cursor hovers the button. When the user clicks one of buttons or options, some feedback will be shown beneath the buttons. The feedback text is either displayed in red, for incorrect, or in green if correct. The

colors work as a visual cue, and is used by many applications and systems, associating, which helps provide clear feedback. If the user clicks a wrong answer the user will have to try again, until the correct answer is picked. When the correct option is pressed, a "Next Question" appears below the feedback. After the 3 questions are answered, clicking the "Next Question" button, will present the flag, which can be seen in Figure 26.

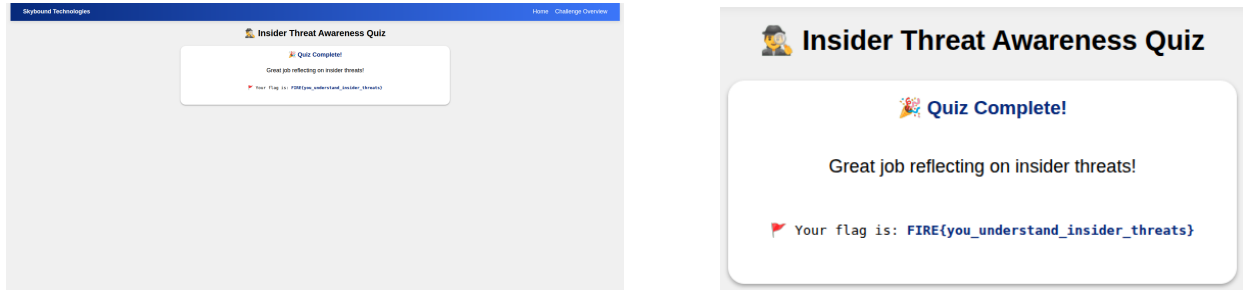


Figure 26: The full page is shown on the left, while the cropped section on the right displays how the flag is presented.

## 6.2 Module 2: Insider Threat Types Quiz

Module 2 builds directly on the foundations laid in Module 1. Where the first module established what an insider threat is, Module 2 sharpens the user's ability to diagnose why a specific act occurred by drilling into the intentional vs. unintentional distinction. It continues the narrative of Skybound Technologies, using the established characters to frame the importance of discerning motive. The learning material is relatively short for module 2, and the technical complexity of the questions posed in the challenge is increased.

The module touches on the following frameworks as demonstrated in Table 8.

Framework	Inclusion status for current module	Notes on status for inclusion
<i>NICE Workforce Framework for Cybersecurity</i>	✓	Overlap with previous module and addition of new TKS statements
<i>CISA Insider Threat Mitigation Guide</i>	✓	The learning material draws on the definitions provided by the Guide
<i>Critical Pathway to Insider Risk</i>	✓	The examples used in the quiz are all implicitly on the CPIR axis.
<i>MITRE Insider Threat TTP KB v2.0</i>	✓	The examples used in the quiz mimic actual TTP's seen in MITRE's catalog

Table 8: Frameworks inclusions status, module 2

The main focus for module 2 is to provide the user with knowledge and skills that makes them able to engage with the task: *"Identify potential insider threats" (T1983)*. Figure 27 shows the TKS statements that Module 2 aims to address. The full list of in-scope TKS statements for the course can be seen in Table 1 in subsection 4.2.1 where a short descriptive text expands on the contents of each statement. Figure 22 shows the TKS statements actually implemented in the course.

Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
T1983	Identify potential insider threats	S0907	Skill in identifying insider threats	K1261	Knowledge of known insider attacks
		S0896	Skill in recognizing behavioral patterns	K1258	Knowledge of insider threat tactics
		S0890	Skill in performing threat analysis	K1257	Knowledge of insider threat policies and procedures
		S0848	Skill in performing behavioral analysis	K1256	Knowledge of insider threat operational indicators
				K1249	Knowledge of digital and physical security vulnerability remediation principles and practices
				K1248	Knowledge of digital and physical security vulnerabilities
				K0785	Knowledge of insider threat tools and techniques
				K0721	Knowledge of risk management principles and practices
				K0684	Knowledge of cybersecurity threat characteristics
				K0682	Knowledge of cybersecurity threats

Figure 27: Module 2. TKS Statements

A more granular demonstration of how each of these TKS statements are covered in module 2 will be presented in both the following learning material and challenge sections.

### Learning material

The learning material for Module 2 directly builds on the scenario at Skybound Technologies, where Dana (IT Manager) is investigating whether a data leak was deliberate or accidental. It reiterates the suspicious situations involving Carl, Lori, and Jordan. The core of the material defines intentional and unintentional insider threats, providing an example for each and linking them back to the Skybound characters. It also briefly discusses why this distinction is vital for tailoring defenses and maintaining a healthy organizational culture.

#### *Alignment with NICE Workforce Framework for Cybersecurity*

The learning material for Module 2 continues to reinforce several NICE Framework Knowledge (K) statements previously introduced and subtly brings in new dimensions. The definitions and examples of intentional and

unintentional insider threats enhance the understanding of *"known insider attacks"* (K1261) and *"insider threat tactics"* (K1258) by adding the layer of intent. The Skybound context, where Carl's after-hours access, Lori's accidental document forwarding, and Jordan's disagreeable behavior are contemplated, which further contextualizes *"insider threat operational indicators"* (K1256). Doing so provides the user insight into *"insider threat tools and techniques"* (K0785) and a high-level introduction to *"cybersecurity threat characteristics" & "threats"* (K0684, K0682). The discussion on tailoring defenses based on threat type implicitly relates to *"knowledge of insider threat policies and procedures"* (K1257) and *"risk management principles and practices"* (K0721), as understanding intent is crucial for appropriate risk mitigation strategies. The material's emphasis on discerning motive also touches upon the foundational knowledge for recognizing behavioral patterns the skill *"recognizing behavioral patterns"* (S0896) and knowledge of not only *"digital and physical security vulnerabilities"* (K1248) but also the *"digital and physical security vulnerability remediation principles and practices"* (K1249).

#### *Alignment with CISA Insider Threat Mitigation Guide*

The learning material continues to align with the CISA Insider Threat Mitigation Guide by focusing on the fundamental CISA-supported distinction between intentional and unintentional insider threats. The provided definitions and examples for both categories directly reflect CISA's conceptualizations. The learning material section "Why This Matters" discusses tailored defenses and cultural impact, which are key considerations in CISA's broader guidance on establishing an insider threat program. This reinforces for novices the practical implications derived from an authoritative source.

#### *Alignment with Critical Pathway to Insider Risk*

CPIR lens applied as in Module 1 in the learning material, see Table 7 for mapping of characters to the CPIR framework. The challenge section for Module 2 demonstrates how CPIR was applied to the scenarios.

### **Challenge**

#### *Alignment with NICE Workforce Framework for Cybersecurity*

The challenge quizzes in Module 2 requires the user to *"Identify potential insider threats"* (T1983) by distinguishing between intentional and unintentional. This directly tests their comprehension of *"insider threat tactics"* (K1258) and *"insider threat operational indicators"* (K1256). Moreover, the user gets to practice; *"identifying insider threats"* (S0907), *"recognizing behavioral patterns"* (S0896), *"performing threat analysis"* (S0890) and *"performing behavioral analysis"* (S0848) by having to actively decide on the the distinction between intentional and unintentional illustrated by the realistic scenarios.

#### *Alignment with Critical Pathway to Insider Risk*

The quiz scenarios in Module 2 reflect different points along the CPIR, even if not explicitly stated. Each of the scenarios seek to include as a minimum a stressor and a concerning behavior, see a mapping of scenario 1 in Table 9. The addition of more examples which map to CPIR, can help the user relate to how personal situations and stressors are key components in the manifestation of different types of insider threats.

Pathway stage	How it is represented in scenario 1
<i>Personal predisposition</i>	Scenario 1: No predisposition involved
<i>Stressors</i>	Scenario 1: "feeling unfairly passed over for promotion"
<i>Concerning behaviors</i>	Scenario 1: "secretly copies proprietary design files"

Table 9: Mapping scenario 1 to Critical Pathway to Insider Risk

*Alignment with MITRE Insider Threat TTP KB v2.0*

Module 2 does not explicitly state MITRE or "TTP", however the scenarios embody simplified versions of actual TTPs. Without touching on all the scenarios nor all TTPs, some of the TTPs in scenario 1 will be used as an example of the use of the framework.

Scenario 1 is: "An employee, feeling unfairly passed over for promotion, secretly copies proprietary design files onto a USB drive. He then contacts a competitor, seeking a better offer.". In this scenario the employee uses implicit trust to get access, eg. Tactic: *TA0001: Initial Access* and Technique: *T1199: Trusted Relationship*. Further, his mean of exfiltrating the data maps to Tactic: *TA0010: Exfiltration* and Technique: *T1052.001: Exfiltration over USB* and potentially Tactic: *TA0009: Collection* and a subsequent range of Techniques like *T1005: Data from Local System*, *T1119: Automated Collection*, etc. See Figure 3 or Appendix A.2 for the "green-seen" chart listing the known TTPs of insider threats.

*Description of the challenge*

This challenge layout can be seen in Figure 28. After the header bar is the module's challenge name presented, "Insider Threat Types Quiz", with an emoji with a monocle. Just beneath the header text, is a white box with text explaining the main concept of this challenge. Below it is another white box containing the scenarios number, followed by the scenario text, and underneath two buttons with "intentional" and "unintentional".

Figure 28: This is how the second challenge would be presented to the user. This is the first task.

The user will be given a total of 5 scenarios and determine whether it would be considered an intentional or an unintentional insider threat, in regards to the learning material presented. If correct, the feedback text for the scenario will, again, be presented in a green color, but now also with a green check mark. If incorrect, in red, and with a red cross(as seen in Figure 29). If correct a "Next Scenario" button appears beneath the feedback, allowing the user to proceed to the next scenario. If incorrect, the user must attempt again until the correct option is selected. After the 5 scenarios are completed, the user is presented with the flag. The flag is presented similarly to how challenge 1 does, (see Figure 26 for reference) The flag and text are just different.

Figure 29: The feedback from the first scenario.

### 6.3 Module 3: Is This a Phishing Email... ?

Module 3 pivots from “who?” (Module 1) and “why?” (Module 2) to the very practical “how does the threat often start?” — through social engineering but specifically phishing. These types of attacks are a prime example of how trust can be exploited, a theme that emerged as significant in our expert interviews (section 5) concerning the modern threat landscape (Concept 4: "Trust culture and emerging technologies create a double-edged landscape", see section 5).

The users are asked in the challenge to step into Skybound’s help desk queue, inspecting seven quarantined messages and deciding **Phish** or **Legit**. The theory page is much richer than in Module 2, covering e-mail anatomy, red-flag checklists, and good security hygiene, while the challenge ramps up technical realism with embedded HTML e-mails and live markup of each indicator.

The module touches on the following frameworks as demonstrated in Table 10.

Framework	Inclusion status for current module	Notes on status for inclusion
NICE Workforce Framework for Cybersecurity	✓	Extends and overlaps with previous modules
CISA Insider Threat Mitigation Guide	-	While the module draws heavily on CISA, it is specifically not the Guide being used
Critical Pathway to Insider Risk	-	No apparent implicit or explicit use
MITRE Insider Threat TTP KB v2.0	✓	The emails generated for the help desk mimic specific TTPs

Table 10: Frameworks inclusions status, module 3

The main focus for module 3 is to provide the user with knowledge and skills that makes them able to engage with the task: *"Identify potential insider threats" (T1983)*, specifically related to phishing vectors. Figure 30 shows the TKS statements that Module 3 aims to address. The full list of in-scope TKS statements for the



course can be seen in Table 1 in subsection 4.2.1 where a short descriptive text expands on the contents of each statement. Figure 22 shows the TKS statements actually implemented in the course.

Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
<b>T1983</b>	<i>Identify potential insider threats</i>	<b>S0913</b>	<i>Skill in performing link analysis</i>	<b>K1261</b>	<i>Knowledge of known insider attacks</i>
		<b>S0890</b>	<i>Skill in performing threat analysis</i>	<b>K1258</b>	<i>Knowledge of insider threat tactics</i>
		<b>S0848</b>	<i>Skill in performing behavioral analysis</i>	<b>K1256</b>	<i>Knowledge of insider threat operational indicators</i>
		<b>S0540</b>	<i>Skill in identifying network threats</i>	<b>K1249</b>	<i>Knowledge of digital and physical security vulnerability remediation principles and practices</i>
		<b>S0477</b>	<i>Skill in identifying anomalous activity</i>	<b>K0785</b>	<i>Knowledge of insider threat tools and techniques</i>
				<b>K0721</b>	<i>Knowledge of risk management principles and practices</i>
				<b>K0683</b>	<i>Knowledge of cybersecurity vulnerabilities</i>
				<b>K0682</b>	<i>Knowledge of cybersecurity threats</i>

Figure 30: Module 3. TKS Statements

A more granular demonstration of how each of these TKS statements are covered in module 3 will be presented in both the following learning material and challenge sections.

### Learning material

The learning material for Module 3, titled "Phishing & Personal Security Habits" (step3.md), prepares the learner for a practical challenge by first explaining the fundamental components of an email and how they can be manipulated. It then defines phishing and lists common types. A key section, "The Anatomy of a Phishing Email" - provides a detailed table (visualized as an image) of email elements to inspect and typical phishing clues. This is followed by an example phishing email for learners to analyze. The material offers a "Handy Red Flag Checklist" and a section on "Personal Security Habits," such as MFA and strong passwords, presented visually.

### Alignment with NICE Workforce Framework for Cybersecurity

The learning material significantly contributes to several NICE Framework K-statements. The detailed breakdown of email anatomy, phishing types, and indicators directly imparts "*Knowledge of cybersecurity threats*" (K0682), "*Knowledge of cybersecurity vulnerabilities*" (K0683) and "*Knowledge of insider threat tactics*" (K1258)

by explaining how emails can be exploited. The "Anatomy of a Phishing Email" section and the "Red Flag Checklist" provide learners with *"Knowledge of insider threat operational indicators" (K1256)*, specifically how these indicators manifest in phishing attempts. Understanding these indicators is a form of *"Knowledge of known insider attacks" (K1261)*, as phishing is a prevalent attack vector. The "Personal Security Habits" section promotes *"Knowledge of digital and physical security vulnerability remediation principles and practices" (K1249)* and *"Knowledge of risk management principles and practices" (K0721)* by suggesting MFA and strong passwords as preventative measures.

## Challenge

The concept for this challenge is to have the user review emails and determine whether they are legitimate or a phishing attempt. The user is tasked with finding and identifying indicators that suggest the email may be phishing, which are covered in the learning material.

### *Alignment with NICE Workforce Framework for Cybersecurity*

The challenge for Module 3, is a direct application and reinforcement of a range of TKS statements. Users inspect seven HTML emails and decide if they are "Phish" or "Legit". This activity develops *"Skill in identifying network threats" (S0540)* – in this case, threats via email - and *"Skill in identifying anomalous activity" (S0477)* along side *"Skill in performing behavioral analysis" (S0848)* by spotting deviations from legitimate email characteristics. Mismatched sender domains, urgent subject lines, malicious links, or suspicious attachments hones the *"Skill in performing link analysis" (S0913)* and general *"Skill in performing threat analysis" (S0890)* while testing *"Knowledge of insider threat tools and techniques" (K0785)*.

### *Alignment with MITRE Insider Threat TTP KB v2.0*

The phishing emails presented in the challenge effectively simulate various MITRE ATT&CK TTPs for phishing, these are however not in scope for the Insider Threat TTP KB. Rather, the use of phishing is done typically by actors outside the organization wishing to perhaps create an unintentional insider scenario. The use of phishing align with Tactic: *TA0043: Reconnaissance* and Technique: *T1589: Gather Victim Identity Information* and if succesully compromising an account, the attacker has gained *TA0003: Persistence* and *TA0005: Defense Evasion* via *T1078: Valid Accounts*. See Figure 3 or Appendix A.2 for the "green-seen" chart listing the known TTPs of insider threats.

### *Description of the challenge*

#### Emails

To begin with, some lookalike emails were created, for the user to review. The emails were designed to resemble a typically representation of an email. The emails should also provide the freedom to change, edit and modify the content, and also enable some interactivity.

The emails were also created with HTML, CSS and JS. This allowed a freedom to change, edit and modify the content, whie still keeping a template and enabling some interactivity. The HTML Page is shown in Figure 31. These emails generally contain 5 main fields or components: **From**, **To**, **CC**, **Subject**, and **Text Body**. However

one of the emails also included an **Attachment field**, making a sixth component in that particular case, which is displayed beneath CC and above the Subject<sup>10</sup>. These 6 components are some of the key elements that the user will look at when determining whether it is phishing or legitimate.

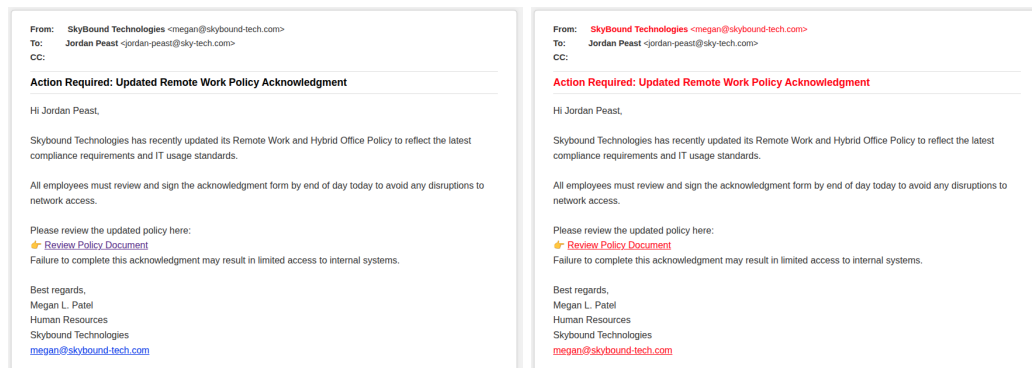


Figure 31: The left image is one of the 7 emails used. While the right image is the same image but showing the indications).

The information the user has is from the learning material includes the persons Dana, Lori, Carl and Jordan, and the email domain for Skybound Technologies, which is "sky-tech.com". The persons were included in the emails, to keep the narrative relevant. In every email one of their names appears.

In the left image of Figure 31, is the senders email (the **From** field), which is one of the indicators that this email is phishing. The right image in Figure 31, presents how it is visually shown to the user, by changing the specific indicators text to be in a red color and the font to be bold. This functionality is done by the use of JS.

## The User Interface

The first step was to provide the user with some emails to review. The next step was to design and implement a user interface to support the necessary interactions needed. The layout should include, a visual and interactive representation of the html email lookalike, having the choices "phishing" and "legit" connected to the changing html email, and lastly overview of the current objective. The resulting layout is shown in in Figure 32. Beginning just below the header bar, the name of the challenge, "Is This a Phishing Email... ?"

<sup>10</sup>This can be found in Appendix A.10 Figure 64 for a visual clarification.

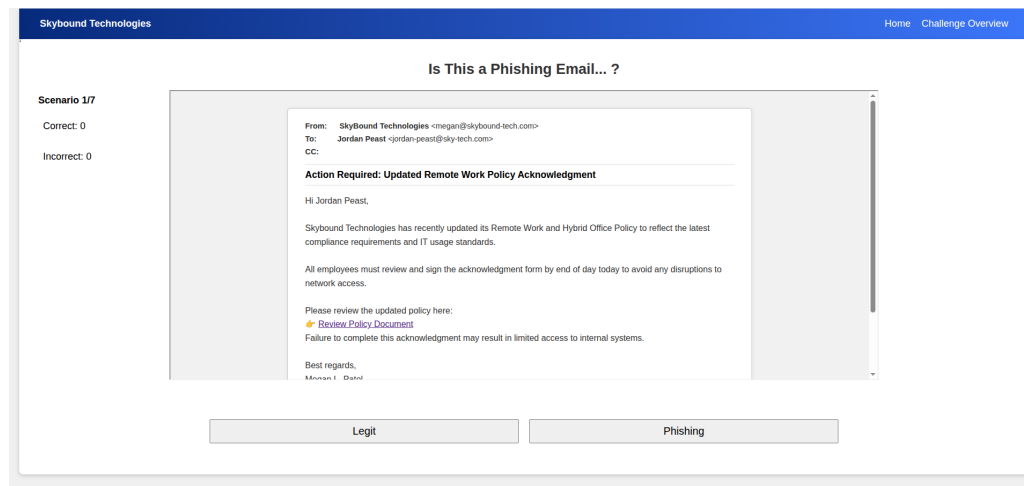


Figure 32: This is how the third challenge would be presented to the user. This is the first task, which contains the email from Figure 31.

The representation of the html email as seen in Figure 32 has a deliberate size constraint to enable scroll bars. If the content exceeds the area, both vertical and horizontal scroll bars appear. Both the vertical and horizontal scroll bars are expected and deliberate. The area's height constraint is to ensure the layout fits within a single visual frame. While the vertical scroll bar, is always present<sup>11</sup>. This width constraint also ensures the html email will be displayed as intended, and would help to keep consistency between the different emails. The vertical scroll bar also serve the purpose of indicating there is some interactivity with the email. By providing a visual cue, the scroll bar, the user would know that some additional content is hidden and it can be viewed if scrolled. The desire was this interaction would encourage further exploration of the email, particularly the links. The links in the email are interactive, which is suggested by the visual cue of it being blue, while the plain text is black. This is a common practice across systems, which hopefully would drive the user to interact with it. If the user interacts with the link, by simply hovering it with the cursor, it would change to a hand, providing visual feedback of it being interactive. The choice of having the vertical scroll bar should help guide the user of it's interactive nature, and was desired to indicate that the email was not simply a static picture. Since the links are also used as "indicators", as seen in Figure 31, Where the link would redirect the user to "MaliciousSite". This would be identified by hovering the link or right clicking and inspect the link.

The "MaliciousSite" was created, to allow redirection if clicked, it can be seen in Appendix A.11.

In the left side of the user interface is the overview of the objective, as seen in Figure 32. The "Scenario 1/7" represent the current scenario, 1, out of a total of 7. While the "Correct" and "Incorrect" tracks the amount of right and wrongs. This also serves as feedback, allowing them to track their progress, while also providing an overview of the duration of the challenge.

The "legit" and "phishing" buttons in Figure 32 is the options the user has to decide upon in each scenario.

<sup>11</sup>However if the viewport height reaches approximately 1200 pixels or more, it may no longer appear.

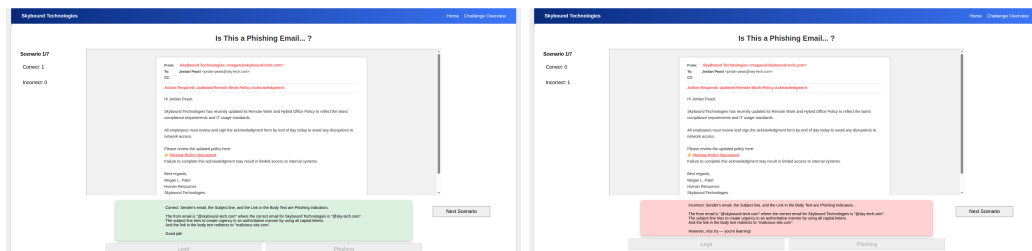


Figure 33: The Feedback from choosing either correctly(Left image) or incorrectly(Right image).

Once the user selects either of the two, feedback is presented, As shown in Figure 33. The feedback will again appear either in a green box if correct, or a red box if incorrect.

The text is similar, explaining each phishing indicator but differ in few ways. For instance if correct the feedback starts with "Correct:" and could end with a "good job!". While if incorrect it would start with "Incorrect:" and could end with "However nice try – you're learning!".

When the feedback is presented for a phishing email the specific phishing indicators, also mentioned in the feedback text, are visually highlighted red and bold as seen in Figure 31 and Figure 33. While a non-phishing emails changes nothing.

This visual feedback indicating what was the phishing indicators was using JS. It helps provide clear reference, feedback and unambiguous information to the user to understand, what exactly the feedback is addressing in the email. Which was specially considered to encompass the criteria of feedback in both flow and gamification. Even if the feedback text would be more extensive, compared to previous challenges, this was decided upon to provide a clear full view of each indicator every time, to leave nothing unsaid and provide clear unambiguous feedback. If the email is legitimate, the feedback will be short - "There should not be any indicators this was phishing" and nothing would be highlighted in the email. Clicking both "Legit" or "Phishing" reveals the corresponding feedback, but also a small button on the right side - the "Next Scenario" button. This button will let the user proceed to the next email. When the button is clicked the layout is "reset", and the next email is shown, until the last has been reviewed and completed. When the last email is reviewed, the final page is presented. The final page contains the course's logo where the email usually was, and a celebratory text above it, containing their final outcome - "Thanks for your help! You got x out of 7 correct, good work!", where x is the total correctly answered. While the flag is presented where the feedback usually is, but with a gray background.

That concludes the 3rd challenges layout and how it functionalities. Some additional thoughts went into the challenge. The "Next Scenario" button appears when both incorrect and correct, the reasoning is there are only 2 choices, and the feedback is similar, this enables a tracking of incorrect and correct answers. Which could give incentive to an additional goal or objective of completing as many scenarios correctly. Having the user click the correct answer afterwards would create a redundant step which serves no use, so removing it should increase user friendliness. This messes a bit with the consistency from the previous challenges. But includes another gamification element, another use of "points", that are not related to the campfire platform(see subsection 3.4.3). As mentioned it also helps by providing the user with an overview of the challenges magnitude and their current performance in the challenge.

## 6.4 Module 4: I Didn't Mean to Let Them In

Module 4 continues from where Module 3 left of with the perspective of “how does the threat often start?” — this time focused more intently on social engineering. In the five scenarios used in the challenge the user is asked for the correct course of action in distinct social engineering situations. The theory in the learning material is again relatively light, introducing the psychological buttons that social engineers use to achieve their objectives.

The module touches on the following frameworks as demonstrated in Table 11.

Framework	Inclusion status for current module	Notes on status for inclusion
<i>NICE Workforce Framework for Cybersecurity</i>	✓	Extends and overlaps with previous modules
<i>CISA Insider Threat Mitigation Guide</i>	-	While the module draws heavily on CISA, it is specifically not the Guide being used
<i>Critical Pathway to Insider Risk</i>	-	No apparent implicit or explicit use
<i>MITRE Insider Threat TTP KB v2.0</i>	✓	Challenge scenarios model specific TTPs

Table 11: Frameworks inclusions status, module 4

Still for module 4, the primary competency remains *"Identify potential insider threats" (T1983)*, now broadened from digital phishing to blending physical and cyber vectors. Figure 30 shows the TKS statements that Module 4 aims to address. The full list of in-scope TKS statements for the course can be seen in Table 1 in subsection 4.2.1 where a short descriptive text expands on the contents of each statement. Figure 22 shows the TKS statements actually implemented in the course.

Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
T1983	Identify potential insider threats	S0907	Skill in identifying insider threats	K1261	Knowledge of known insider attacks
		S0896	Skill in recognizing behavioral patterns	K1258	Knowledge of insider threat tactics
		S0890	Skill in performing threat analysis	K1257	Knowledge of insider threat policies and procedures
		S0848	Skill in performing behavioral analysis	K1249	Knowledge of digital and physical security vulnerability remediation principles and practices
				K1248	Knowledge of digital and physical security vulnerabilities
				K0721	Knowledge of risk management principles and practices
				K0684	Knowledge of cybersecurity threat characteristics
				K0683	Knowledge of cybersecurity vulnerabilities
				K0682	Knowledge of cybersecurity threats

Figure 34: Module 4. TKS Statements

A more granular demonstration of how each of these TKS statements are covered in module 4 will be presented in both the following learning material and challenge sections.

### Learning material

The learning material for Module 4 begins by framing social engineering as "hacking people". It introduces key psychological triggers attackers leverage, and outlines key social engineering tactics like: Pretexting, Tailgating, Phone Scams, Casual Oversharing, ect., each with an example. Following this, it presents protective habits under "Protecting Against Manipulation," such as challenging unfamiliar faces and verifying callers, again with a visual aid.

#### *Alignment with NICE Workforce Framework for Cybersecurity*

The learning material for Module 4 significantly reinforces and expands upon several Knowledge statements. By explaining psychological triggers (Authority, Urgency, Familiarity, Scarcity) and tactics like Pretexting, Tailgating, and Vishing, it deepens the "Knowledge of cybersecurity threats" & "threat characteristics" (K0682 & K0684), "Knowledge of digital and physical security vulnerabilities" (K1248) and "Knowledge of cybersecurity vulnerabilities" (K0683), particularly how human behavior can be a vulnerability. The descriptions of these

tactics serve as concrete examples of *"known insider attacks"* (K1261) or methods that facilitate such attacks, often leading to unintentional insider complicity. Understanding these social engineering techniques also directly contributes to *"Knowledge of insider threat tactics"* (K1258) by showcasing how attackers manipulate individuals. The section "Protecting Against Manipulation" offers remediation advice, aligning with *"Knowledge of digital and physical security vulnerability remediation principles and practices"* (K1249) and *"Knowledge of risk management principles and practices"* (K0721).

## Challenge

This challenge is designed to present users with scenarios where they must assess the situation and determine the appropriate course of action. The user will choose between predefined options. The primary goal is to promote critical thinking and reflection on social engineering threats and general security best practices. The aim is to improve users' awareness and decision making when faced with potentially malicious or suspicious situations. While the learning material addresses the theoretical concepts, this challenge is intended to provide an opportunity for users to apply and use the knowledge interactively, developing their skills.

### *Alignment with NICE Workforce Framework for Cybersecurity*

The challenge in Module 3, provides practical application of Skill statements through five distinct scenarios, while underpinning Knowledge statements already introduced. Each scenario requires the user to identify the correct course of action in social engineering scenes, thereby developing their *"Skill in identifying insider threats"* (S0907), *"Skill in recognizing behavioral patterns"* (S0896), *"Skill in performing behavioral analysis"* (S0848) and *"Skill in performing threat analysis"* (S0890) specifically in social engineering contexts. In order to choose the correct course of action in the scenarios, the user will be tested in their knowledge of: *"insider threat tactics"* (K1258), *"digital and physical security vulnerability remediation principles and practices"* (K1249), *"insider threat policies and procedures"* (K1257) and *"cybersecurity threats"* (K0682).

### *Alignment with MITRE Insider Threat TTP KB v2.0*

Much like in Module 3, the social engineering scenarios could more fittingly be mapped to MITRE ATT&CK. With that being said, a successful social engineering campaign can be argued to fall under *TA0042: Resource Development* and *TA0043: Reconnaissance* with the goals of *T1650: Acquire Access* and *T1589: Gather Victim Identity Information*. See Figure 3 or Appendix A.2 for the "green-seen" chart listing the known TTPs of insider threats.

### *Description of the challenge*

First a set of tasks or scenarios were created. A total of 5 tasks or scenarios was created for this challenge. The challenge was created in html, the layout resembles that of the third challenge, for reference see Figure 35. This decision was made to maintain consistency, and also to enable reuse of the structure and html across multiple challenges, with edits made to suit the current challenge's needs.

The layout does differ in some ways from challenge 3. Firstly below the header bar, the text of the current scenario would be displayed. This was the tasks or scenarios mentioned. Secondly instead of emails some



visual graphics would replace the majority of the layout. The visual graphics were created to complement the scenarios, providing the user with something more than just textual content to look at. These visual graphics were images meant to enhance both the experience and the scenarios, therefore they need to be relevant and aligned with the scenario's context, so they do not become a distraction from the task at hand. The images were generated using AI, with each image prompted to match the scenario it accompanies, to ensure the visual directly relates to the scenario. Thirdly instead of 2 options the user would be presented with 3 options to choose between creating more complexity, and choices to choose from.

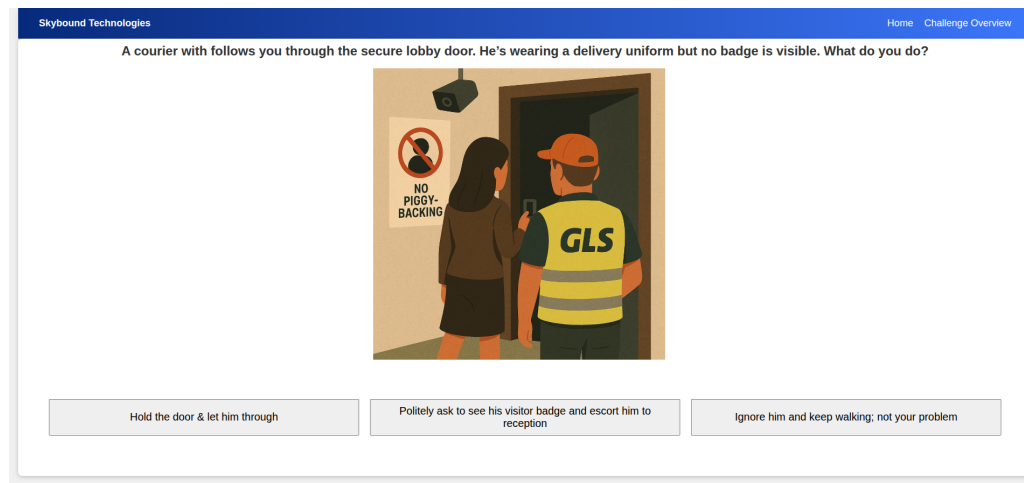


Figure 35: This is how the fourth challenge would be presented to the user. This is the first task.

As seen in Figure 35, the task would be

"A courier with follows you through the secure lobby door. He's wearing a delivery uniform but no badge is visible. What do you do?"

The image underneath correlates to the task, and follows some constraints in the sizing. For example if the browser window gets smaller, so would the image, enabling all the page's content fitting inside a single visual frame. The 3 buttons underneath, contains the different choices the user must decide between. The 3 choices in the example of Figure 35 are:

"Hold the door & let him through"

"Politely ask to see his visitor badge and escort him to reception"

"Ignore him and keep walking; not your problem"

Regardless of the choice being correct or incorrect, feedback is presented in the form of a pop-up, as seen in Figure 36. The feedback follows same pattern of incorrect being associated to red, and correct to green. This is shown in the background color of the pop-up. Additionally if the choice was incorrect, the user must select another option until the correct option is chosen. Once the correct option is selected a "Next Scenario" button appears to the right (as seen in Figure 36). This button prompts a layout reset, and the next scenario to load with related image, and begin. The user would need to pick correctly on each of the 5 scenarios, before they can proceed and get the flag.

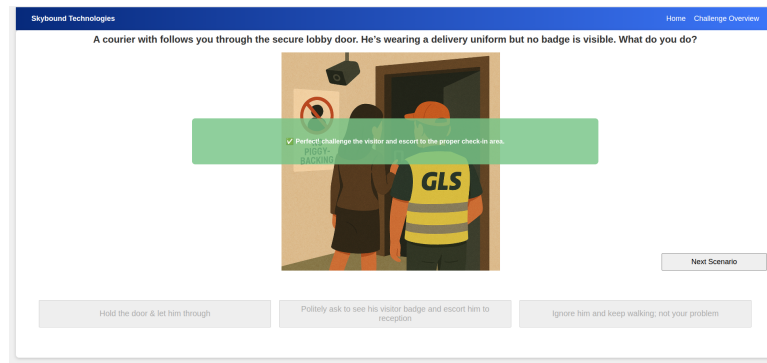


Figure 36: This is the correct feedback prompt from the first task in challenge 4

The feedback is directly addressing the choice made by the user, as seen in Figure 37, where the first feedback correlates to picking "Hold the door & let him through". The second is from picking "Politely ask to see his visitor badge and escort him to reception", and lastly the third is from third option - "Ignore him and keep walking; not your problem".

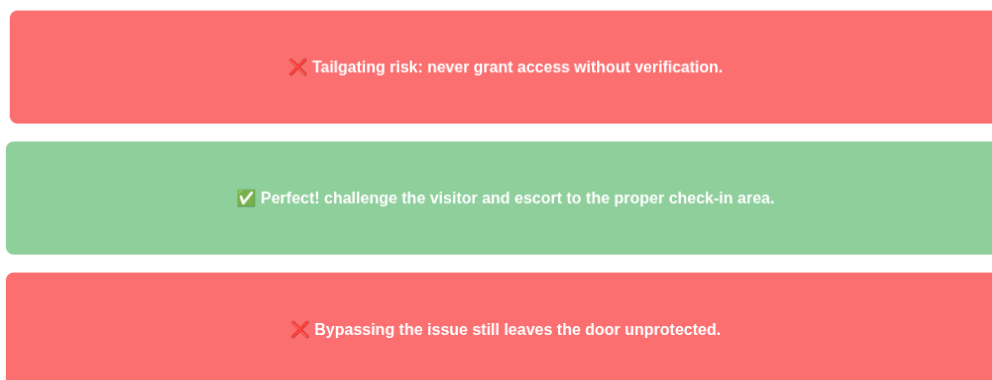


Figure 37: The feedback from top to bottom, represent the options from left to right in Figure 35

The flag is then presented similarly to Challenge 3. The top section's text is now "You had your fun at the door, now lets move on", and the course logo will be displayed beneath and followed by a text field underneath displaying the flag for challenge 4.

## 6.5 Module 5: An Everyday Help Desk, or ?

Having learned "who" (Module 1), "why" (Module 2) and "how does the threat often start?" (Module 3 & 4), the course now turns to the equally practical question "when should we act?". Module 5 aims to equip users with the ability to spot and triage early behavioral and technical warning indicators of an insider threat. The learning material introduces behavioral and technical cues) and walks through Carl, Lori and Jordans recent activities that seem suspicious. In the challenge, users must decide, under time-pressure, whether to **Accept** or **Deny** simulated help desk request. The help desk request are designed to force the user to balance the tension between urgency and due diligence, and highlight how subtle red flags can be missed when cognitive load is high.

The module touches on the following frameworks as demonstrated in Table 12.

Framework	Inclusion status for current module	Notes on status for inclusion
NICE Workforce Framework for Cybersecurity	✓	Continues the focus on T1983 Identify potential insider threats and extends to T1974 Conduct insider-threat risk assessments
CISA Insider Threat Mitigation Guide	✓	Primary source for the behavioral/technical indicator taxonomy used in the theory page
Critical Pathway to Insider Risk	✓	Behavioral indicators (stress, disgruntlement) mapped to pathway stages to contextualize the red flag list
MITRE Insider Threat TTP KB v2.0	✓	Challenge tickets represent concrete TTPs (e.g. unauthorized data staging, privilege escalation)

Table 12: Frameworks inclusions status, module 5

Module 5 deepens the learner's capability to *spot* and *evaluate* insider threat precursors vis à vis "*Identify potential insider threats*" (T1983), but also extends into "*Conduct insider-threat risk assessments*" (T1974). Figure 38 shows the TKS statements that Module 5 aims to address. The full list of in-scope TKS statements for the course can be seen in Table 1 in subsection 4.2.1 where a short descriptive text expands on the contents of each statement. Figure 22 shows the TKS statements actually implemented in the course.

Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
T1983	Identify potential insider threats	S0907	Skill in identifying insider threats	K1261	Knowledge of known insider attacks
T1974	Conduct insider threat risk assessments	S0896	Skill in recognizing behavioral patterns	K1258	Knowledge of insider threat tactics
		S0890	Skill in performing threat analysis	K1257	Knowledge of insider threat policies and procedures
		S0848	Skill in performing behavioral analysis	K1256	Knowledge of insider threat operational indicators
		S0477	Skill in identifying anomalous activity	K0721	Knowledge of risk management principles and practices

Figure 38: Module 5. TKS Statements

A more granular demonstration of how each of these TKS statements are covered in module 5 will be presented in both the following learning material and challenge sections.

### Learning material

The learning material for Module 5 revisits Skybound Technologies and the narrative established in previous modules. Dana (IT Manager) explains and points to the various behavioral and technical indicators for Carl, Lori, and Jordan, whose suspicious activities are recapped. The proverbial meat of the learning material is in fact the segregation of warning indicators into: behavioral (e.g., changes in habits, dissatisfaction) and technical (e.g., abnormal access, large downloads). Beyond introducing the segregation, the material emphasizes why these indicators matter for early intervention, appropriate response, and fostering organizational awareness. This emphasis echoes the interview findings that effective security is an organizational obligation, where individual training contributes to broader governance rituals and a better security culture (Concept 2: "Security is an organizational obligation operationalized through governance rituals", see section 5)

*Alignment with NICE Workforce Framework for Cybersecurity*

It is with Module 5 that the course takes a foray into *"Conduct insider threat risk assessments"* (T1974), while maintaining focus on *"Identify potential insider threats"* (T1983). In the learning material a substantial effort is made to impart K-statements relevant to identifying and assessing insider threats. The detailed descriptions of behavioral and technical indicators directly provide *"Knowledge of insider threat operational indicators"* (K1256). Using the characters as examples of these indicators (eg. discussing Carl's late work and access to sensitive repositories without tickets or Jordan's open dissatisfaction and out of scope system access). This directly supports *"Knowledge of known insider attacks"* (K1261) by illustrating common precursors. The material's distinction between malicious intent and harmless oversights begins to touch upon *"Knowledge of insider threat tactics"* (K1258) and the basics of *"Knowledge of risk management principles and practices"* (K0721). The explicit link to the Guide yet again reinforces *"Knowledge of insider threat policies and procedures"* (K1257).

*Alignment with CISA Insider Threat Mitigation Guide*

Definitions and nomenclature around behavioral and technical indicators are quoted verbatim from the Guide. Furthermore the module links to the Guide for further reading.

*Alignment with Critical Pathway to Insider Risk*

At this juncture no new usage of CPIR is applied. The mapping and use of CPIR happens by way of the characters from the narrative as detailed in Table 7.

*Alignment with MITRE Insider Threat TTP KB v2.0*

The learning material utilizes the phrasing "technical indicators" from the Guide. While not directly mapped to MITRE TTPs, a range of these indicators such as "Abnormal access attempts to high value data or systems" and "Efforts to disable monitoring or security measures" conceptually align with MITRE Insider Threat TTP KB. For instance can "Efforts to disable monitoring or security measures" effortlessly be mapped to a *TA0005: Defense Evasion* Tactic, specifically the Technique: *T1562.001: Disable or Modify Tools*. **Challenge**

The concept for this challenge, is to have the user engage with a simulated help desk interface and **approve** or **deny** a range of requests.

*Alignment with NICE Workforce Framework for Cybersecurity*

The challenge acts as application of several TKS statements in a simulated, time pressured environment. Users must evaluate help desk requests and decide to **"Accept"** or **"Deny"** them based on provided "Help Desk Guidelines" (Least Privilege, Approval for Sensitive Data, Role-Based Access) (*"Knowledge of risk management principles and practices"* (K0721) and *"Knowledge of insider threat policies and procedures"* (K1257)). This activity actively develops *"Skill in identifying insider threats"* (S0907), *"Skill in performing behavioral analysis"* (S0848), *"Skill in identifying anomalous activity"* (S0477), *"Skill in performing threat analysis"* (S0890) and *"Skill in recognizing behavioral patterns"* (S0896) as users must infer if a request is legitimate or a potential policy violation/indicator of risk based on the provided guidelines. For example will scenario 1 ask the user to gauge if

an IT intern should be allowed access to company wide payroll records, a clear violation of established policy.

### *Alignment with CISA Insider Threat Mitigation Guide*

While not explicitly present in the challenge scenarios, some of the behavioral indicators found in the scenarios can be mapped to the Guide. For example can scenario 5 "The head of facilities & operations requests access to Dana's folder named "Pictures" be mapped to the behavioral indicator: *"Unwillingness to comply with established rules, procedures, or organizational policies"* [11, p. 66].

### *Alignment with MITRE Insider Threat TTP KB v2.0*

Much like the associated learning material, the challenge does not explicitly point out TTPs. The scenarios tight coupling with actual TTP elements like using established help desk processes to aid in *TA0004: Privilege Escalation* via for example *T1548: Abuse Elevation Control Mechanism*, is why the MITRE framework is stated as being included in Module 5. While not established in the scenarios, the role of help desk employee and handling tickets makes the user a line of defense against Tactics like *TA0003: Persistence* and *TA0004: Privilege Escalation* when they have to spot the potentially malicious request in the "unending" queue of tickets.

### *Description of the challenge*

This challenge was supposed to be on time. This a new game element used in this challenge, which creates time pressure. To prepare the user before beginning the challenge, a separate introduction page was created.

#### **Intro to Challenge 5.**

This was page was meant as an introduction to the user. As seen in Figure 39 the content does not fit within a single view, this was intentionally to have the introduction appear without a visual cue immediately available to begin the challenge.

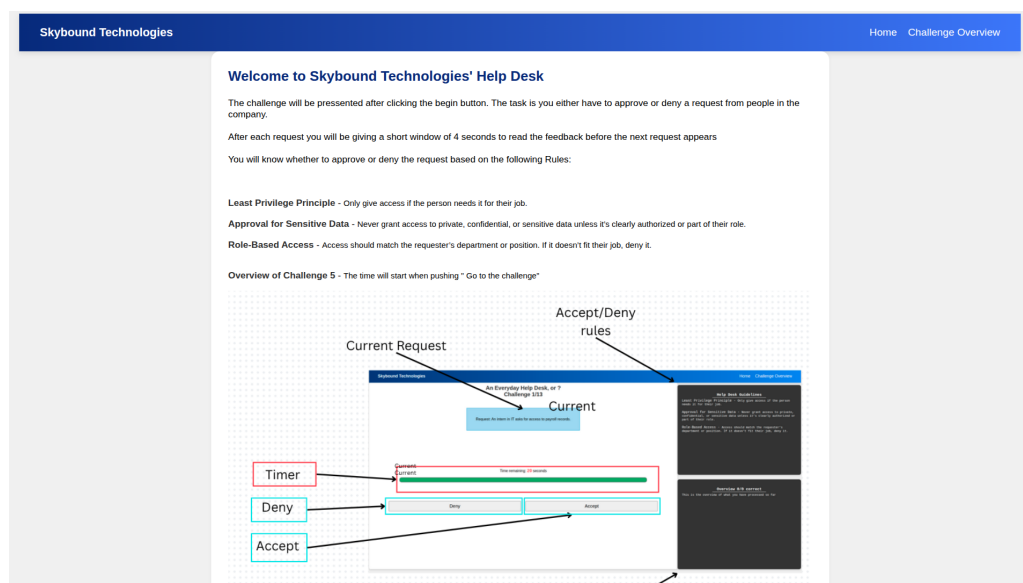


Figure 39: Caption

In the introduction page firstly there is a "Welcome to Skybound Technologies' Help Desk" header with a de-

scription of the upcoming challenge. Explaining that the user will either have to approve or deny requests, after each answer the user will have 4 seconds to review the feedback before the next request appears. Underneath are the rules that facilitates the reason behind why a request should be approved or denied. Beneath this, is an image of the challenge's layout. This image contains an overview with helpful text to give the user a chance to familiarize themselves with the layout, before time begins and they are put on the spot. The user will have to scroll down from the previously mentioned content, to get access to the Button "Go to the challenge", that starts the challenge.

**The help desk interface** The challenge's layout can be seen in Figure 40. It contains the challenge's name in the top, with a 1/11, meaning the first out of 11 requests. This provide the user with an overview of current challenge out of a total 11, providing useful feedback to help keep track of the magnitude of the whole challenge. The blue square underneath this, contains the request text, the current task, which should be approved or denied. The user will have to read and chose one of the buttons beneath. The buttons contains the words Deny and Accept.

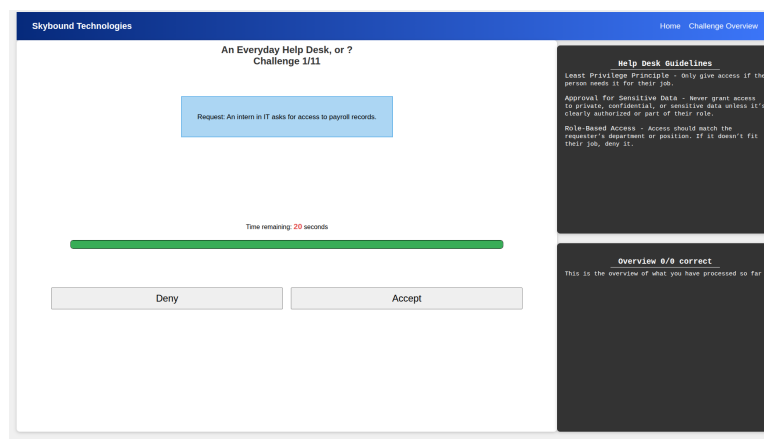


Figure 40: Caption

In the right side are 2 black boxes, the top one containing the rules mentioned earlier in the introduction for challenge 5. While the bottom one contains the handled requests. These handled requests starts with either a green check mark or a red cross, depending on it being correct or incorrect, followed by "Accepted - " or "Denied -". Lastly the handled request's text, this can be seen in Figure 41, which also presents the feedback. In this instance the answer was incorrect, so the feedback is displayed in a red box, the feedback explains the reason why the user's answer was incorrect.

**Incorrect:** The people in the finance department should, and needs to have access to the shared folders in their department.

**Request:** The head of finance requests access to the finance team's shared folders.

Time remaining: 12 seconds

Deny Accept

**Help Desk Guidelines**

**Least Privilege Principle** - Only give access if the person needs it for their job.

**Approval for Sensitive Data** - Never grant access to private, confidential, or sensitive data unless it's clearly authorized or part of their role.

**Role-Based Access** - Access should match the requester's department or position. If it doesn't fit their job, deny it.

**Overview 0/1 correct**

This is the overview of what you have processed so far

- ✗ Accepted - An intern in IT asks for access to payroll records.
- ✗ Denied - The head of finance requests access to the finance team's shared folders.

Figure 41: Caption

## 6.6 Module 6: MailMole

Module 6 is the finale. It is here Dana IT manager asks the user to comb through nine quarantines emails, and hunt for the proof of an intentional insider threat. In module 3 the user was asked to distinguish between the binary “Phish/Legit” verdict, the challenge in module 6 requires correlation across headers, links, sender aliases and attachments to identify an intentional insider and the evidence that implicates them. The learning material for module 6 is very brief, and serves as a concise methodological reminder, then sends the user straight into a rudimentary DFIR challenge.

The module touches on the following frameworks as demonstrated in Table 13.

Framework	Inclusion status for current module	Notes on status for inclusion
NICE Workforce Framework for Cybersecurity	✓	Further expanding on utilized TKS statements, with particular focus on Skills
CISA Insider Threat Mitigation Guide	-	No direct involvement in the module
Critical Pathway to Insider Risk	✓	No direct mapping, however both stressors and concerning behaviors are exhibited in the challenge
MITRE Insider Threat TTP KB v2.0	✓	The challenge emails represent concrete TTPs (e.g. exfiltration)

Table 13: Frameworks inclusions status, module 6

Module 6 is primarily practical and focus on equipping the users with the ability to not only detect a malicious email but also articulate who the insider is, how they operated, and which artifacts constitute the “smoking gun. In short it deepens the focus on *"Identify potential insider threats (T1983)"* and touches on *"Conduct insider threat risk assessments" (T1974)*. Figure 42 shows the TKS statements that Module 6 aims to address.

The full list of in-scope TKS statements for the course can be seen in Table 1 in subsection 4.2.1 where a short descriptive text expands on the contents of each statement. Figure 22 shows the TKS statements actually implemented in the course.

Task ID	Task Description	Skill ID	Skill Description	Knowledge ID	Knowledge Description
<b>T1983</b>	Identify potential insider threats	<b>S0913</b>	Skill in performing link analysis	<b>K1261</b>	Knowledge of known insider attacks
<b>T1974</b>	Conduct insider threat risk assessments	<b>S0907</b>	Skill in identifying insider threats	<b>K1258</b>	Knowledge of insider threat tactics
		<b>S0896</b>	Skill in recognizing behavioral patterns	<b>K1256</b>	Knowledge of insider threat operational indicators
		<b>S0890</b>	Skill in performing threat analysis	<b>K1248</b>	Knowledge of digital and physical security vulnerabilities
		<b>S0866</b>	Skill in performing log file analysis	<b>K0785</b>	Knowledge of insider threat tools and techniques
		<b>S0854</b>	Skill in performing data analysis	<b>K0684</b>	Knowledge of cybersecurity threat characteristics
		<b>S0848</b>	Skill in performing behavioral analysis	<b>K0683</b>	Knowledge of cybersecurity vulnerabilities
		<b>S0477</b>	Skill in identifying anomalous activity	<b>K0682</b>	Knowledge of cybersecurity threats

Figure 42: Module 6. TKS Statements

A more granular demonstration of how each of these TKS statements are covered in module 6 will be presented in both the following learning material and challenge sections.

### Learning material

As stated, Module 6 is focused on practicality. The learning material sets the stage by stating that after practicing identifying obvious phishing, Dana (IT Manager) now requires a closer inspection of nine quarantined emails. The objective is clearly stated: "identify the insider threat, use what you know about the employees of Skybound Technologies and what you have learned so far about analyzing an email". It does not introduce any new concepts or insights.

### Challenge

Module 6, "MailMole," serves as the final challenge, designed to transition learners from identifying overt phishing attempts to conducting a rudimentary email forensic investigation. Participants were tasked with downloading a collection of EML files, representing quarantined emails from Skybound Technologies, with the objective of identifying an intentional insider threat and the specific "smoking gun" evidence implicating them.



*Alignment with NICE Workforce Framework for Cybersecurity*

Users are asked to engage in a rudimentary form of digital forensics by analyzing the emails. This requires *"Skill in performing log file analysis"* (S0866) at a conceptual level (email headers, content), *"Skill in performing data analysis"* (S0854) to connect pieces of information across multiple emails, and *"Skill in performing link analysis"* (S0913) to understand where links might lead or what their true nature is. The task of identifying the "smoking gun" necessitates *"Skill in identifying insider threats"* (S0907) and *"Skill in performing threat analysis"* (S0890) by correlating email content with known employee situations (e.g. Jordan's disgruntlement, Carl's activities, Lori's mistakes). The challenge prompts users to *"recognize behavioral patterns"* (S0896) as reflected in email communications. Successfully identifying the intentional insider and their methods means the learner has applied most of the chosen Knowledge statements, but particularly; K1256, K1258, K0785 and K1261. The challenge is foundational for the novices to apply learned knowledge and develop analytical skills relevant to *"Identify potential insider threats"* (T1983) and *"Conduct insider threat risk assessments"* (T1974) evaluating evidence and distinguishing signal from noise.

*Alignment with Critical Pathway to Insider Risk*

With this challenge, the CPIR axis is followed to its endpoint; the hostile act [11, p. 42]. The user sees the culmination of previous stressors and concerning behaviors in the active engagement in a hostile act. While, again, not being mapped explicitly to CPIR, the fact that the narrative demonstrates the progression on the axis is done intentionally to provide the narrative a realistic flow.

*Alignment with MITRE Insider Threat TTP KB v2.0*

Although emails contain attempts of phishing sent to Skybound Technologies, the relevant TTP comes from the email where the intentional insider threat sends a zip archive containing client project files to a competitor. A clear sign of *TA0010: Exfiltration* by *T1567: Exfiltration Over Web Service*.

*Description of the challenge*

EML files were generated manually within a text editor to simulate realistic email traffic. For pedagogical clarity and to focus the analysis on core content and headers, these files were intentionally simplified, omitting complex elements such as DMARC, DKIM, SPF records, and extensive traceability headers commonly found in full email exchanges, see Figure 43 for an example.

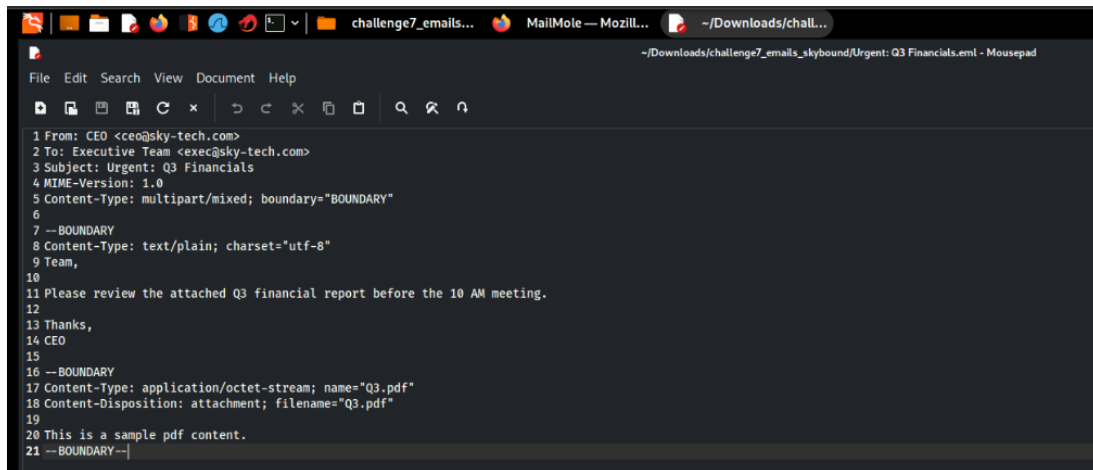


Figure 43: A example eml file opened on the Campfire Security's platform platform

The collection of emails was curated to provide a diverse analytical experience: one email was a defanged and anonymized version of an actual phishing message personally received by the author (see Figure 44). While others were crafted to emulate plausible benign internal communications (for example Figure 43). The challenge emails made sure to demonstrate behavior and technical indicators such as an example of an unintentional data leak (Appendix A.12 Figure 73) and expressions of employee disgruntlement (Appendix A.12 Figure 69). Beyond that, of course, one of the emails (Appendix A.12 Figure 68) indicates active and **intentional** data exfiltration (note that the emails are both in Appendix as stated but can also be found in the separate zip archive). Some of the emails reference attachments by filename, the actual file contents were either placeholder/sample files or simply metadata descriptions without the full embedded file, focusing the user on analyzing the context and indicators surrounding the attachment rather than the attachment's content itself.

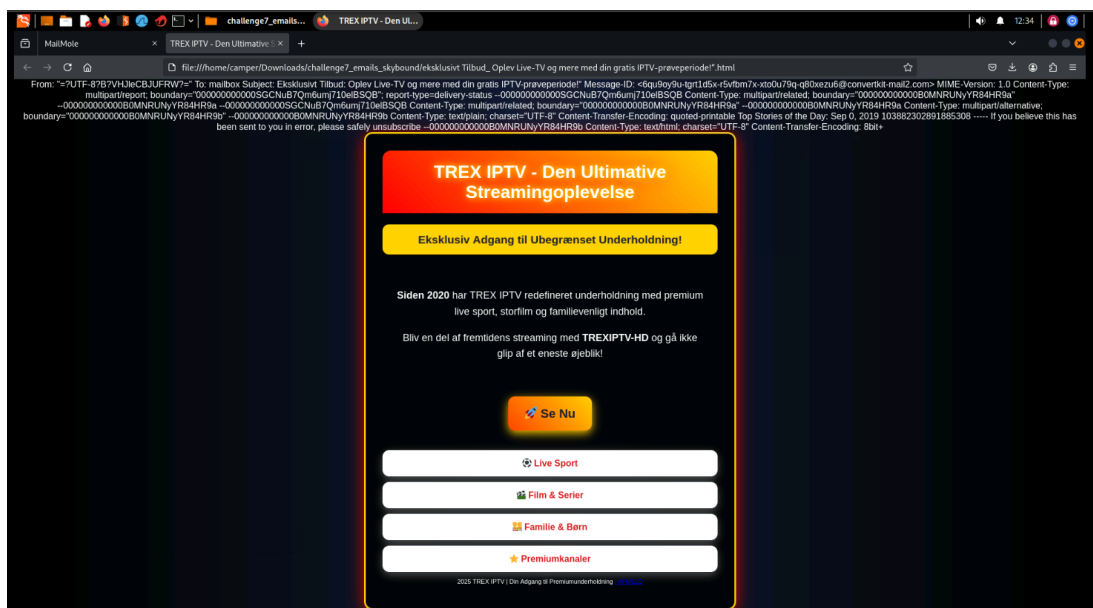


Figure 44: A html rendered version of one of the challenge mails

In order for the user to get the files they have to download and unpack them. The Challenge Overview page

provides a direct download link (Figure 45, and unpacking is a matter of right-clicking the folder and choosing unpack (Figure 46).

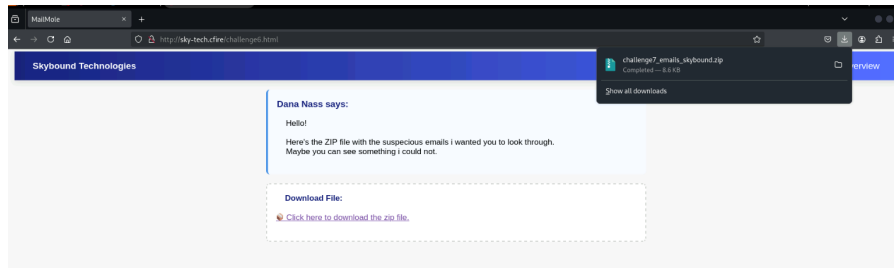


Figure 45: Screenshot of Challenge Overview and download link

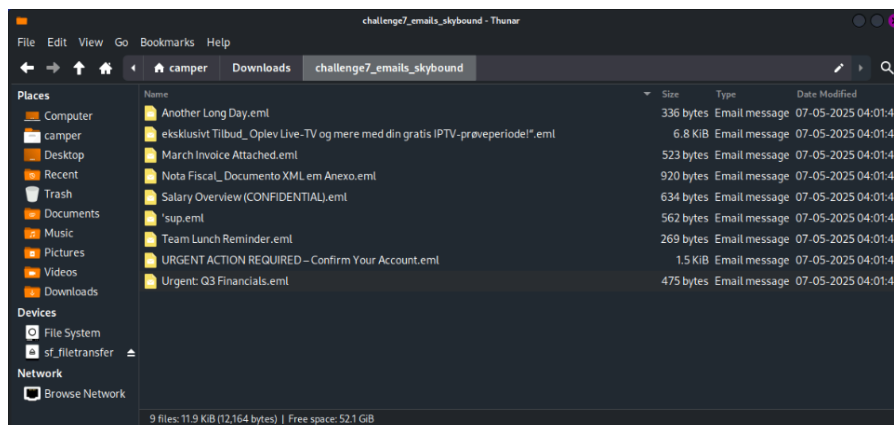


Figure 46: Screenshot of unpacked emails in the Campfire Security's platform

Solving the challenge and finding the flag requires the user to find the correct email and combine the receiver's first name with the last word in the email (Figure 47).

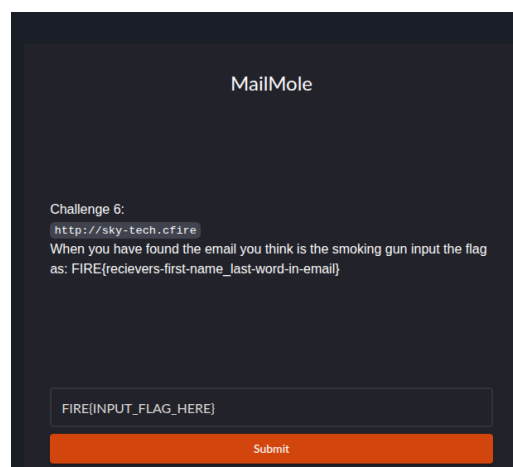


Figure 47: Input flag here

## 7 Results: Testing the Material in a Workshop

It was of the outmost importance for us to test our course as a part of the project. To reiterate the purpose of the testing from subsection 4.3: The purpose of the test was twofold: firstly, to ascertain the understandability and feasibility of the CTF course for individuals considered cybersecurity novices, and secondly, to collect qualitative feedback that could guide iterative refinements efforts.

In this section, the main findings from the testing will be presented. It is composed of a combination of insights gleaned from observational notes taken by the researchers during the workshop and from questionnaires completed by the participants immediately afterward.

As an overview, we will firstly present some overarching observations from the course, before proceeding into results from the feedback schema. During the workshop we observed several instances of the participants looking focused and engaged, our notes frame the participants as leaning towards their screen staring intently and other body language indications, such as frowning of the brows and a thoughtful finger on pursed lips A.6. Further, we have noted a few instances of laughs from the participants as they stumble on details that are funny to them. We saw the same reaction to particular intense and animated attempt at solving the last challenge where one of the participants thought they had a breakthrough (which sadly they did not at that instance). During the workshop we saw little active collaboration between the participants, but what collaboration there was later turned out to be a disturbance for P2. In the feedback form P2 states *It is difficult to focus when people are talking around you. You can easily feel pressured to not read the material as thoroughly* [translated by the researchers] - see Appendix A.13 for original text.

We had a good time during the workshop, and our experience indicates that so did the participants.

### Focused Attention

The questions related to Focused Attention from User Engagement Scale-Short Form (UES-SF), relates to how absorbed and concentrated participants were during the experience, as presented in subsection 4.3. For a graphic representation of the distribution of answers related to this scoring, see Appendix A.14 Figure 77

The highest score a participant can rate Focused Attention is 5 (which indicates positive sentiment), the lowest is 1 - calculated as per [53]. The participants scores are demonstrated in Table 14.

Participant ID	Combined scoring for question	Max points available
P1	3.67	5
P2	2.67	5
P3	4	5
P4	2	5

Table 14: Scores for Focused Attention

P1 and P3 were at least partly “in the zone” during play with scores of 3.67 and 4 out of 5 possible. One participant, P4 never quite “clicked” with the material giving a total score of 2. It is maybe not surprising that it was in fact P4 who had to leave during the workshop because of incoming work-related task. Further, observing P4

during the workshop they demonstrated indications of being frustrated and distracted from very early on even sighing audibly (see Danish observation notes in Appendix A.4). P4s early departure and frustration might have influenced their scoring of Focused Attention, however that does not mean their experience and feedback is not relevant to the course. At a minimum it stresses and echoes the points also brought up in the interview with Thomas Kristmar: *"When doing awareness and cybersecurity training it is important that you are allowed to do it, at a time that fits with your everyday tasks"* [translated from Danish by the researchers](Appendix A.7) Without a fitting dedication of time and resources, it can hinder the experience of Focused Attention.

### Perceived Usability

The questions related to Perceived Usability from UES-SF, relates to understanding the ease of use and the level of frustration experienced by participants, as presented in subsection 4.3. For a graphic representation of the distribution of answers related to this scoring, see Appendix A.14 Figure 78

Beware the scoring of this table is inverted compared to the Focused Attention, in Table 15 a **max score of 5 would indicate a negative sentiment** while a low score is positive.

Participant ID	Combined scoring for question	Max points available
P1	3	5
P2	1.33	5
P3	2.33	5
P4	2.33	5

Table 15: Scores for Perceived Usability

P2 seem to have experienced very little frustration with the course with a score of only 1.33 of 5. Whereas the other participants express slightly higher levels of frustration with the course. During the workshop we observed some of this frustration unfold. In the beginning we observed technical difficulties with getting the challenge not displaying properly, which was quickly fixed. What is perhaps more pertinent are the frustration points expressed later in the workshop. For example, in the initial approximate 25min there was confusion regarding whether or not the participants were to answer individually or wait for each other and answer together via group discussions A.6. This is despite the fact that we attempted to set out clear guidelines in our opening talk - the first 25mins frustration indicated we failed in that communication. Moreover, frustration was expressed during Challenge 3, where some of the participants expressed it was hard to identify the spoofed Skybound Technologies email domain, as they claimed not knowing the correct one. To that point, we learned after approximate 32min that one of the participants had not caught on to that the learning material changed when progressing to the next challenge. After the testing and questionnaire was done the participants had a casually conversation with us before leaving. Here they mentioned they felt there was a lot of text in the learning material, calling it a "wall of text".

### Aesthetic Elements

The questions related to Aesthetic Elements from UES-SF, relates to the users experience of the visual appeal

of the course, as presented in subsection 4.3. For a graphic representation of the distribution of answers related to this scoring, see Appendix A.14 Figure 79

A max score of 5 in Table 16 indicates a positive sentiment.

Participant ID	Combined scoring for question	Max points available
<i>P1</i>	2.33	5
<i>P2</i>	4.33	5
<i>P3</i>	3	5
<i>P4</i>	3.33	5

Table 16: Scores for Aesthetic Elements

For Aesthetic Elements the outlier is P1, who is most critical with a score of 2.33 of 5. Sadly, we did not capture an elaboration of the score.

### Reward Factor

The last question from UES-SF is regarding Reward Factor, which relates to the perceived value of the experience, as presented in subsection 4.3. For a graphic representation of the distribution of answers related to this scoring, see Appendix A.14 Figure 80

As previous, in Table 17 a high score indicates a positive sentiment.

Participant ID	Combined scoring for question	Max points available
<i>P1</i>	4	5
<i>P2</i>	4.33	5
<i>P3</i>	4	5
<i>P4</i>	3	5

Table 17: Scores for Reward Factor

Noteworthy here, is the relatively high perceived value despite the brief 1-hour runtime of the workshop. P4 is the outlier with a score of 3 out of 5. P4s cybersecurity experience level is significantly higher than the other participants, and also higher than the target audiences. As such, the score of nine is for us deemed a very good score, as it for us indicates that both cybersecurity novices and more experienced individuals potentially can glean value from the course.

**Overall Engagement Score** As per the UES-SF guide [53] the overall engagement score can be calculated as a summarization of the level of engagement felt by the participants during the course, see Table 18.

Participant ID	Overall Engagement Score
<i>P1</i>	3.25
<i>P2</i>	4
<i>P3</i>	3.67
<i>P4</i>	3

Table 18: Overall Engagement Score

**Participants previous experience** Figure 48 shows the group is evenly split between having previous experience with CTFs or not. This provides an opportunity to gather insights from both participants familiar and unfamiliar with CTFs. The two different perspectives could add more nuance to the feedback and provide valuable information. The more familiar participants might provide insights based on their previous experiences with CTFs, while the unfamiliar participants could offer a fresh, new and unspoiled perspective.

4. Have you previously participated in a CTF?



Figure 48: Participants experience with CTFs

### Difficulty of the challenges

Three of the four participants rated the overall difficulty as “Easy” while one chose “Neither easy nor difficult”, see Figure 49.

9. How was the overall difficulty of the challenges



Figure 49: Experience of overall difficulty

In the following, all quotes are translated by the authors and can be seen in their original form in Appendix

A.13.

Although the tasks were perceived as straightforward, most participants singled out the final e-mail-forensics flag as markedly harder: P1: “*The last challenge was difficult*” and P2 states: “*The last 'key' was hard to find - maybe more guiding*”. Even the second most experienced participant - P3 - echoed this pattern, describing the earlier items as “very easy” but the last as “more challenging”. Taken together, the data suggest the challenge ladder is pitched correctly for novices up to Challenge 5, but the final step introduces a noticeable spike. Perhaps adding additional but optional hints there could smooth the difficulty curve without diluting earlier tasks.

### Preferences for CTF vs. traditional methods

Enthusiasm for the gamified format is evident from the feedback. Three participants selected “Strongly Agree” when asked if they preferred this style of learning to conventional training, while the fourth was neutral - see Figure 50.

11. I prefer this style of learning compared to traditional methods ?



Figure 50: Preferences for CTF or traditional methods

No one expressed a negative preference. Comments reinforce the rating, P2 called the explanations “down to earth”, and P3 stated that hands-on security problems are already “front of mind” and therefore more engaging than passive instruction. These findings align with the literature that CTFs can boost motivation, even for users with minimal prior experience.

### The effect of story telling on the experience and engagement

Narrative elements landed ambiguously with the participants. On experience, three of four respondents selected “Uncertain,” while only P3 said “Yes” to the narrative influencing the experience, see Figure 51.



12. Did the story telling influence your experience?



Figure 51: Story tellings influence on experience

On how the narrative affect engagement, the split was No (two participants), Uncertain (one), Yes (one), see Figure 52.

14. Did the storytelling affect your engagement



Figure 52: Story tellings influence on engagement

Qualitative remarks clarify the ambiguity: P2 felt the narrative text was “a bit irrelevant until the end” and tended to skim it once the pattern became clear; P3 remarked that “a little roleplay is always good for immersion” (see Appendix A.13). In short, the story neither distracted nor powerfully enhanced engagement for most participants. If that reflects the nature of narratives in general or only reflects the narrative and exposition provided in our course is unclear from the feedback. However future iterations of the course might seek to condense exposition and weave critical narrative clues into the challenges instead, so the plot feels functional rather than ornamental.

### Ability to explain a concept to colleague

All four participants answered “Yes” when asked whether they could now teach at least one course concept to someone else, see Figure 53. Of note is that we did not test their claim, but it relies solely on their feeling of being capable.

16. Do you believe you could explain at least one concept or technique from the course to a colleague ?



Figure 53: Ability to explain a concept post workshop

Leaving the workshop with a feeling of being capable is very positive, and hopefully emboldens the participants to engage with cybersecurity material going forward.

Across all nine points of feedback the direction is overwhelmingly positive: usability, aesthetics, motivation, appropriate difficulty, and (crucially) self-reported knowledge transfer all meet or exceed expectations. The most glaring critiques are the limited impact of the storyline and the frustrations felt by one participant. Given the small participant group (four Statens IT staff) any inferential statistics would be meaningless, but still, two pragmatic findings stand out:

- The CTF format achieves to leave the participants confident they can explain an insider threat concept.
- Future iterations could benefit from investing in richer game mechanics rather than narrative exposition.

These findings will be further unpacked in the discussion section and could potentially be used for any next design iteration of the Campfire Security module.

## 8 Discussion

This section critically examines the project findings, reflecting on the development and testing of a CTF course designed to teach cybersecurity novices about insider threats. It will explore the contributions of this work, the methodological limitations encountered, and the implications for usability and user experience in the context of cybersecurity education. The discussion aims to address the primary research question: *How can CTF be leveraged to inform cybersecurity novices about the fundamentals of insider threats?* and the sub-research question: *How is CTF a relevant concept for teaching cybersecurity?*

### 8.1 Our Contribution

Firstly we wish to discuss our novel contribution to the cybersecurity field, presented here first as a list and subsequently expanded upon. We highlight the following contributions, some of which are interconnected:

- A CTF course dedicated to insider threats
- Emphasis on interactive and gamified learning for insider threats
- The grounding of said CTF course in authoritative frameworks and theory
- Operationalizing complex concepts and frameworks towards cybersecurity novices
- Synthesis of expert opinion on the state of cybersecurity training in organizational settings
- An empirical evaluation for a novice audience

This project makes several contributions to the field of cybersecurity education, particularly in the challenging domain of insider threats when targeting a novice audience. The modules developed emphasize hands-on activity, requiring users to actively analyze scenarios, inspect emails, and make decisions, rather than passively consuming theoretical information. This was a direct response to the observation that existing materials on insider threats sometimes lack interactivity. A primary contribution is the development of a structured, multi-module CTF course specifically designed to introduce the fundamentals of insider threats to individuals with limited prior cybersecurity knowledge. Our review of existing cybersecurity training platforms indicated that while insider threats are sometimes mentioned, they are often treated as a subtopic within broader subjects like Identity and Access Management or supply chain security, rather than receiving dedicated, in-depth attention through an interactive learning experience tailored for beginners. This CTF course aims to fill that perceived gap by providing a focused educational resource. A distinctive aspect of this contribution is the explicit and systematic grounding of the course in authoritative cybersecurity frameworks and established learning theories. Specifically, concepts from CISA's Insider Threat Mitigation Guide, the Critical Pathway to Insider Risk (CPIR), and the MITRE Insider Threat TTP Knowledge Base were integrated into the learning material and challenge design. During the creation of the course, we debated the extent to which to directly include the names of the frameworks for further grounding. From our perspective, the academic value of the course could be increased by more direct implementation and reference to said frameworks, however that consideration was to be balanced with the inherent need for the course not to become a proverbial "wall of text" (more on that point later in subsection 8.3).

The dedication to include frameworks stem from a wish to provide a transparent and multifaceted theoretical underpinning in an effort to move beyond ad hoc content creation we experience on other platforms, where references to authoritative sources or detailed pedagogical rationales may be less apparent. Furthermore, the project contributes a practical demonstration of how complex, and often abstract, insider threat concepts and associated Tasks, Knowledge, and Skills (TKS) statements can be operationalized into accessible, interactive CTF challenges suitable for novices. The use of TKS statements can be seen as yet another way in which we sought to ground the course in academic rigorous rationale. A drawback to the way we operationalized the statements is the fact that the utilization is in fact purely theoretical, we did not validate that the participants themselves felt or experienced being exposed to the TKS statements contents.

An underutilized aspect, from our perspective, was the expert interview with Thomas Kristmar. His extensive experience provides a range of critical real world perspectives some of which resonated with the projects pedagogical foundations. His critique of traditional, passive training methods, such as PowerPoint presentations and non-interactive mandatory courses, strongly aligned with the project's use of the CTF format. He highlighted the importance of flexibility in training delivery, suggesting that learners should be able to engage with material at times that suit their workflow to maximize motivation and absorption. While the workshop setting for testing had its own time constraints, the CTF module, being hosted on the Campfire Security platform, is inherently designed for self-paced learning, thereby accommodating this crucial aspect. All these points fit well within our approach and the considerations we made during the process. Kristmar did however have many more perspective and points, which were relevant but not in scope for the project (see section on future works in section 9), including pivoting the course material to include *espionage* as theme, see section 5. A point which was in scope, but perhaps underutilized was: "Behavior changing training hinges on: relevance, interactivity and contextual fit" (see Appendix A.9). This concept highlights one perspective on what the goal of cybersecurity training is: behavior change. While gathering feedback from our participants, we did not make any attempts to test if the knowledge and skills result in actual behavior change. A somewhat mitigating point is our participants' self-reported ability to explain a concept from the course to a colleague.

The project included an empirical evaluation of the developed CTF course through a workshop with employees from Statens It. The testing provided valuable feedback on the module's understandability, usability, and engagement from the perspective of the target audience, which included participants who fit neatly in our target audience, cybersecurity novices. Such empirical data, even from a small sample, is essential for the iterative refinement of the material, our biggest gripe is that we did not have the opportunity to prioritize utilizing the feedback to improve the course.

## 8.2 Methodological Reflections & Limitations

Here we present and acknowledge certain methodological reflections and inherent limitations present in said methodological approach.

While the workshop as presented in the previous section provided valuable insights and presents a novel avenue for our project, the approach has limitations. Firstly regarding the participant group size. While this group size allowed for rich qualitative feedback and observational insights into *their* experiences with the module, it is insufficient for drawing statistically generalizable conclusions about the module's effectiveness or the broader novice population's response. The findings, therefore, offer a valuable but snapshot style assessment, rather than a comprehensive, widely applicable assessment. In line with this argumentation is the unclear definition of the term *novices*. While participants from Statens It identified their own experience levels as mostly novices, their employment within an IT organization might differentiate them from novices in entirely non-technical fields. Their general IT work experience could influence their baseline understanding, technical comfort, and interaction with the CTF material, suggesting that the results may be mostly applicable to novices within similar organizational contexts. A substantiation of the term *novice* could help make our content more applicable to other contexts, as the term without a clearer definition could mean different things in different contexts.

The workshop format itself presents further limitations. While being an academically acknowledged way to gather feedback and perform test, the entire session including the CTF play through and feedback collection, was condensed into approximately one and a half hours (a one-hour workshop followed by a 30-minute evaluation). This limited timeframe, compounded by one participant needing to attend to other work duties and leaving the workshop early, may have impacted the depth of engagement and the thoroughness of feedback. This situation contrasts with the expert advice received from Thomas Kristmar, who emphasized the importance of allowing individuals to undertake training at times that fit their schedules and permit dedicated focus, rather than as a mandated task during a busy workday. Our test setup, by necessity of coordinating a group of participants, did not fully align with this ideal of learner controlled timing and flexibility.

When discussing insights gleaned from the interview with Thomas Kristmar, it is important to also critique the approach taken with interviews in general through this project. The process involved a single researcher transcribing, coding, and analyzing both the interview transcript and the accompanying observation notes. Although this approach was systematic and thorough, the involvement of only one analyst introduces a potential for subjective interpretation of the data. A more robust approach might have involved both team members independently coding the interview and then collaboratively discussing and reconciling their findings to improve the reliability of the analysis. More broadly for the interviews, it is important to highlight the under-utilization of the interview conducted with Kristian Larsen from Campfire Security. That interview was conducted late in the process and, while valuable, a thorough analysis of it was deemed out of scope when prioritizing our efforts in the late stages of the project.

The collaborative nature of this project with Campfire Security also introduced limiting parameters. An inherent direction for the project was to develop a CTF module which meant that alternative pedagogical approaches for introducing insider threats were not explored within this project's scope. And while the participants all announced their preferences for the CTF format over *traditional methods* (see section 7) we acknowledge that we neither clearly define traditional methods nor test our CTF vs. any other methods. Furthermore, the modules were designed specifically for Campfire Security's platform. Consequently, both the design, features, and user

experience of the CTF are intrinsically hardwired to the capabilities and constraints of this particular platform, which may affect the transferability of the specific module or findings to other learning environments.

### 8.3 Usability and User Experience

In line with discussions of the Campfire Security platform, the following the discuss the usability and user experience of our CTF course. The project argues and substantiates for how design is paramount to the effectiveness of a course, also when targeted towards novices.

A positive find was that participants generally found the challenges to be do-able. Three out of four rated the difficulty overall as "Easy" and one as "Neither easy nor difficult". From the perspective of flow theory, which posits that optimal engagement occurs when a task's challenge aligns closely with the user's skill level, an "Easy" rating could potentially indicate a risk of boredom. Having neither "Too Easy" nor "Too Difficult" presented in the feedback indicates that it is at least uncertain whether it actually diverged into boredom or anxiety. The largely positive Overall Engagement and Reward Factor scores (see section 7), suggests that participants remained engaged and found the experience valuable despite the perceived ease of most tasks. It is noteworthy that the final e-mail forensics challenge in Module 6 (see subsection 6.6) was consistently singled out as markedly more difficult, indicating a potential difficulty spike that could potentially disrupt flow.

The role and impact of the narrative featuring Skybound Technologies and its employees received mixed feedback. While intended to provide context and enhance engagement, three of four respondents were "Uncertain" if the narrative influenced their experience, and the impact on engagement was similarly divided. Qualitative comments clarified this: one participant (P2) found the narrative text "a bit irrelevant until the end" (see section 7) tending to skim it once the pattern of its non-immediate utility in early challenges became clear, while another (P3) felt that "a little roleplay is always good for immersion" (see section 7). This suggests that while the characters and company were a consistent thread, the narrative's direct functional relevance might not have been consistently apparent until the final module. Future iterations of the course could benefit from a more integrated narrative, if the desired positive outcomes of a narrative is to be achieved. This while still balancing the density of information provided. The proverbial "wall of text" which some of the participants experienced could have influenced how one participant did not initially realize the learning material was changing with each new module progression. Similarly, during Module 3, some participants expressed difficulty identifying the spoofed Skybound Technologies email domain, despite this information being available in the learning material and challenge description. Furthermore, participants was surprised that Challenge 5 was timed, even though this was explained on an introductory page for that specific challenge. These occurrences, along with initial confusion during the workshop about whether to proceed individually or wait for group discussion, point towards a need for enhancing the clarity of instructions, both within the CTF interface and in how the course structure is communicated by facilitators.

Regarding the sub-research question about the relevance of CTFs for teaching cybersecurity, the feedback was overwhelmingly positive. Three participants "Strongly Agreed" that they preferred this style of learning com-

pared to "traditional methods", with the fourth being neutral (see 7. Comments highlighting the "down to earth" (see Appendix A.13) explanations and the engaging nature of hands-on security problems reinforce this preference. This aligns well with existing literature suggesting that CTFs can significantly increase participant motivation, engagement, and the development of practical skills (see subsection 3.4). However, as stated previously in subsection 8.2, it is important to note that the limitation in the term "traditional methods" might lack clarity, which means that participants compared the CTF experience to their varied personal understanding of traditional training. Additionally, this project did not include a direct comparison by testing the same learning material delivered through a non-CTF format, or having a control group. Accepting the participants feedback on preference at face value does follow suit both the Overall Engagement Score and with what we glean from both the literature and interview (see section 3 and section 5 respectively) giving at least indications of CTFs being relevant for teaching cybersecurity. A question for debate then emerges: is the course developed in this project still a CTF?. This question is pertinent and thought provoking because our design, while firmly based in the challenge based and interactive format known from CTFs, also incorporates substantial introductory learning material for each module, a narrative structure, and a primary focus on fundamental understanding for novices rather than purely on competitive puzzles often associated with traditional CTFs. While the term "CTF" can be broad, our course adopts a particular but not unique prioritization of pedagogical goals over competitive elements, and thus might not be a classic CTF but something else entirely. Regardless of whether it strictly adheres to a classic definition of CTF or is considered a 'CTF-inspired' educational experience, the positive feedback on engagement and preference suggests that the core principles borrowed from the CTF concept, ie. hands-on problem solving, contextualized scenarios, and gamified interaction, can be highly relevant and effective for teaching cybersecurity to this audience.

Regarding the main research question concerning how CTFs can be leveraged to inform cybersecurity novices about insider threat fundamentals. This project suggests that leveraging CTF to inform about cybersecurity, can be achieved through a combination of structured, interactive challenges grounded in authoritative frameworks, and a gamified approach which enhances engagement. The key leverage points identified through this project include the operationalization of theoretical knowledge and frameworks into condensed learning material sections and hands-on tasks. It further attempts to leverage a narrative to contextualize the experience for the participants, though this point requires more careful integration. There are however some limitations to that claim based on our findings, as factors such as: our participant group size, the timeboxed workshop format and the unclear definition of the term CTF all are factors which potentially negates some of the conclusive power of our project. The developed CTF course aimed to make the complex topic on insider threats accessible even for novices and, despite some usability critiques, generally succeeded in creating a positive experience preferred over undefined "traditional methods" by our participants. Furthermore the complete agreeance from participants on being able to explain a concept from the insider threat theme further suggest a successful experience, also observing that most, if not everyone completing the course material and associated challenges.

## 9 Conclusion

This project explores how a CTF course can be leveraged to inform cybersecurity novices about insider threats. This was achieved by developing a dedicated insider threat course in collaboration with Campfire Security. The project also investigates how CTF can serve as a relevant concept for teaching cybersecurity by evaluating the relevant literature, interviewing a subject matter expert, and critically testing the developed material with a small test group.

The main contribution to cybersecurity education resources is an interactive and gamified CTF course specifically and exclusively focused on informing cybersecurity novices about insider threats. The course was developed using content from authoritative sources and integrated well established frameworks like CISA's Mitigation Guide and MITRE's TTPs into the course material.

The primary research question: *RQ: How can CTF be leveraged to inform cybersecurity novices about the fundamentals of insider threats* was addressed by the development of a structured, informative, gamified and interactive CTF experience for cybersecurity novices. While the CTF and its implementation were generally well received, the evaluation indicates that the narrative element was not adequately incorporated, and subsequently not providing the intended enriched user experience. Despite this, the overall evaluation of our participant suggests that CTFs can indeed be effectively leveraged to inform cybersecurity novices about the fundamentals of insider threats.

The sub-research question: *SubRQ: How is CTF a relevant concept for teaching cybersecurity?* was also successfully addressed. Participants indicated a clear preference for this interactive style over traditional methods, a finding that aligns with the literature and the expert interview insights highlighting CTFs' potential to boost engagement, enjoyment and practical skill acquisition. These findings underscore the value of CTF based approaches in making complex cybersecurity topics more accessible and engaging for novice learners.

While these results are promising, the study acknowledges limitations such as the small participant group for the workshop evaluation and the lack of evaluation on the participants learning outcomes. Which means the findings should be seen as indicative rather than broadly generalizable at this stage.

### Future Work

To build upon this work, several avenues for future research are seen as viable:

Firstly, the feedback from the participants should be incorporated into the course via a iterative design loop. Following that, further testing could be done on a larger and more diverse group of cybersecurity novices. This could enhance qualitative data and provide an avenue for collecting quantitative insights.

Secondly, pivoting the project toward a teaching oriented approach vis-à-vis merely informing could provide a valuable avenue for research. Our research focus specifically not on learning as knowledge and learning in general are hard to measure without an extensive and long testing period. Pivoting to also include a knowledge focus or behavioral change indicators alongside the established measurement points from this project, would



provide stronger and more empirical evidence of the impact of CTF in an education context.

Thirdly, an avenue presents itself in the development of new CTF modules which further utilize the frameworks especially integrating more TKS statements and increasingly complex TTPs. This would serve as the logical next progression, moving the course from a focus on novices to a more advanced context.

Fourth, an exploration of the use of narratives in CTFs, with a goal of finding different approaches to incorporate the narrative in a meaningful and engaging manner. Thorough research could help facilitate the integration of narratives in a meaningful way in this type of learning formats.

## References

- [1] AAU, *Rules for the use of generative ai at aau*, Retrieved May 05, 2025. [Online]. Available: <https://www.students.aau.dk/rules/rules-for-the-use-of-generative-ai#what-should-i-pay-attention-to?>.
- [2] OpenAI, *O4-mini*, Retrieved May 05, 2025. [Online]. Available: <https://platform.openai.com/docs/models/o4-mini>.
- [3] Campfire Security, *About campfire security*, Retrieved May 18, 2025. [Online]. Available: <https://campfiresecurity.dk/about>.
- [4] Campfire Security, *Campfire security*, Retrieved Jun 2, 2025. [Online]. Available: <https://app.campfiresecurity.dk/>.
- [5] Microsoft, *What is an insider threat? unraveling insider risks* / *Microsoft Security*, Retrieved Mar 21, 2025, from <https://www.microsoft.com/en-us/security/business/security-101/what-is-insider-threat>. [Online]. Available: <https://www.microsoft.com/en-us/security/business/security-101/what-is-insider-threat>.
- [6] CISA, *Defining Insider Threats* / *CISA*, Retrieved Mar 11, 2025, from <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>. [Online]. Available: <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>.
- [7] Ponemon Institute, *2025 cost of insider risks global report*, Retrieved Mar 24, 2025, from [https://www2.dtexsystems.com/1/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025\\_Cost\\_of\\_Insider\\_Risks\\_Global\\_Report\\_by\\_Ponemon\\_and\\_DTEX.pdf](https://www2.dtexsystems.com/1/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf). [Online]. Available: [https://www2.dtexsystems.com/1/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025\\_Cost\\_of\\_Insider\\_Risks\\_Global\\_Report\\_by\\_Ponemon\\_and\\_DTEX.pdf](https://www2.dtexsystems.com/1/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf).
- [8] C. David Hylender, P. Langlois, A. Pinto, and S. Widup, *Verizon 2024 data breach investigations report*, Retrieved Mar 21, 2025, from <https://www.verizon.com/business/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf>. [Online]. Available: <https://www.verizon.com/business/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf>.
- [9] J. Holdsworth and M. Kosinski, *What is pretexting?* / *IBM*, Retrieved Mar 24, 2025, from <https://www.ibm.com/think/topics/pretexting>. [Online]. Available: <https://www.ibm.com/think/topics/pretexting>.
- [10] NIST, *Nist cybersecurity framework (csf) 2.0*, Retrieved May 11, 2025. [Online]. Available: <https://doi.org/10.6028/NIST.CSWP.29>.
- [11] CISA, *Insider threat mitigation guide*, Retrieved Mar 21, 2025. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>.

- [12] M. F. Lenzenweger and E. D. Shaw, “The critical pathway to insider risk model: Brief overview and future directions,” *Counter-Insider Threat Research and Practice*, 2022, Retrieved May 11, 2025. [Online]. Available: <https://citrap.scholasticahq.com/article/36186-the-critical-pathway-to-insider-risk-model-brief-overview-and-future-directions>.
- [13] S. E. Institute, “Common sense guide to mitigating insider threats, seventh edition,” Tech. Rep., Sep. 2022, Retrieved May 11, 2025. [Online]. Available: <https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/>.
- [14] G-Research, *Introducing the insider attack matrix*, Retrieved May 11, 2025. [Online]. Available: <https://www.gresearch.com/news/introducing-the-insider-attack-matrix/>.
- [15] MITRE, *Insider threat ttp knowledge base v2.0.0*, Retrieved May 11, 2025. [Online]. Available: <https://center-for-threat-informed-defense.github.io/insider-threat-ttp-kb/>.
- [16] MITRE, *Green = seen: Insider tactics, techniques, and procedures*, Retrieved May 11, 2025. [Online]. Available: <https://center-for-threat-informed-defense.github.io/insider-threat-ttp-kb/knowledgebase/>.
- [17] MITRE, *Insider threat ttp knowledge base v2.0.0 / limitations*, Retrieved May 11, 2025. [Online]. Available: <https://center-for-threat-informed-defense.github.io/insider-threat-ttp-kb/analysis/#limitations>.
- [18] NICCS, *Workforce framework for cybersecurity (nice framework) / niccs*, Retrieved Mar 20, 2025, Nov. 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-181r1>.
- [19] NICCS, *Nice 2.0 / niccs*, Retrieved Mar 21, 2025, Mar. 2025. [Online]. Available: <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>.
- [20] NICCS, *One-pager / workforce framework for cybersecurity (nice framework)*, Retrieved Mar 20, 2025, May 2023. [Online]. Available: [https://www.nist.gov/system/files/documents/2023/06/05/NICE%20Framework%20%28NIST%20SP%20800-181%29\\_one-pager\\_508Compliant.pdf](https://www.nist.gov/system/files/documents/2023/06/05/NICE%20Framework%20%28NIST%20SP%20800-181%29_one-pager_508Compliant.pdf).
- [21] CTFtime team, *What is capture the flag?* Retrieved May 20, 2025. [Online]. Available: <https://ctftime.org/ctf-wtf/>.
- [22] Hack The Box, *Platform rules*, Retrieved May 20, 2025. [Online]. Available: <https://app.hackthebox.com/rules>.
- [23] S. Stieglitz, C. Lattemann, S. Robra-Bissantz, R. Zarnekow, and T. Brockmann, *Gamification*. Springer, 2017.
- [24] M. Csikszentmihalyi, R. Larson, *et al.*, *Flow and the foundations of positive psychology*. Springer, 2014, vol. 10.
- [25] M. Csikszentmihalyi, “Flow: The psychology of optimal experience,” in Jan. 1990.
- [26] H. Sharp, Y. Rogers, and J. Preece, *Interaction design: beyond human-computer interaction*, 5th ed. Wiley, 2019.

- [27] J.-H. Holmi, “Advantages and challenges of using capture-the-flag games in cyber security education,” B.S. thesis, J.-H. Holmi, 2020.
- [28] Tryhackme, *Learn cyber security / tryhackme cyber training*, Retrieved Jun 2, 2025. [Online]. Available: <https://tryhackme.com/>.
- [29] Root Me, *Welcome [root me : Hacking and information security learning platform]*, Retrieved Jun 2, 2025. [Online]. Available: <https://www.root-me.org/?lang=en>.
- [30] picoCTF, *Picoctf - cmu cybersecurity competition*, Retrieved Jun 2, 2025. [Online]. Available: <https://picoctf.org/>.
- [31] ctfLearn, *Ctflearn - learn to hack*, Retrieved Jun 2, 2025. [Online]. Available: <https://ctflearn.com/>.
- [32] HackThisSite, *Hack this site*, Retrieved Jun 2, 2025. [Online]. Available: <https://www.hackthissite.org/>.
- [33] HTB Academy, *Best online cybersecurity courses & certifications / htb academy*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/>.
- [34] PortSwigger Academy, *Web security academy: Free online training from portswigger*, Retrieved Jun 2, 2025. [Online]. Available: <https://portswigger.net/web-security>.
- [35] HTB Academy, *Frequently asked questions*, Retrieved May 25, 2025. [Online]. Available: <https://academy.hackthebox.com/faq>.
- [36] HTB Academy, *Intro to academy*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/module/details/15>.
- [37] HTB Academy, *Skill paths*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/paths>.
- [38] Cry0l1t3, *Network enumeration with nmap*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/module/details/19>.
- [39] PandaSt0rm and Sentinal, *Network enumeration with nmap*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/module/details/243>.
- [40] Cry0l1t3, *Introduction to information security*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/module/details/293>.
- [41] vaultia, *Introduction to red teaming ai*, Retrieved Jun 2, 2025. [Online]. Available: <https://academy.hackthebox.com/module/details/294>.
- [42] PortSwigger Academy, *All web security academy topics / web security academy*, Retrieved Jun 2, 2025. [Online]. Available: <https://portswigger.net/web-security/all-topics>.
- [43] PortSwigger Academy, *Learning paths / web security academy - portswigger*, Retrieved Jun 2, 2025. [Online]. Available: <https://portswigger.net/web-security/learning-paths>.
- [44] PortSwigger Academy, *Lab: Sql injection vulnerability in where clause allowing retrieval of hidden data / web security academy*, Retrieved Jun 2, 2025. [Online]. Available: <https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data>.

- [45] PortSwigger Academy, *Sql injection - portswigger*, Retrieved Jun 2, 2025. [Online]. Available: <https://portswigger.net/web-security/learning-paths/sql-injection/sql-injection-retrieving-hidden-data/sql-injection/lab-retrieve-hidden-data>.
- [46] PortSwigger Academy, *Hall of fame - web security academy*, Retrieved Jun 2, 2025. [Online]. Available: <https://portswigger.net/web-security/hall-of-fame>.
- [47] Campfire Security, *Campfire security*, Retrieved Jun 2, 2025. [Online]. Available: <https://app.campfiresecurity.dk/courses>.
- [48] Campfire Security, *Campfire security*, Retrieved Jun 2, 2025. [Online]. Available: <https://app.campfiresecurity.dk/course/6>.
- [49] M. D. Myers and M. Newman, "The qualitative interview in is research: Examining the craft," *Information and Organization*, vol. 17, no. 1, pp. 2–26, 2007, Retrieved April 18, 2025, ISSN: 1471-7727. DOI: <https://doi.org/10.1016/j.infoandorg.2006.11.001>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1471772706000352>.
- [50] M. Lichtman, "Making meaning from your data," *Qualitative Research in Education: A User's Guide*, pp. 241–268, 2013, Retrieved May 16, 2025. [Online]. Available: [https://us.sagepub.com/sites/default/files/upm-binaries/45660\\_12.pdf](https://us.sagepub.com/sites/default/files/upm-binaries/45660_12.pdf).
- [51] NICCS, *Workforce framework for cybersecurity (nice framework) / insider threat analysis*, Retrieved May 22, 2025, Jan. 2025. [Online]. Available: <https://niccs.cisa.gov/workforce-development/nice-framework/work-role/insider-threat-analysis>.
- [52] R. Krueger, *Observation in evaluation*, Retrieved May 31, 2025, 2017. [Online]. Available: <https://www.betterevaluation.org/sites/default/files/2023-05/Observation%20R.Krueger%2010.17.pdf>.
- [53] H. L. O'Brien, P. Cairns, and M. Hall, *User engagement scale (ues-sf)-short form*, Retrieved May 11, 2025. [Online]. Available: [https://dissemination-implementation.org/wp-content/uploads/2024/09/User-Engagement-Scale\\_instrument-short.pdf](https://dissemination-implementation.org/wp-content/uploads/2024/09/User-Engagement-Scale_instrument-short.pdf).
- [54] R. Streefkerk, *Transcribing an interview*, Retrieved May 16, 2025. [Online]. Available: <https://www.scribbr.com/methodology/transcribe-interview/>.

## A Appendix

### A.1 Framework Sections that were Removed

#### A.1.1 NIST Cybersecurity Framework v2.0

Published in February 2024, the NIST CSF(Cybersecurity Framework) 2.0[10] added a range of changes to the framework, in particular though the addition of a dedicated **GOVERN** function was noteworthy.



Figure 54: CFS Functions[10]

As Figure 54 demonstrates the CSF consists of six functions **GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER**. The framework explicitly states it is targeted towards a broad audience and designed to be technology-, sector-, and size-agnostic, making them an ideal enterprise-level lens for understanding and mitigating insider risk across industries etc. Further, the framework is outcome-centric, taking great care to limit itself to describing potential desirable outcomes an organization might aspire to achieve. Thus avoiding both prescribing outcomes and designating how said outcomes might be achieved.

As presented via the definitions of insider risk, it is clear that insider incidents are rarely caused by a single technical lapse; they usually emerge from gaps in governance, culture, or processes that span the whole organization. Using the CSF's outcome oriented approach and common vocabulary helps communication of enterprise level risk management between decision makers and security teams. Specifically, CSF provides the capability of building **Organizational Profiles**, both a current- and a target-profile. For insider threats, the current profile would be a description of how insider threat outcomes are currently satisfied across the six Functions, while the target then describes a desired future state. Further, **Tiers** allows the organization to gauge current and strive towards future maturity goals for their security programs. Ranging from **Tier 1 - Partial**, **Tier 2 - Risk Informed**, **Tier 3 - Repeatable** and **Tier 4 - Adaptive**, these Tiers provide a shorthand description of a maturity level. For example a Tier 1 organization may handle insider incidents ad hoc, whereas a Tier 4 embeds adaptive controls and predictive analytics into daily operations.

Building on CSF's macro lens, CISA Insider Threat Mitigation Guide offers program level depth tailored to insiders.

### A.1.2 CERT Common Sense Guide 7th Ed.

The **CERT Common Sense Guide 7th edition** (CSG) is a 2022 publication, which has its roots dating back to 2001 where staff from Carnegie Mellon University started studying the problems of mitigating insider threats and managing insider risk[13]. Since then, the CSG has grown to include data from over 3000 insider incidents and having published more than 150 publications. The CSG's aim is to provide current evidence based recommendations for mitigating insider threats and managing insider risk. In those terms; threat and risk, lies two distinct perspectives. *Threat* refers to the potential of an individual to use their access either maliciously or unintentionally in a way which can negatively affect the organization[13, p. 6]. Where as *risk* refers to the extend of impact and likelihood associated with the uncovering of an insider threat [ibid.]. With these two perspectives in scope of the recommendations provided, the CSG echoes what has been established from previous frameworks: insider threat/risk management programs are a socio-technical endeavour. With that, the groups identified by the CSG as key stakeholders, when targeting their recommendations follow rather intuitively as:

- Management
- Human resources
- Legal counsel
- Physical security
- Information technology
- Information security
- Data owners
- Software engineers

Prior to presenting the recommendations themselves, the CSG provides a few top findings from their dataset. Of note here is the apparent alignment in language between CSG and CPIR regarding stressors and concerning behavior. The top five *stressors*, *concerning behaviors*, *data exfiltration methods* and *sabotage methods* shown in Figure 55, provides a neat overview of the most common elements.

<b>Top Five Stressors</b> <table> <tr> <th></th> <th>Incidents</th> </tr> <tr> <td>1. Termination</td> <td><b>375</b></td> </tr> <tr> <td>2. Resignation</td> <td><b>245</b></td> </tr> <tr> <td>3. Internal Position Change</td> <td><b>55</b></td> </tr> <tr> <td>4. Organization M&amp;A Activity</td> <td><b>43</b></td> </tr> <tr> <td>5. Emerging Financial Problems</td> <td><b>33</b></td> </tr> </table>		Incidents	1. Termination	<b>375</b>	2. Resignation	<b>245</b>	3. Internal Position Change	<b>55</b>	4. Organization M&A Activity	<b>43</b>	5. Emerging Financial Problems	<b>33</b>	<b>Top Five Concerning Behaviors</b> <table> <tr> <th></th> <th>Incidents</th> </tr> <tr> <td>1. Went to Work for a Competitor</td> <td><b>89</b></td> </tr> <tr> <td>2. Disgruntled</td> <td><b>57</b></td> </tr> <tr> <td>3. Suspicious Foreign Travel</td> <td><b>55</b></td> </tr> <tr> <td>4. Financial Conflict of Interest</td> <td><b>53</b></td> </tr> <tr> <td>5. Physical Property Theft</td> <td><b>50</b></td> </tr> </table>		Incidents	1. Went to Work for a Competitor	<b>89</b>	2. Disgruntled	<b>57</b>	3. Suspicious Foreign Travel	<b>55</b>	4. Financial Conflict of Interest	<b>53</b>	5. Physical Property Theft	<b>50</b>
	Incidents																								
1. Termination	<b>375</b>																								
2. Resignation	<b>245</b>																								
3. Internal Position Change	<b>55</b>																								
4. Organization M&A Activity	<b>43</b>																								
5. Emerging Financial Problems	<b>33</b>																								
	Incidents																								
1. Went to Work for a Competitor	<b>89</b>																								
2. Disgruntled	<b>57</b>																								
3. Suspicious Foreign Travel	<b>55</b>																								
4. Financial Conflict of Interest	<b>53</b>																								
5. Physical Property Theft	<b>50</b>																								
<b>Top Five Data Exfiltration Methods Observed</b> <table> <tr> <th></th> <th>Incidents</th> </tr> <tr> <td>1. Email</td> <td><b>141</b></td> </tr> <tr> <td>2. Removable Media</td> <td><b>90</b></td> </tr> <tr> <td>3. Paper</td> <td><b>80</b></td> </tr> <tr> <td>4. Web</td> <td><b>61</b></td> </tr> <tr> <td>5. Verbal</td> <td><b>42</b></td> </tr> </table>		Incidents	1. Email	<b>141</b>	2. Removable Media	<b>90</b>	3. Paper	<b>80</b>	4. Web	<b>61</b>	5. Verbal	<b>42</b>	<b>Top Five Sabotage Methods Observed</b> <table> <tr> <th></th> <th>Incidents</th> </tr> <tr> <td>1. Critical Data Modified</td> <td><b>135</b></td> </tr> <tr> <td>2. Critical Data Deleted</td> <td><b>91</b></td> </tr> <tr> <td>3. Denial of Service Attack—General</td> <td><b>79</b></td> </tr> <tr> <td>4. Malicious Code Inserted</td> <td><b>42</b></td> </tr> <tr> <td>5. Social Engineering</td> <td><b>35</b></td> </tr> </table>		Incidents	1. Critical Data Modified	<b>135</b>	2. Critical Data Deleted	<b>91</b>	3. Denial of Service Attack—General	<b>79</b>	4. Malicious Code Inserted	<b>42</b>	5. Social Engineering	<b>35</b>
	Incidents																								
1. Email	<b>141</b>																								
2. Removable Media	<b>90</b>																								
3. Paper	<b>80</b>																								
4. Web	<b>61</b>																								
5. Verbal	<b>42</b>																								
	Incidents																								
1. Critical Data Modified	<b>135</b>																								
2. Critical Data Deleted	<b>91</b>																								
3. Denial of Service Attack—General	<b>79</b>																								
4. Malicious Code Inserted	<b>42</b>																								
5. Social Engineering	<b>35</b>																								

Figure 55: Data points from CERT Common Sense Guide 7th Ed.

### Best practices at a glance

As stated, this section is to serve as an overview of the frameworks, therefore the 22 best practise recommendations will only be introduced. Expansion of relevant best practices will be done in sections regarding the building of the course, see section 6. The 22 best practises are:

1. Know and protect critical assets
2. Formalise an insider risk management program
3. Document and enforce administrative controls
4. Monitor and respond to suspicious behaviour from hire to retire
5. Manage negative work environment issues
6. Include insider risk in enterprise risk assessments
7. Be vigilant about social media exposure
8. Structure work to minimise stress and mistakes
9. Embed insider threat awareness in recurring training
10. Enforce strict password and account management
11. Govern privileged user access
12. Correlate multi source monitoring data to monitor employee actions
13. Control and monitor remote- and mobile- access
14. Baseline normal user- and network- behaviour
15. Enforce least privilege and separation of duties



16. Set explicit security clauses in cloud contracts
17. Institutionalise change control
18. Implement secure backup and recovery processes
19. Mitigate unauthorized data exfiltration
20. Implement comprehensive termination procedures
21. Align workforce incentives with organisational goals
22. Systematically learn from prior incidents

Each practice chapter follows a consistent blueprint: stakeholder graphic, implementation challenges, “quick wins” versus “high-impact” solutions, metrics, mappings to external standards and illustrative case studies[13, p. 9].

While increasingly tactical, the recommendations provided by the CSG are still relatively executive in nature. For example, best practice nr. 10 **Implement Strict Password and Account Management Policies and Practices** has a few recommendations, including: *“Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.”*[13, p. 76]. While that recommendation might ring true, it is arguably not a recommendation that is straightforward to implement based on what the CSG provides. In an effort not to misrepresent the recommendations, Figure 56 shows the list of recommendations which apply to all organizations, for best practice nr. 10.

### Quick Wins and High-Impact Solutions

#### All Organizations

The recommendations in this subsection apply to all organizations.

- ✓ Establish account management policies and procedures for all accounts created on all information systems. These policies should address how accounts are created, reviewed, and terminated. The policy should also address who authorizes the account and what data they can access.
- ✓ Perform audits of account creation and password changes by system administrators. The account management process should require that users request new accounts via a help desk ticket. (Members of the help desk should not be able to create accounts.) Confirm the legitimacy of requests to reset passwords or create accounts by correlating such requests with help desk logs.
- ✓ Define password requirements and train users to create strong passwords. Some systems can tolerate long passwords. Encourage users to use passwords that include proper punctuation and capitalization, thereby increasing password strength and making it more memorable to the user.
- ✓ Security training should include instruction about how workforce members can block visual access to others as they type their passwords.
- ✓ Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.

Figure 56: Quick wins and high impact solutions for recommendation nr. 10[13]

So far the section on insider threat frameworks has moved from an executive level strategic point of view towards a tactical view. The following framework **Insider Attack Matrix**, pushes onward by arranging insider techniques along a dedicate kill chain, moving from static best practice recommendations to into a sequenced map of attacker behavior.

### A.1.3 G-Research Insider Attack Matrix

The Insider Attack Matrix is presented by G-research, a leading European quantitative finance research firm [14]. Their research on insider threats stem from their interest in protecting valuable intellectual property. With an outset in a CERT Guide to Insider Threats and 50 separate well documented insider incidents, the Insider Attack Matrix presents itself as both a matrix and as an expansion of the Lockheed Martin Cyber Kill Chain, see Figure 57. It is important to note that the Insider Attack Matrix implicitly focuses on *intentional insider threat* as introduced with CISA's definitions in subsection 2.1.

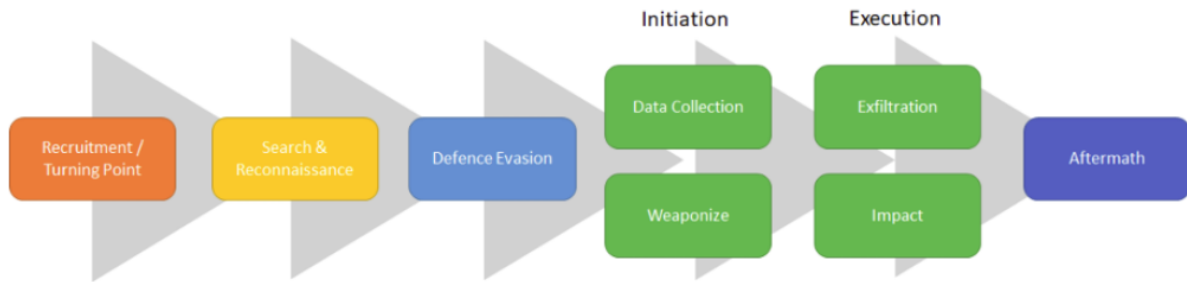


Figure 57: Insider Killchain[14]

With Figure 57 the aim is to demonstrate how insider attacks typically progress through various phases. The initial phase, **Recruitment/Turning Point**, points to that an insider might either be malicious from the start, or have been turned by a major event - as stated previously, this implicitly narrows the Insider Attack Matrix's focus to intentional insider threats. Subsequently, an insider attack typically moves through the **Search/Reconnaissance** and **Defence Evasion** phases, where the insider searches for valuable access or data and attempts to hide their actions. The **Initiation** phase is a critical point, it is here the attacker does *something* that could harm the company, either data collection (eg. gathering technical documentation) or weaponizing (eg. installing malware). **Execution**, as implied, is where data is actively exfiltrated or the impact of the weaponization is felt. According to the article, this phase is where most organizations focus their efforts detection and prevention through monitoring, backups and incident response plans. Lastly, the **Aftermath** phase is where the attacker usually has succeeded in exploiting the organization. For the organization, reaching this phase in an insider incident usually implies remediation, prosecution and retrospective analysis of the events[14]. Notably, a bleak comment is presented towards the end of the article: "[...] a large percentage of attacks studied to produce this Kill Chain were not detected until this point [at Aftermath phase, red.]"[14].

Expanding on the established, the article takes a step towards tactical implementation with the matrix they produce, by viewing each phase through the lens of **Tactics** and **Techniques** as understood by the MITRE ATT&CK framework (for more in MITRE see subsubsection 2.2.3). With the breakdown of the kill chain into Tactics and Techniques, the matrix provides defenders with actionable steps to take in order to set up detections at any phase of the insider kill chain. A small version of the matrix is shown in Figure 58.

## Matrix

Kill Chain / Tactics	Recruitment /Turning point	Search /Reconnaissance	Defense Evasion	Initiate		Execution /Action	Impact	Aftermath
				Data Collection	Weaponise	Exfiltrate		
Techniques	Malicious Recruitment	Searching through data not application to job	Deleting Logs/IT evidence	Unauthorised access <ul style="list-style-type: none"> <li>Accessing services with correct creds (but shouldn't have access)</li> <li>Password theft</li> </ul>	Download malware	Leveraging remote access	Deletion of data	Gloating
	Make Contact	Contacting people for info/help not applicable to job	Destroying physical evidence	Coercing contacts	Writing malicious code	External technical exfiltration <ul style="list-style-type: none"> <li>Dropbox</li> <li>Email</li> <li>USB/CD</li> </ul>	Editing critical data	Frivolous purchases
	Exposed to temptation (Unreviewed/regulated processes)	Applying for promotions/job changes	Impersonation/Masquerading	Keylogger	Unauthorised access	External physical exfiltration <ul style="list-style-type: none"> <li>Printing large amounts</li> <li>Taking photos</li> <li>Memorising</li> <li>Writing down</li> </ul>	Attack availability	Last minute /unannounced holidays/travel?
	Surprising Change in Behaviour	Suspicious requests not compliant with company policy	Requesting staff overlook responsibilities	Collecting data in a centralized place	Installing malicious code		Transfer of money	Surprise Resignation
	Unprofessional Behaviour	Malicious unapproved access to other systems	Defensive Collusion	Authorised Access	Testing Malicious Code		Extortion	Refuses promotion /team transfer
	Resignation/ Surprise Resignation	Online research on how to build malicious code	Exploit Turbulence		Privilege Escalation		Public release of data	Created a competing company
	Disgruntlement				Abuse of process			Attempt to steal customers from the company
	Dismissal							Confession
	Change in personal life							

Figure 58: Insider Attack Matrix[14]

As addendum to the matrix, the article supplies examples, indicators of compromise and citations/sources for each technique. For example for Defence Evasion/Deleting logs/IT evidence the matrix provides the following entry, shown in Figure 59:

### Defence Evasion

Techniques	Examples / Procedures	Citation
Deleting logs/IT evidence	Deleting temp files on Company Computer (e.g. BYOD laptop)	Cert Guide to Insider Threats: Theft of IP 1
	Deleting bash logs	Cert Guide to Insider Threats: Miscellaneous 6
	Deleting database logs	Cert Guide to Insider Threats: Fraud 11
	Reformat backups	Cert Guide to Insider Threats: Fraud 11

Figure 59: A cropped version of Defence Evasion technique examples[14]

The matrix's addition of examples/procedures to each technique found in a given phase, allows - as stated previously - defenders the possibility of setting up detections and preventive controls for any phase in the insider attack kill chain. In the quest towards an ever more tactically view of insider threats we will next explore

MITRE's Insider Threat TTP Knowledge Base, which allows for encoding of techniques for automation and analytics.



## A.2 The Green-"seen" Chart

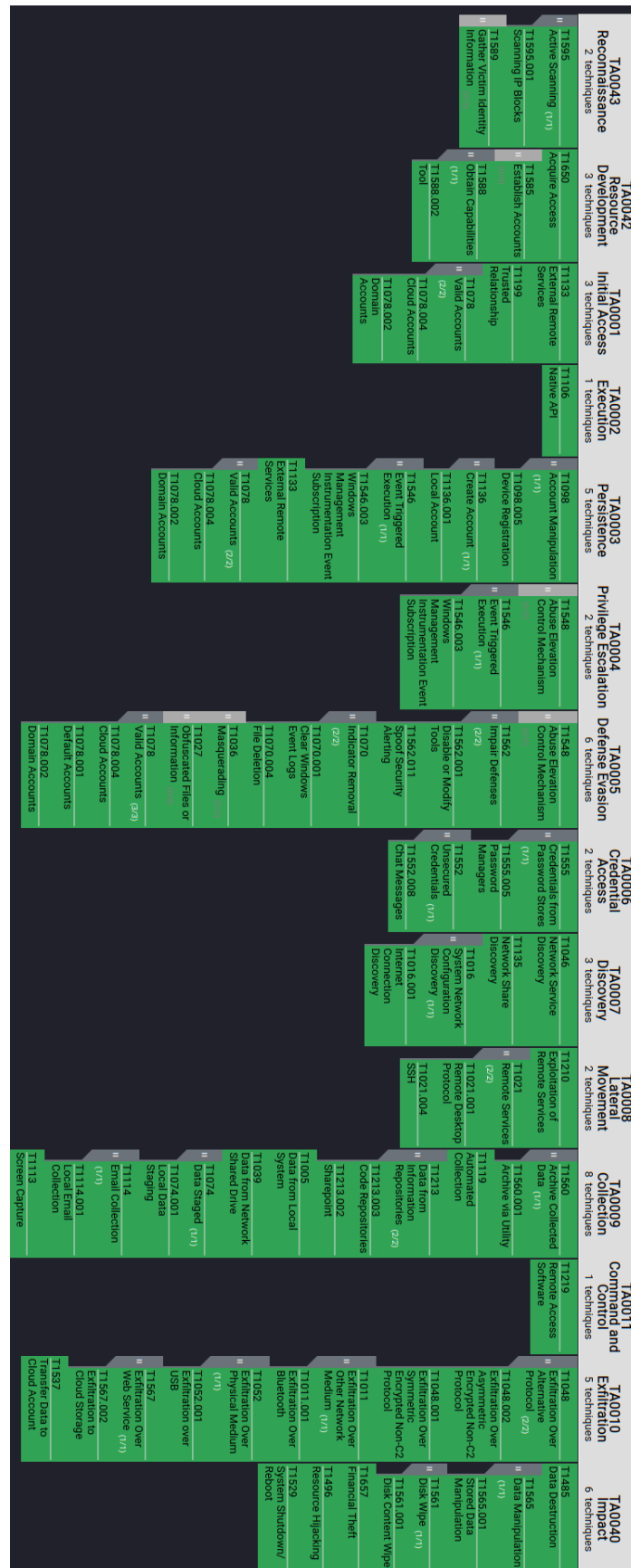


Figure 60: The green = "seen"-chart for insiders [16]

### **A.3 Work Role - Insider Threat Analysis**

**PROTECTION and  
DEFENSE (PD)**

**Insider Threat Analysis (PD-WRL-005):** Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations.

OPM Code: TBD

v2.0.0 TKS ID	v2.0.0 TKS Description	Task to Knowledge & Skill Alignments
K0635	Knowledge of decryption	
K0636	Knowledge of decryption tools and techniques	
K0637	Knowledge of data repositories	
K0656	Knowledge of network collection tools and techniques	
K0657	Knowledge of network collection policies and procedures	
K0674	Knowledge of computer networking protocols	
K0675	Knowledge of risk management processes	
K0676	Knowledge of cybersecurity laws and regulations	
K0677	Knowledge of cybersecurity policies and procedures	
K0678	Knowledge of privacy laws and regulations	
K0679	Knowledge of privacy policies and procedures	
K0682	Knowledge of cybersecurity threats	
K0683	Knowledge of cybersecurity vulnerabilities	
K0684	Knowledge of cybersecurity threat characteristics	
K0689	Knowledge of network infrastructure principles and practices	
K0707	Knowledge of database systems and software	
K0710	Knowledge of enterprise cybersecurity architecture principles and practices	
K0721	Knowledge of risk management principles and practices	
K0734	Knowledge of Risk Management Framework (RMF) requirements	
K0735	Knowledge of risk management models and frameworks	
K0751	Knowledge of system threats	
K0752	Knowledge of system vulnerabilities	
K0778	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0784	Knowledge of insider threat laws and regulations	
K0785	Knowledge of insider threat tools and techniques	
K0802	Knowledge of chain of custody policies and procedures	
K0862	Knowledge of data remediation tools and techniques	
K0870	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Knowledge of enterprise architecture (EA) principles and practices	
K0909	Knowledge of abnormal physical and physiological behaviors	
K1014	Knowledge of network security principles and practices	
K1023	Knowledge of network exploitation tools and techniques	
K1031	Knowledge of risk mitigation tools and techniques	
K1085	Knowledge of exploitation tools and techniques	
K1096	Knowledge of data analysis tools and techniques	
K1151	Knowledge of digital evidence cataloging tools and techniques	
K1152	Knowledge of digital evidence extraction tools and techniques	
K1154	Knowledge of digital evidence packaging tools and techniques	
K1155	Knowledge of digital evidence preservation tools and techniques	
K1180	Knowledge of organizational cybersecurity goals and objectives	
K1188	Knowledge of organizational policies and procedures	
K1197	Knowledge of priority intelligence requirements	
K1209	Knowledge of risk mitigation principles and practices	
K1241	Knowledge of cultural, political, and organizational assets	
K1242	Knowledge of cybersecurity review processes and procedures	
K1243	Knowledge of cybersecurity threat remediation principles and practices	
K1244	Knowledge of cybersecurity tools and techniques	
K1245	Knowledge of data exfiltration tools and techniques	
K1246	Knowledge of data handling tools and techniques	
K1247	Knowledge of data monitoring tools and techniques	
K1248	Knowledge of digital and physical security vulnerabilities	
K1249	Knowledge of digital and physical security vulnerability remediation principles and practices	
K1250	Knowledge of external organization roles and responsibilities	
K1251	Knowledge of external referrals policies and procedures	
K1252	Knowledge of high value asset characteristics	
K1254	Knowledge of insider threat hub policies and procedures	
K1255	Knowledge of insider threat hub operations	
K1256	Knowledge of insider threat operational indicators	
K1257	Knowledge of insider threat policies and procedures	
K1258	Knowledge of insider threat tactics	
K1259	Knowledge of insider threat targets	
K1260	Knowledge of intelligence laws and regulations	
K1261	Knowledge of known insider attacks	
K1262	Knowledge of network endpoints	
K1263	Knowledge of notification policies and procedures	
K1265	Knowledge of organizational objectives, resources, and capabilities	
K1267	Knowledge of previously referred potential insider threats	
K1268	Knowledge of risk reduction metrics	
K1269	Knowledge of security information and event management (SIEM) tools and techniques	
K1270	Knowledge of suspicious activity response processes	
K1271	Knowledge of system alert policies and procedures	
K1272	Knowledge of system components	
K1273	Knowledge of threat investigation policies and procedures	
K1274	Knowledge of threat modeling tools and techniques	
K1275	Knowledge of User Activity Monitoring (UAM) tools and techniques	
S0378	Skill in decrypting information	
S0391	Skill in creating technical documentation	
S0442	Skill in collecting network data	
S0477	Skill in identifying anomalous activity	
S0540	Skill in identifying network threats	
S0558	Skill in developing algorithms	
S0559	Skill in performing data structure analysis	
S0579	Skill in preparing reports	
S0588	Skill in performing threat modeling	
S0610	Skill in communicating effectively	
S0688	Skill in performing network data analysis	
S0690	Skill in performing midpoint collection data analysis	
S0728	Skill in preparing briefings	



S0748	Skill in querying data	
S0791	Skill in presenting to an audience	
S0817	Skill in building internal and external relationships	
S0821	Skill in collaborating with internal and external stakeholders	
S0848	Skill in performing behavioral analysis	
S0854	Skill in performing data analysis	
S0866	Skill in performing log file analysis	
S0874	Skill in performing network traffic analysis	
S0890	Skill in performing threat analysis	
S0896	Skill in recognizing behavioral patterns	
S0900	Skill in analyzing information from multiple sources	
S0902	Skill in building relationships remotely and in person	
S0904	Skill in correlating data from multiple tools	
S0905	Skill in determining what information may helpful to a specific audience	
S0906	Skill in identifying insider risk security gaps	
S0907	Skill in identifying insider threats	
S0908	Skill in determining the importance of assets	
S0909	Skill in integrating information from multiple sources	
S0910	Skill in performing cyberintelligence data analysis	
S0911	Skill in performing data queries	
S0912	Skill in performing human behavioral analysis	
S0913	Skill in performing link analysis	
S0916	Skill in recognizing recurring threat incidents	
T1056	Acquire resources to support cybersecurity program goals and objectives	K1180: Knowledge of organizational cybersecurity goals and objectives K1209: Knowledge of risk mitigation principles and practices K1268: Knowledge of risk reduction metrics
T1057	Conduct an effective enterprise continuity of operations program	K1180: Knowledge of organizational cybersecurity goals and objectives K1188: Knowledge of organizational policies and procedures K1268: Knowledge of risk reduction metrics
T1062	Contribute insider threat expertise to organizational cybersecurity awareness program	K1262: Knowledge of network endpoints K1272: Knowledge of system components K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques S0911: Skill in performing data queries K0633: Knowledge of decryption K0636: Knowledge of decryption tools and techniques K0637: Knowledge of data repositories K0656: Knowledge of network collection tools and techniques K0657: Knowledge of network collection policies and procedures K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1258: Knowledge of insider threat tactics K1261: Knowledge of known insider attacks S0378: Skill in decrypting information S0442: Skill in collecting network data S0912: Skill in performing human behavioral analysis
T1084	Identify anomalous network activity	S0866: Skill in performing log file analysis S0874: Skill in performing network traffic analysis
T1085	Identify potential threats to network resources	K0675: Knowledge of risk management processes K0721: Knowledge of risk management principles and practices K0734: Knowledge of Risk Management Framework (RMF) requirements K0735: Knowledge of risk management models and frameworks K1031: Knowledge of risk mitigation tools and techniques
T1160	Develop risk mitigation strategies	K0675: Knowledge of risk management processes K0721: Knowledge of risk management principles and practices K0734: Knowledge of Risk Management Framework (RMF) requirements K0735: Knowledge of risk management models and frameworks K1031: Knowledge of risk mitigation tools and techniques
T1162	Recommend security changes to systems and system components	K1180: Knowledge of organizational cybersecurity goals and objectives K1209: Knowledge of risk mitigation principles and practices K1268: Knowledge of risk reduction metrics
T1227	Manage cybersecurity budget, staffing, and contracting	K0675: Knowledge of risk management processes K0721: Knowledge of risk management principles and practices K0734: Knowledge of Risk Management Framework (RMF) requirements K0735: Knowledge of risk management models and frameworks K1031: Knowledge of risk mitigation tools and techniques
T1266	Recommend risk mitigation strategies	K1115: Knowledge of Chain of Custody (CoC) processes and procedures K1151: Knowledge of digital evidence cataloging tools and techniques K1152: Knowledge of digital evidence extraction tools and techniques K1154: Knowledge of digital evidence packaging tools and techniques K1155: Knowledge of digital evidence preservation tools and techniques K1246: Knowledge of data handling tools and techniques K1247: Knowledge of data monitoring tools and techniques K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques
T1324	Process digital evidence	K1115: Knowledge of Chain of Custody (CoC) processes and procedures K1151: Knowledge of digital evidence cataloging tools and techniques K1152: Knowledge of digital evidence extraction tools and techniques K1154: Knowledge of digital evidence packaging tools and techniques K1155: Knowledge of digital evidence preservation tools and techniques K1246: Knowledge of data handling tools and techniques K1247: Knowledge of data monitoring tools and techniques K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques
T1325	Document digital evidence	K0682: Knowledge of cybersecurity threats K0683: Knowledge of cybersecurity vulnerabilities K0684: Knowledge of cybersecurity threat characteristics K0751: Knowledge of system threats K0752: Knowledge of system vulnerabilities K1139: Knowledge of cybersecurity threats and vulnerabilities S0848: Skill in performing behavioral analysis S0896: Skill in recognizing behavioral patterns S0912: Skill in performing human behavioral analysis
T1439	Assess the behavior of individual victims, witnesses, or suspects during cybersecurity investigations	

		K1115: Knowledge of Chain of Custody (CoC) processes and procedures K1151: Knowledge of digital evidence cataloging tools and techniques K1152: Knowledge of digital evidence extraction tools and techniques K1154: Knowledge of digital evidence packaging tools and techniques K1155: Knowledge of digital evidence preservation tools and techniques K1246: Knowledge of data handling tools and techniques K1247: Knowledge of data monitoring tools and techniques K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques
T1510	Preserve digital evidence	
T1592	Conduct cybersecurity reviews	K1242: Knowledge of cybersecurity review processes and procedures
T1690	Identify exploitable technical or operational vulnerabilities	K1248: Knowledge of digital and physical security vulnerabilities
		K0674: Knowledge of computer networking protocols K0682: Knowledge of cybersecurity threats K0683: Knowledge of cybersecurity vulnerabilities K0684: Knowledge of cybersecurity threat characteristics K0707: Knowledge of database systems and software K0751: Knowledge of system threats K0752: Knowledge of system vulnerabilities K0862: Knowledge of data remediation tools and techniques K1014: Knowledge of network security principles and practices K1243: Knowledge of cybersecurity threat remediation principles and practices K1274: Knowledge of threat modeling tools and techniques
T1712	Recommend potential courses of action	S0540: Skill in identifying network threats
		K0635: Knowledge of decryption K0636: Knowledge of decryption tools and techniques K0637: Knowledge of data repositories K0656: Knowledge of network collection tools and techniques K0657: Knowledge of network collection policies and procedures K1259: Knowledge of insider threat targets
T1737	Develop intelligence collection strategies	S0378: Skill in decrypting information S0442: Skill in collecting network data
		K0635: Knowledge of decryption K0636: Knowledge of decryption tools and techniques K0637: Knowledge of data repositories K0656: Knowledge of network collection tools and techniques K0657: Knowledge of network collection policies and procedures K1259: Knowledge of insider threat targets
T1743	Identify information collection gaps	S0442: Skill in collecting network data
		K1254: Knowledge of insider threat hub policies and procedures K1263: Knowledge of notification policies and procedures K1265: Knowledge of organizational objectives, resources, and capabilities S0559: Skill in performing data structure analysis S0579: Skill in preparing reports S0728: Skill in preparing briefings S0791: Skill in presenting to an audience
T1799	Notify appropriate personnel of imminent hostile intentions or activities	S0690: Skill in performing midpoint collection data analysis
T1801	Determine validity and relevance of information	S0854: Skill in performing data analysis
		K1096: Knowledge of data analysis tools and techniques K1271: Knowledge of system alert policies and procedures
T1969	Document system alerts	S0690: Skill in performing midpoint collection data analysis S0854: Skill in performing data analysis
		K1271: Knowledge of system alert policies and procedures
T1970	Escalate system alerts that may indicate risks	S0690: Skill in performing midpoint collection data analysis S0854: Skill in performing data analysis
		K1250: Knowledge of external organization roles and responsibilities
T1971	Disseminate anomalous activity reports to the insider threat hub	S0817: Skill in building internal and external relationships S0902: Skill in building relationships remotely and in person
		K1241: Knowledge of cultural, political, and organizational assets
T1973	Conduct independent comprehensive assessments of target-specific information	S0902: Skill in building relationships remotely and in person S0908: Skill in determining the importance of assets
		K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1248: Knowledge of digital and physical security vulnerabilities K1249: Knowledge of digital and physical security vulnerability remediation principles and practices K1257: Knowledge of insider threat policies and procedures K1258: Knowledge of insider threat tactics
T1974	Conduct insider threat risk assessments	S0910: Skill in performing cyberintelligence data analysis
		K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1248: Knowledge of digital and physical security vulnerabilities K1249: Knowledge of digital and physical security vulnerability remediation principles and practices K1257: Knowledge of insider threat policies and procedures K1258: Knowledge of insider threat tactics
T1975	Prepare insider threat briefings	S0910: Skill in performing cyberintelligence data analysis
		S0690: Skill in performing midpoint collection data analysis S0854: Skill in performing data analysis
T1976	Recommend risk mitigation courses of action (CoA)	S0906: Skill in identifying insider risk security gaps
		S0900: Skill in analyzing information from multiple sources
T1977	Coordinate with internal and external incident management partners across jurisdictions	S0909: Skill in integrating information from multiple sources
		K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1258: Knowledge of insider threat tactics K1267: Knowledge of previously referred potential insider threats
T1978	Recommend improvements to insider threat detection processes	S0690: Skill in performing midpoint collection data analysis S0854: Skill in performing data analysis

T1979	Collect digital evidence that meets priority intelligence requirements	K0676: Knowledge of cybersecurity laws and regulations K0677: Knowledge of cybersecurity policies and procedures K0678: Knowledge of privacy laws and regulations K0679: Knowledge of privacy policies and procedures K1197: Knowledge of priority intelligence requirements K1260: Knowledge of intelligence laws and regulations
T1980	Develop digital evidence reports for internal and external partners	K0676: Knowledge of cybersecurity laws and regulations K0677: Knowledge of cybersecurity policies and procedures K0678: Knowledge of privacy laws and regulations K0679: Knowledge of privacy policies and procedures K1197: Knowledge of priority intelligence requirements K1260: Knowledge of intelligence laws and regulations  S0559: Skill in performing data structure analysis S0579: Skill in preparing reports S0610: Skill in communicating effectively S0728: Skill in preparing briefings S0791: Skill in presenting to an audience S0817: Skill in building internal and external relationships
T1981	Develop elicitation indicators	K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1257: Knowledge of insider threat policies and procedures K1258: Knowledge of insider threat tactics  S0912: Skill in performing human behavioral analysis
T1982	Identify high value assets	K0689: Knowledge of network infrastructure principles and practices K0710: Knowledge of enterprise cybersecurity architecture principles and practices K0778: Knowledge of enterprise information technology (IT) architecture principles and practices K0870: Knowledge of enterprise architecture (EA) reference models and frameworks K0871: Knowledge of enterprise architecture (EA) principles and practices K1252: Knowledge of high value asset characteristics
T1983	Identify potential insider threats	S0690: Skill in performing midpoint collection data analysis S0854: Skill in performing data analysis
T1985	Identify imminent or hostile intentions or activities	K1254: Knowledge of insider threat hub policies and procedures K1261: Knowledge of known insider attacks K1265: Knowledge of organizational objectives, resources, and capabilities
T1986	Develop a continuously updated overview of an incident throughout the incident's life cycle	S0900: Skill in analyzing information from multiple sources S0909: Skill in integrating information from multiple sources
T1987	Develop insider threat cyber operations indicators	K1256: Knowledge of insider threat operational indicators  S0748: Skill in querying data S0900: Skill in analyzing information from multiple sources S0909: Skill in integrating information from multiple sources
T1988	Integrate information from cyber resources, internal partners, and external partners	S0900: Skill in analyzing information from multiple sources S0909: Skill in integrating information from multiple sources
T1989	Advise insider threat hub inquiries	K1255: Knowledge of insider threat hub operations  S0817: Skill in building internal and external relationships S0905: Skill in determining what information may be helpful to a specific audience S0907: Skill in identifying insider threats
T1990	Conduct cybersecurity insider threat inquiries	K1244: Knowledge of cybersecurity tools and techniques K1269: Knowledge of security information and event management (SIEM) tools and techniques  S0748: Skill in querying data S0904: Skill in correlating data from multiple tools S0913: Skill in performing link analysis
T1991	Deliver all-source cyber operations and intelligence indications and warnings	K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1248: Knowledge of digital and physical security vulnerabilities K1249: Knowledge of digital and physical security vulnerability remediation principles and practices K1257: Knowledge of insider threat policies and procedures K1258: Knowledge of insider threat tactics
T1992	Interpret network activity for intelligence value	S0910: Skill in performing cyberintelligence data analysis
T1993	Monitor network activity for vulnerabilities	K1248: Knowledge of digital and physical security vulnerabilities K1245: Knowledge of data exfiltration tools and techniques K1248: Knowledge of digital and physical security vulnerabilities
T1994	Identify potential insider risks to networks	S0874: Skill in performing network traffic analysis K0635: Knowledge of decryption K0636: Knowledge of decryption tools and techniques K0637: Knowledge of data repositories K0656: Knowledge of network collection tools and techniques K0657: Knowledge of network collection policies and procedures K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1261: Knowledge of known insider attacks  S0378: Skill in decrypting information S0442: Skill in collecting network data S0890: Skill in performing threat analysis S0912: Skill in performing human behavioral analysis
T1995	Document potential insider risks to networks	S0559: Skill in performing data structure analysis S0579: Skill in preparing reports S0728: Skill in preparing briefings S0791: Skill in presenting to an audience
T1996	Report network vulnerabilities	K1248: Knowledge of digital and physical security vulnerabilities  S0558: Skill in developing algorithms S0559: Skill in performing data structure analysis S0579: Skill in preparing reports S0728: Skill in preparing briefings S0791: Skill in presenting to an audience

T1997	Develop insider threat investigation plans	K0909: Knowledge of abnormal physical and physiological behaviors K1257: Knowledge of insider threat policies and procedures K1270: Knowledge of suspicious activity response processes K1273: Knowledge of threat investigation policies and procedures  S0477: Skill in identifying anomalous activity
T1998	Investigate alleged insider threat cybersecurity policy violations	K0909: Knowledge of abnormal physical and physiological behaviors K1257: Knowledge of insider threat policies and procedures K1270: Knowledge of suspicious activity response processes K1273: Knowledge of threat investigation policies and procedures  S0477: Skill in identifying anomalous activity
T1999	Refer cases on active insider threat activities to law enforcement investigators	K0674: Knowledge of computer networking protocols K0682: Knowledge of cybersecurity threats K0683: Knowledge of cybersecurity vulnerabilities K0684: Knowledge of cybersecurity threat characteristics K0751: Knowledge of system threats K0752: Knowledge of system vulnerabilities K1014: Knowledge of network security principles and practices K1251: Knowledge of external referrals policies and procedures K1274: Knowledge of threat modeling tools and techniques  S0540: Skill in identifying network threats S0588: Skill in performing threat modeling S0688: Skill in performing network data analysis K1180: Knowledge of organizational cybersecurity goals and objectives K1188: Knowledge of organizational policies and procedures K1268: Knowledge of risk reduction metrics  S0559: Skill in performing data structure analysis S0579: Skill in preparing reports S0728: Skill in preparing briefings S0791: Skill in presenting to an audience S0817: Skill in building internal and external relationships S0821: Skill in collaborating with internal and external stakeholders
T2001	Establish an insider threat risk management assessment program	K0721: Knowledge of risk management principles and practices K1248: Knowledge of digital and physical security vulnerabilities
T2003	Evaluate organizational insider risk response capabilities	K0909: Knowledge of abnormal physical and physiological behaviors K0944: K1252: Knowledge of high value asset characteristics  S0391: Skill in creating technical documentation S0477: Skill in identifying anomalous activity S0695: S0751: S0848: Skill in performing behavioral analysis S0866: Skill in performing log file analysis S0910: Skill in performing cyberintelligence data analysis
T2004	Document insider threat information sources	K0784: Knowledge of insider threat laws and regulations K0785: Knowledge of insider threat tools and techniques K1248: Knowledge of digital and physical security vulnerabilities K1249: Knowledge of digital and physical security vulnerability remediation principles and practices K1257: Knowledge of insider threat policies and procedures K1258: Knowledge of insider threat tactics  S0910: Skill in performing cyberintelligence data analysis
T2005	Conduct insider threat studies	K1023: Knowledge of network exploitation tools and techniques K1085: Knowledge of exploitation tools and techniques
T2006	Identify potential targets for exploitation	K0689: Knowledge of network infrastructure principles and practices K0710: Knowledge of enterprise cybersecurity architecture principles and practices K0778: Knowledge of enterprise information technology (IT) architecture principles and practices K0870: Knowledge of enterprise architecture (EA) reference models and frameworks K0871: Knowledge of enterprise architecture (EA) principles and practices K1023: Knowledge of network exploitation tools and techniques K1085: Knowledge of exploitation tools and techniques
T2007	Analyze potential targets for exploitation	K1262: Knowledge of network endpoints K1272: Knowledge of system components K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques  S0911: Skill in performing data queries
T2009	Develop insider threat targets	K1262: Knowledge of network endpoints K1272: Knowledge of system components K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques  S0911: Skill in performing data queries S0916: Skill in recognizing recurring threat incidents
T2010	Maintain User Activity Monitoring (UAM) tools	K1262: Knowledge of network endpoints K1272: Knowledge of system components K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques  S0911: Skill in performing data queries
T2011	Monitor the output from User Activity Monitoring (UAM) tools	K1262: Knowledge of network endpoints K1272: Knowledge of system components K1275: Knowledge of User Activity Monitoring (UAM) tools and techniques  S0911: Skill in performing data queries

## A.4 Workshop and Debrief Notes

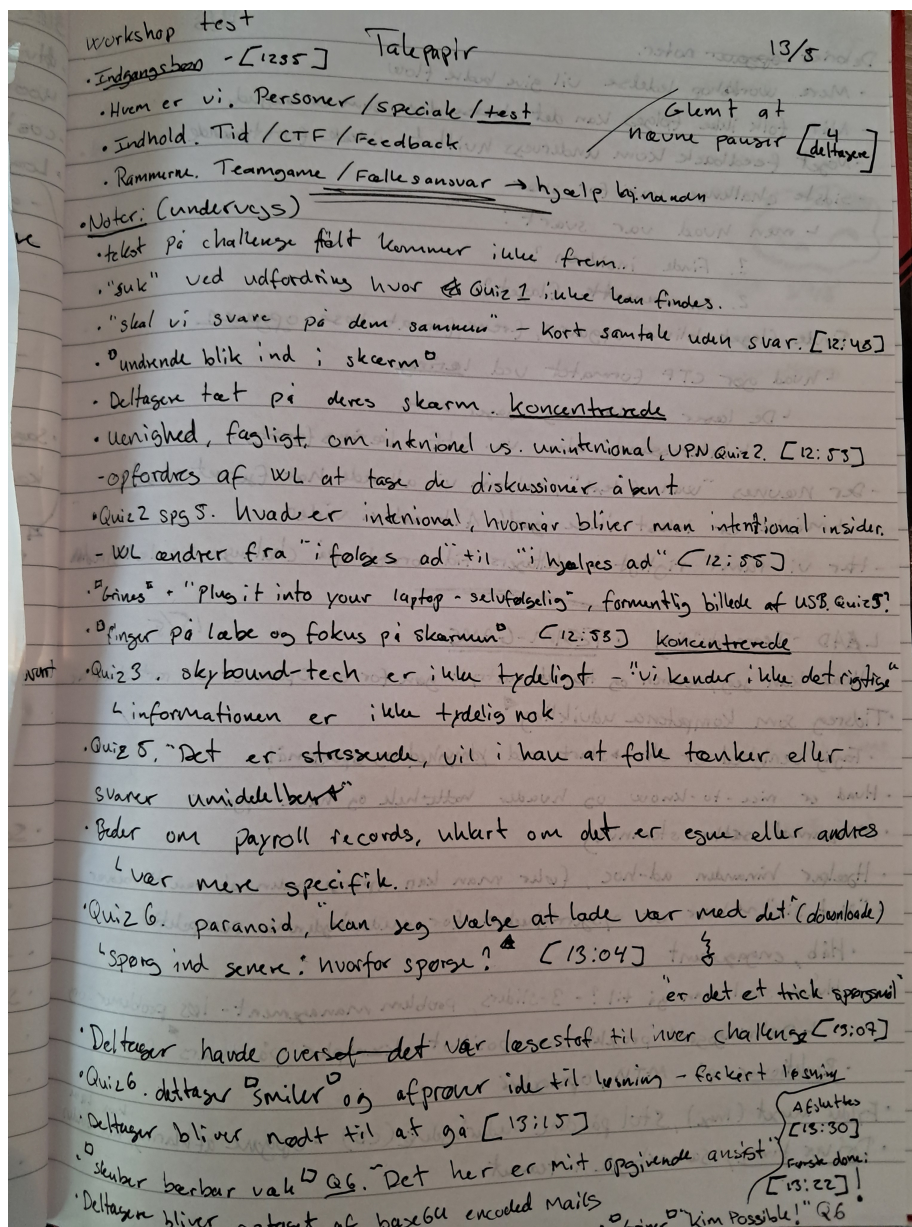


Figure 61: Workshop observation notes

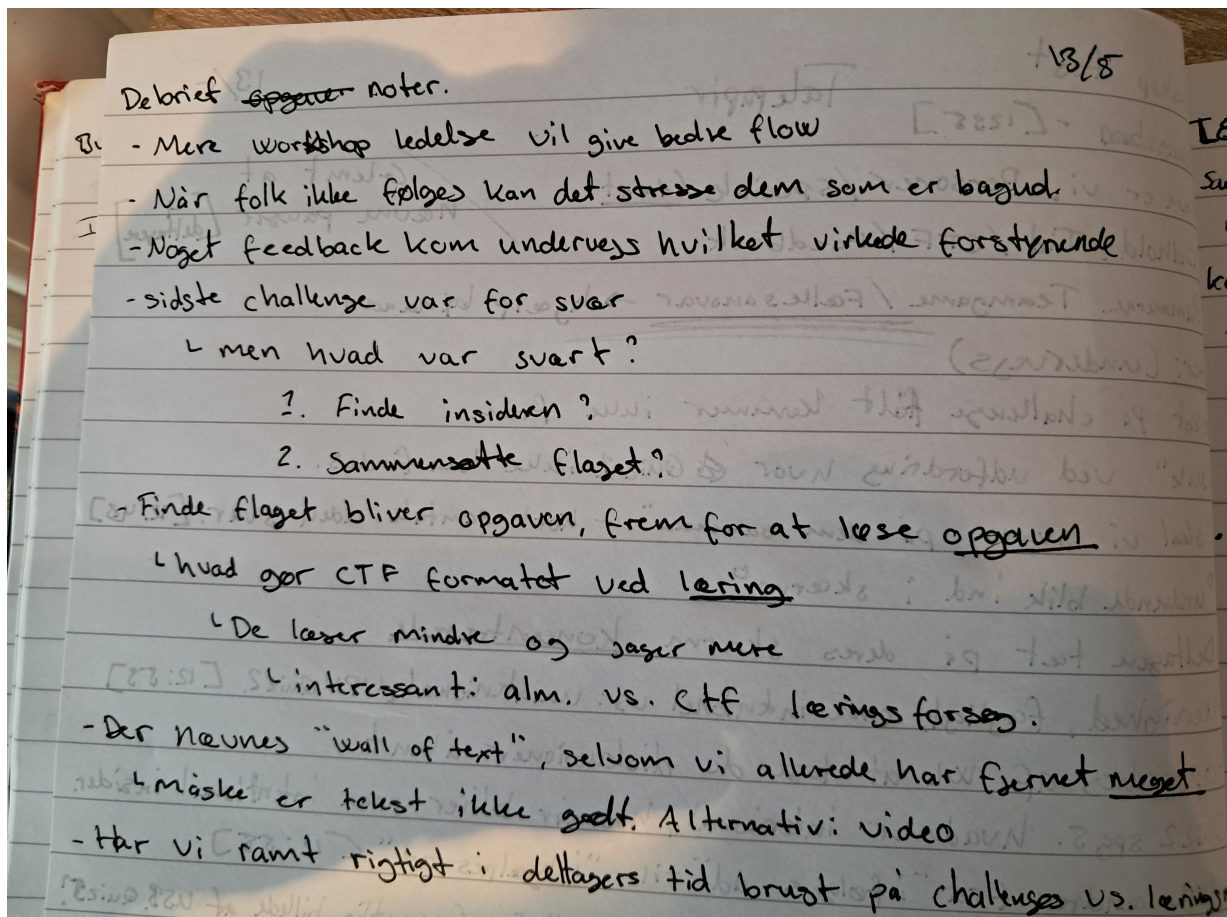


Figure 62: Debrief notes post workshop

## A.5 Interview transcription with Kristian Larsen (not analyzed or utilized further)

Transcript May 23, 2025, 1:07PM

Nikolaj Jørgensen started transcription

Nick Büchmann Blume 0:03 Oh, so like, I couldn't understand.

Nikolaj Jørgensen 0:07 Sure.

Nick Büchmann Blume 0:08 Yeah.

Nikolaj Jørgensen 0:09 So First off, Christian, are you OK with us recording and transcribing this interview?

Kristian Larsen 0:16 Yes.

Nikolaj Jørgensen 0:17 Awesome. And in the report, do you want to remain anonymous or can we use your name?

Kristian Larsen 0:23 You can use my name.

Nikolaj Jørgensen 0:25 Cool. We're going to talk about 3, like major topics, and I've sent you some of the questions that I thought of while writing these topics. But if we don't touch on all the questions, that's OK as well. The first topic here that we would like your thoughts on are what you see as necessary for someone who is a cybersecurity novice to know about insider threats.

Kristian Larsen 0:53 No, that is a a broad question.

Nikolaj Jørgensen 0:56 It is.

Kristian Larsen 0:58 And I think it it's important that you have like some kind of base baseline to talk about. To base the discussion on when you're talking about insiders, if you look at the like a company case. I think it's important that you have as a company some kind of case to work with when you're working with insiders in order to like, reflect on like what does an insider actually mean? For my organization.

Nikolaj Jørgensen 1:29 Yeah. So, so in that I.

Kristian Larsen 1:29 That doesn't mean that the sorry.

Nikolaj Jørgensen 1:32 No, please.

Kristian Larsen 1:33 Yeah. So that doesn't mean that you have to like create different types of courses for different organizations. It just means that you need some kind of active learning environment to facilitate decision.

Nikolaj Jørgensen 1:46 Yeah. OK. So so both in. So what I'm hearing you say, and please correct me, but in terms of like having a case, it's also it makes me think at least it's also about for the company who is taking the course for them to know what is actually valuable for us to protect so. What are we and what is our threat landscape look like? Is that kind of what you meant with with the case? Or am I misunderstanding something?

Kristian Larsen 2:13 Yes, to some extent. So if you're looking at at fundamentals in terms of like what is an insider threat, I think it's important that first of all, you need to know the fundamentals before you can actually like of the of the concept of an insider before you can actually start a having. A common language for discussing how do you mitigate the insider threat in your organization?

Nikolaj Jørgensen 2:39 OK. Yeah, so yeah, common language and and understanding of what it is before we can even start to have the conversation. OK. Yeah. OK.

Kristian Larsen 2:46 Yes.

Nikolaj Jørgensen 2:46 That makes sense.

Kristian Larsen 2:47 Yeah.

Nikolaj Jørgensen 2:49 So, and it's no secret that you have a CTF platform. How do you see this sort of learning to to be used in in that like in in the? How can it be used to teach new people about, for example, insider threats so and and here it's important to say that you and we of course know that we are making a course for you, so that shouldn't be like something that's secret. So don't feel like you have to answer it.

Kristian Larsen 3:19 Yeah.

Nikolaj Jørgensen 3:19 Want to make a course like you did, but whatever comes to mind.

Kristian Larsen 3:22 Yeah. Yeah. So the basic idea behind the CTF format is to actually give like active hands on learning environments for different types of tasks. One popular use case for it is for competitions where you want to like measure. If someone has successfully completed a task. But in terms of like the more soft skills. There's like different ways you can use it. It's a super support like the detective parts of the learning process. And one of them is that you actually have to actively engage with the topic that you're working with when

you're working in a CCF style. Format. Most mostly. First of all, because you cannot just. Guess based on a set like multiple choice. But it's especially the hands on part of the CTF format that really makes the big difference in terms of like learning outcome.

Nikolaj Jørgensen 4:37 Yeah, definitely so. So what I'm hearing there is also that this multiple choice thing is actually in your mind, not a part of the CTF concept. Is that is that correctly? Am I hearing you right?

Kristian Larsen 4:54 Not necessarily. Like you can have multiple choice as a part of it if it's like. A. Behind an exercise. So maybe you have to like complete a successful multiple choice in order to get the flag for example, or successfully understand how to complete a task in order to get the flag. And so there's like a lot of different ways you can apply it. But the main idea behind it is, of course, also the gamification part. Why you actually gave me fire the learning process so that it's not just immersive choice, but it's actually something where we can reward finding the right answer and. Getting your desired learning outcome.

Nikolaj Jørgensen 5:41 OK. Yeah, that makes sense. So in terms of, as you know, we are designing this course for insider learning or insider threats. What? What made you think? When we started talking about this project in the 1st place, that insider threats was something that was valuable to make a CTF or a learning course about.

Kristian Larsen 6:07 So this is not something that I can tell you in a recorded interview by, at least in terms of details. But but the main problem is that inside of threads is one of the big issues in the at least Danish corporate life at the moment when we look. At cyber security threats, it's like one of the one of the big ones in terms of like. A financial consequences. And that is why it's important that. Organizations learn about this, and I think it's better to learn about it in an active learning environment than in this to just complete a normal choice.

Nikolaj Jørgensen 6:52 Awesome. Yeah. And if you just on in line with what you were saying before about you, you can't say it on a recorded interview? You're of course free to if you find out that you've said something you shouldn't share. Please reach out and we'll delete.

Kristian Larsen 7:03 Yeah.

Nikolaj Jørgensen 7:05 Delete it from the transcript.

Kristian Larsen 7:07 Of course.

Nikolaj Jørgensen 7:08 But let's pivot a little bit. So we're gonna talk now about your experience, about for teaching, especially novices of rookies or people new to cybersecurity in general. We're very much interested in just First off the basics. Of like what is your experience of teaching, especially new new newcomers?

Kristian Larsen 7:30 So I think one thing that I would like to address in terms of like teaching newcomers is especially. The learning curve for the first half hour of experience. This type of learning format. They need a lot of support. For like getting started and understanding learning environment that they because it's something that they're not used to. And it's in that way. There's like an extra step where you need to, like, make sure they understand the learning environment that they're in before they can Start learning. And this usually takes like 20 to 30 minutes, depending on the individual. So in terms of that it it that is the hurdle in terms of using this time of learning environment is to is basically just getting started. And when they've gotten started



and understanding and they have an understanding of the learning environment. And and how it works. Then usually learning curve from there is a really nice for a lot of people. In terms of, if you look at like the role of the facilitator. When you're looking at novice. Newcomers, I think. The. This facility has an important role when when teaching new people how to use these types of learning environments. In. And that doesn't mean that the facilitator need to be really skilled in terms of cybersecurity, but it just need.

Nikolaj Jørgensen 9:11 Yeah.

Kristian Larsen 9:17 They just need to have the right tools for helping people getting started.

Nikolaj Jørgensen 9:24 And that's an interesting observation, which we also kinda fell into when we did our workshop. Is this facilitator role? How much? One thing is, as you say, just getting them started. Like make sure you create a user. Make sure you understand that this virtual machine does not have access to the Internet. All that stuff. But what about the facilitator's role? Of course, for newcomers as well. But just in general. For leading CTF workshops that's not intended to be competitive, but to be primarily for for learning. What? How do you see the facilitators role in in those types of workshops?

Kristian Larsen 10:06 I think I would see it as as being a guy. So basically you need to guard the. The participant, through the learning experience and make sure to remove unnecessary bumps on the road. And I think it's important to look especially at like the material that you're sending. How does that support? Especially like the newcomers in in their journey into the active learning environment. What we see is that. Some people have trouble reading. And that is not a new tendency. That is something that has been around since. A human started working with computers and technology. But actually reading stuff that is on the screen before just clicking a button. Is actually is actually a challenge and and that is not a limited to learning environments, but it is limited to how people use technology today and how they interact with it.

Nikolaj Jørgensen 11:19 And we fell into the exact same thing with our workshop group. But how do you see? And I don't if this is actually a part of what we wanted to talk about originally, but I think it it would be interesting for me at least to to get your perspective on, should the facilitator actively try to mitigate this from the participants or is it somet? More structural do we have to rethink or redo? How we make learning material on such a platform? So as the participant can't just start clicking buttons like if those are the two options, having the facility to do it or create changing the structure or the format, which one do you lean towards, do you think and and why?

Kristian Larsen 12:05 Think it's a mix? So I think in terms of learning material, it's important that it has been designed with the user in mind and it's the same for the platform. Of course, like the learning journey of like getting started on the platform needs to be designed for the user. So that's like two things. That needs to be addressed basically. And not just one. And.

Nikolaj Jørgensen 12:32 So what do you mean when you say have the user in mind and designed for the user? Can you? Can you put a few more words on that?

Kristian Larsen 12:39 So that means, for example, giving more visual guidance on the platform. That is also something that we are working with at the moment. That is no secret. Because we are paying for the aware of. A. The need to help the user even more in terms of getting started on our platform. In terms of the learning materials. It needs to be. It needs to be tested. And we found out the video materials showed videos work

really well. Instead of having long texts because then they can actually like read, watch the video real quick and then it's in a pace where they will like watch the whole video. If it's not too long and then actually be able to start solving the exercise. So that is something that we're working with quite a lot at the moment is actually making like more interactive materials for videos and then an exit learning exercise afterwards.

Nikolaj Jørgensen 13:36 That's. Fund perspective and and novel to my knowledge at least, I haven't seen that on any CTF platform before. That was just a comment.

Kristian Larsen 13:59 Now.

Nikolaj Jørgensen 14:01 The last thing we wanted to talk about is your perspective on how you see so, and this leads nicely into it. How do you see the CTF format changing over the next years and and in this we were both thinking like are there any industries who are gonna be new to the CTA format and like approach it or and also just how would the CTA format itself change so. Both like the market component of the CTF and the CTFS themselves. How do you see that changing? Over the next years.

Kristian Larsen 14:33 So I think in terms of like how is it gonna change?

Nikolaj Jørgensen 14:37 OK.

Kristian Larsen 14:39 I think the user group was the approximately the same. Maybe more people will be able to access this type of learning format. Going forward, because the library of entry is getting lower and lower, it's getting easier and easier to actually access these scanned learning platforms, but there's still. A lot to be done. So in terms of like how will it change, I think it will be easier to use. But I think it will still primarily be focused around. Both technical but also more soft exercises. And in in our case like I think it's not gonna change a lot in terms of like who we are making this for. Because there's other learning formats that can be used for other types of individuals. But I think we're gonna see it more and more that it's gonna be used. In. The. As a learning format because it is one of the few problem based learning formats where it's actually possible to guide the user in the right direction and just giving them in, the man open-ended exercise.

Nikolaj Jørgensen 16:01 Interesting. And you know, there's a particularly two things I I caught on to what we're saying there you you mentioned that the barrier of entry is becoming lower and lower. I have an idea, but can you elaborate on why that is?

Kristian Larsen 16:17 So one of the reasons is that there's only like a few amount of talented individuals. Who have the technical competencies to use? A lot of the platforms. So there is a clear business case in making. It more available. And from our perspective, of course, there is a perspective in the business case, but another part of it is making these types of learning materials more accessible for individuals who need to learn about it. Because at the moment there's such a huge need for upskilling within subsecurity that if we neglect all of these individuals, who doesn't have the competence and need them by making it too hard to access these materials, then we have a problem.

Nikolaj Jørgensen 17:13 That's a really. Yeah, a really nice perspective on it. And the last thing I wanted to touch on was you mentioned that you you think you'll have more soft exercises. Can you again elaborate a little bit on what you mean by soft?

Kristian Larsen 17:24 Yeah. So in terms of exercises on our platform, what we're working a lot with is of course

like hands on exercises that focus on technical skills, but something that we're working on a lot at the moment is also changing the format so that it will also encompass some of. The more soft skills. So for example compliance oriented. Things. Or more like government governance oriented. Exercises. That could also be soft skills in like the way I define it could also be some of the more. Soft skills within like a blue team. Which which would be like understanding a home source, intelligence, information security and stuff like that.

Nikolaj Jørgensen 18:23 That's an interesting perspective again, and I it made me think of like, yeah, so you mentioned before that probably more or less the same market, but it's just growing, but it makes me think like. The the way you just said that makes me think of of CT FS as a way to. Maybe not substitute, but at least. Enhance typical awareness type training in corporations. Can I get your perspective on on that idea? It's very much just off the cuff, but I would like to hear per point.

Kristian Larsen 18:57 So. In terms of awareness training, what we're seeing a lot of the moment is that if you look at like the normal learning format, then a lot of digital learning materials are using today. Where you just present a video and then give some questions afterwards. In terms of like the learning outcome from these types of learning materials. It can be very limited depending on how it's designed. And another factor is that if you want to teach. Proper skills. Hands on skills within a topic. Then you will need to actually have some kind of active learning environment and that is something that we're seeing that it's starting to change, especially within the field of cyber because it's. Starting to become important. For companies to actually make sure that. That their employees understand and can actually like act on fiber threads in terms of like the security culture.

Nikolaj Jørgensen 20:06 Yeah. OK.

Kristian Larsen 20:07 You don't, you you don't get to understand how to properly mitigate. A. A. Vulnerabilities on an on a service by taking a normal awareness course, even though it's enough for compliance in some situations, but it it doesn't make a difference in terms of how in terms of like limiting your risk as a company.

Nikolaj Jørgensen 20:35 Yeah, yeah, it's the bad kind of compliance. It's compliance for the compliance sake and not for the actual increase in security. That's all of my questions. So I have like two things on the agenda now. I wanna first say Christian, is there anything that you feel like we should have talked about that we didn't?

Kristian Larsen 20:55 No, I think I think I'm good.

Nikolaj Jørgensen 20:58 And then Nick, do you have anything that's really popped up on your end that you wanna ask Christian about? I'll just for the transcript say you're you're nodding or shaking your head. Cool. Well, then I think we're done.

Kristian Larsen 21:16 Cool.

Nikolaj Jørgensen 21:18 I'll stop the recording and hope it stops in the right way.

Nikolaj Jørgensen stopped transcription

## A.6 Observation Notes from Interview

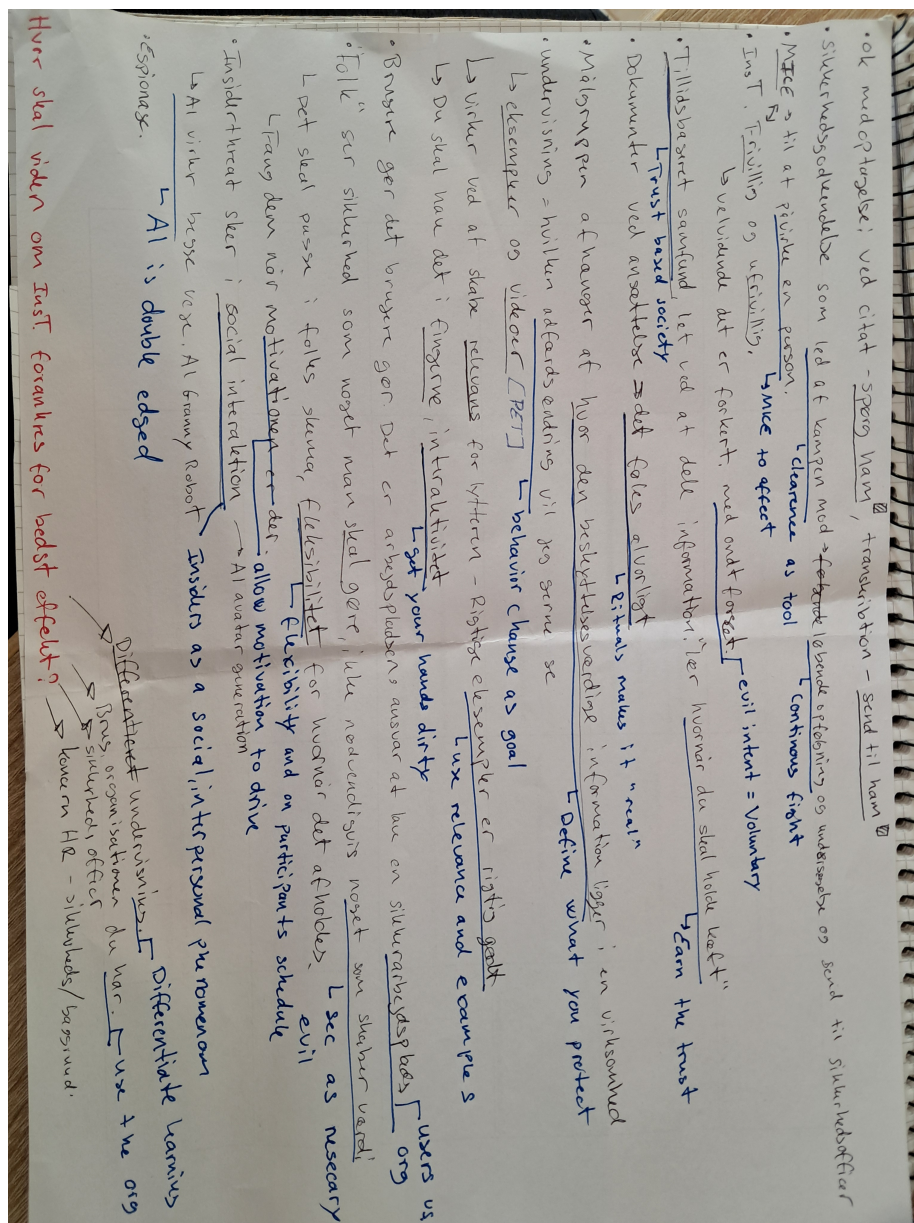


Figure 63: Observation notes with Codes in blue

## A.7 Transcript with Codes

## Interview med Thomas Kristmar

Dato: onsdag d. 30 april 2025

Til stede:

TK = Thomas Kristmar (interview person)

NB = Nick Blume (interviewer)

NJ = Nikolaj Jørgensen (noter og opfølgende spørgsmål)

## Transcript

TK

Pointen er bare jeg skal vide hvad jeg bliver citeret for

NB

Ja helt klart.

TK

Og så skal jeg se transkriptionen, ja.

NB

Er det sådan så du vil have udsnit af rapporten hvor det du siger er med? Eller er det sådan så du bare vil vide..

TK

Hvis jeg ser transkriptionen, så vil jeg antage at det i citere mig for står i transkriptionen. Når det så er sagt, så vil jeg gerne se jeres speciale når det er færdig.

NB

Ja fedt, og vores interview kommer jo i anledning af vores speciale hvor vi samarbejder med Campfire Security. En kort introduktion til hvad vi laver. Hvis det er fint med dig vil vi starte. Hvad er din stilling og rolle og hvilke ansvars områder har du?

TK

Jamen, jeg er områdechef i Statens It i det som hedder Sikkerhed og Compliance, en af to område chefer. Så er jeg også områdechef forendenrigsministerets drift og sikkerhed.

NB

OK, vil du sige insider threats er et vigtigt emne?

TK

Man kan sige ja, selvfølgelig er det det. Det er jo så også derfor for at blive ansat i Statens It skal du have en sikkerhedsgodkendelse, da det ligesom er én af de måder man kan arbejde med insider threats på. Ikke at det garantere noget som helst. Men det at der er en screening af medarbejderne efter væsentlige ændringer af økonomi, eller hvis der dukker ting om som gør dem påvirkelige. Så er der qua den sikkerhedsprofil vi har, en besked til Statens Its sikkerhedsofficer.

Commented [NJ1]: security clearance required

Commented [NJ2]: follow up. Post-hire re-screening

Commented [NJ3]: "security officer" alerts

NB

OK. Så nu kommer vi jo lidt ind på det her med med hvilken adfærd eller hvilke indikatorer der ligesom er på tegn på en insider threat. Nu nævnte du nogle af dem, er der flere du lige lige tænker over?

TK

Nå men altså, der er jo den berømte MICE, som er det der huskeord for hvordan man påvirker folk.

NB

Kan du uddybe?

TK

Ja. Der er **money**. Så er der Incrimination, Compromise og Ego.

**Commented [NJ4]:** MICE "motivations"

NB

OK

TK

Hvis du skal have fat i en, **så er det en af de fire knapper du skal ramme**. Det er ligesom standarden.

**Commented [NJ5]:** MICE "button"

NB

Interessant, hvordan ville du definere en insider threat eller insider threat som koncept?

TK

Jamen, insider threat kommer jo helt overordnet i **to varianter**. Der er én hvor du gør det frivilligt af en eller anden **motivation f.eks. MICE**. Og så en variant hvor du gør det ufrivilligt, **hvor du er lokket til det uden egentlig at vide det**.

**Commented [NJ6]:** voluntary vs. involuntary insiders | note term mis-match compared to CISA?

**Commented [NJ7]:** voluntary insider

**Commented [NJ8]:** involuntary insider

NB

Tror du også det er den almene forståelse af insider threats?

TK

Jeg tror at hvis du ser på det i en dansk eller nordisk kontekst så er der relative håndgribelige eksempler på hvordan insider threats manifestere sig. Altså relativt få eksempler på betroede ansatte gør noget, som man ikke burde gøre. Som altså gør noget velvidende det er forkert. Der er f.eks. Se og Hør sagen, med ham hvor det er tydeligt

motivet var penge, det er bare et eksempel. Tidligere var der flere sager hvor man kunne få adgang via en fødselsattest, det er vel 15 år siden, hvis du havde en fødselsattest så kunne du få et sygesikringskort, med sådan et kunne du få et pas og så kunne du blive hvem end du gerne vil. De lokale kirkekontorer havde dengang ikke super god praksis for at identificere folks identitet når folk dukkede op. Det er heldigvis blevet bedre.

Commented [NJ9]: identity fraud

NB

Det er godt at høre

[fælles latter]

TK

Så man kan sige for at besvare spørgsmål. Jeg tror at de fleste har en fornemmelse af at de [insider trusler red.] er nogen, der gør noget de ikke burde gøre, med ondt forsæt.

Commented [NJ10]: public understanding is a bad intent actor

Timestamp: 05:23

NB

Er der noget du tænker der ligesom mangler i den her almen forståelse nu? Nu nævnte du før der var 2 veje for eksempel, er der noget du tænker i den generelle forståelse, som der mangler?

TK

Der er forskel . F.eks. i udenrigsministeriet er for eksempel meget opmærksom på, de som gør det ufrivilligt, også det man kalder etlicitering. Hvor man interviewer folk og taler med folk til at dem til at hoste op med information. Det er jo et håndværk, man kan lære, hvis man har lyst til den slags. Det er de meget opmærksomme på.

Commented [NJ11]: elicitation as a CRAFT

NB



Er der noget du vil ønske du vidste i fortiden omkring insider threats eller noget du sådan ville ønske folk generelt vidste? F.eks. det her om MICE? Den var interessant. Er der noget du gerne ville have vidst tidligere eller som du mener den almene befolkning burde vide?

TK

Jamen jeg, tror i virkeligheden, fordi vi er et tillidsbaseret samfund. Så har vi nemt til information. I virkeligheden handler det nok om at vide hvornår man skal holde sin kæft

[fælles latter]

Commented [NJ12]: Trust based society

Commented [NJ13]: trust based requires responsibility

NB

Holder i noget af sikkerhedstræning her i Statens It?

TK

Ja. Vi har sikkerhedstræning. Vi har for nyansatte, hvor man også får en lille folder. Nævner den specifikt insider threats? Nej det gør den ikke. Men det er sådan noget med, at man skal være opmærksom på det. Derudover har vi også et lille ritual man skal igennem, når du bliver ansat får du to dokumenter. Først en tavshedserklæring du skal underskrive og en formular til sikkerhedsgodkendelse som du skal udfylde. Det der lille ritual, det gør pludselig at det her det føles sgu alvorligt. Du skriver jo faktisk under på at jf. Straffelovens paragraf 156, hvis jeg husker rigtigt, så kan du, hvis du misbruger dit offentlige embede eller information, så kan du blive straffet med fængsel.

Commented [NJ14]: cybersecurity awareness folder

Commented [NJ15]: onboarding ritual as a signal

Commented [NJ16]: a ritual "with teeth"

NB

Holder i andet cybersikkerhedstræning generelt for nogen i Statens It?

TK

Nej, men det er sådan noget vi forsøger at bygge ind med Campfire Security, som bekendt.

NB

Hvad tror du den typiske målgruppe er for sådan noget cybersikkerhedstræning?

TK

Altså nu er vi jo selvfølgelig et teknik hus, befolket af teknikere.

Commented [NJ17]: tech-workforce

[kort pause]

Det jeg vil sige er, at vi har meget få af det jeg kalder bureaukrater. Dem har vi stort set ikke nogen af, vi har kun teknikkere.

NB

Hvad med mere i sådan et et generelt perspektiv, du ved i en almen virksomhed hvor tror du at målgruppen vil være?

TK

Det kommer nok helt an på hvad virksomheden laver. For i virkeligheden handler det om hvor er den beskyttelsesværdige information og hvad er det du har adgang til. Nogen gange er bogholderen nok at få fat på, andre gange skal der en udvikler til. Det afhænger meget af hvad formålet er med at få fat i en insider. Altså hvorfor er det du forsøger at rekruttere en insider.

Commented [NJ18]: target audience selection based on ROLE?

Commented [NJ19]: locate critical information first

Timestamp: 09:30

[Telefon ringer og Thomas træder ud og tager opkald, optagelse stopper]

[Interview genoptages sammen med optagelse]

Timestamp: 09:45

NB

Jamen lad os komme lidt videre, har du deltaget i sådan noget cybersecurity træning eller lignende, eller har du undervist eller hvad har du af erfaring med at undervise?

TK

Ja til begge dele.

NB

OK. Interessant. Hvad tænker du om at både deltage og undervise? Både positivt og negativt?

TK

Jeg synes helt klart at undervise er super sjovt. Fordi, når du underviser kræver det at du fjerner et lag af kompleksitet og gør det tydeligt hvorfor modtageren skal bruge sin tid på det, altså svare på what is in it for me? Fordi hvis du ikke får den læring formidlet så får du et tomt blik tilbage, og du har ikke nogen effekt. Du vil gerne have en effekt og adfærdsændring. Så det spørgsmål man kunne stille sig selv inden undervisningen er når den her time er gået, hvilken adfærdsændring vil jeg så gerne se? Og det kunne jo i virkeligheden bare være: jeg vil meget gerne have at inden du åbner munden næste gang i fremmedes selskab så tænker du dig lige en ekstra gang om. Det er sådan noget du kan formidle, komme med eksempler eller videoer. PET har i øvrigt glimrende videoer om insider trusler.

Commented [NJ20]: Answer 'what's in it for me?'

Commented [NJ21]: Define the goal as behavior change

NB

Sådan mere generelt om sikkerhedstræning, både om insider trusler men også udenom det emne, hvad tror du hjælper til at den her viden forbliver? Altså hvad sikrer at folk ikke går ud bagefter uden adfærdsændring? Hvad tror du kan være med til at folk beholder den her viden og der sker den her ændring?

TK

Det første det er relevans. Altså forstå, hvorfor fortæller du mig det? Jeg kan give dig uendelig mange detaljer om et slag i 2. Verdenskrig, som jeg synes er helt vildt spændende, men jeg er ikke sikker på at du måske påskønner, som f.eks. hvor mange invasionsstrande var der i 1944? Nej bare se!

Commented [NJ22]: relevance as a driver for retention

Commented [NJ23]: relevance as a driver

[kort pause]

Der var fem.

[fælles latter]

Så altså hvis du f.eks. sidder i udenrigsministeriet hvor en af opgaverne er at tale med folk og møde nye folk og skabe kontakter og skabe mulighed for handelsrelationer og skaffe information om hvad der sker i det pågældende land. Så kommer du til at interagere med folk, som du gerne vil have til at fortælle dig noget stille og roligt. Når man har sådan en dialog så er det menneskeligt naturligt at føle man kommer til at skyldes noget hvis man får information af modparten, det skal du lade værd med. I den situation er det åbenlyst interessant og relevant at få den her viden [om insider trusler red.]. En af de bedste måder er f.eks. at spørge, kan jeg ikke få lov til at give dig en øl? Og når hvad går du så og laver? Så er toget i gang.

Commented [NJ24]: socio-guilt hook

NB

Hvad tænker du om hvordan man gør folk opmærksom på det her bedst muligt? Er det netop ved eksempler?

TK

Eksempler virker, eksempler er altid godt. Rigtige eksempler er rigtig godt. Og så prøve at finde nogle der er af nyere dato.

Commented [NJ25]: real and recent examples

NB

Så eksempler, og noget der har relevans for en?

TK

Ja og typisk noget som er relevant for ens arbejdssituation og ens hverdag. Case in point, du behøver ikke, hvis du ikke har noget der er relevant til dit arbejde, så måske finde noget der er relevant til dit offentlige liv. Når du nu offentligøre fotos, behøver du så have geo-data i? Fordi jeg kan faktisk finde ud af hvor du bor. Og hvis jeg kan finde ud af, så er det også andre som kan. Så er du henne på l'et, Intimidation fra MICE. Så man kan sige, her er et billede af dine børns skole, det er godt nok en frygtlig vej de skal krydse, der sker så mange uheld. Men du arbejder i kommunen? Ej hvor spændende, når du arbejder i skatteforvaltningen? Altså man kan sagtens bruge den slags informationer.

Commented [NJ26]: risk of geolocation data

Commented [NJ27]: Intimidation, MICE

NB

Ja, det er nogle gode eksempler for at tydeliggøre for relevant det kan være med information og at holde kæft

[fælles latter]

NB

Jeg vil gerne høre, vi har været lidt inde over det, men hvordan ser du god cyber sikkerhedstræning?

TK

Det man kan sige er, at det er noget hvor man får lov til at mærke det selv. Hvis du får fingrene i dine tools. Der skal være noget interaktivitet, du skal prøve at få det i fingrene ellers husker du det ikke. Det som med 100 procent sikkerhed ikke virker, det er det som vi har gjort de sidste 20år. Altså den stil hvor du stiller dig foran et powerpoint og taler. Det som med 100 procents sikkerhed ikke virker. Det er at man placere folk til et obligatorisk 45min kursus i cybersikkerhed hvor du ikke kan spole eller skrue på det. Folk er ved at kaste sig ud af vinduerne før de er færdige. Så er der videoer, hvor du efterfølgende skal besvare tre spørgsmål, og det hele er tydeligvis bare en compliance øvelse. Jeg kan bare sige, hvis det ikke var fordi man ikke kan åbne vinduerne så havde folk kastet sig ud af dem.

[fælles latter]

TIMESTAMP: 16:32

NB

I forhold til sådan generelt cybersikkerhedstræning hvem tror du, der kunne gavne mest af det?

TK

Gavn? Prøv at fortælle noget mere

Commented [NJ28]: interactive / hands on learning

Commented [NJ29]: PowerPoint = Failure

Commented [NJ30]: compliance fatigue

Commented [NJ31]: compliance fatigue

NB

Hvem der vil få mest udbytte af det, ift. Enten at kunne gøre det til en daglig praksis eller blive mere sikker i deres arbejde? Du ved lidt almen cyberhygiene ift. Genbrug af password f.eks. Sådan generel cybersikkerhedstræning, hvem tror du det kunne gavne aller mest?

TK

Altså nu kan det nok få lidt karakter af religion ikke? Men det er arbejdsgivers forpligtelse af stille en arbejdsplads til rådighed der er tilstrækkelig sikker. Det er mit udgangspunkt.

Commented [NJ32]: employers responsibility / duty

NB

Så Jeg tror også der underliggende ligger, hvem tror du det er som oftest kvajer sig? Hvis det giver mening?

TK

Altså brugere gør det, som brugere gør. Brugere forsøger sådan set bare at få løst deres arbejde, og hvis man har lavet noget der er åndsvagt, jamen så finder brugeren vej. Altså i gamle dage f.eks., eller det var faktisk ingen gang i gamle dage, det var i '17 at jeg skiftede til en bank og arbejde der. Jeg kom fra FE, og skulle oprette en ny adgangskode til banken. Kode ikke godkendt, argh! Hold da op de må godt nok have nogle vilde krav. Efter lidt tid fandt jeg ud af, at kodeord ikke måtte være over syv tegn og ikke indeholde æø eller å, for det kunne deres gamle mainframe ikke håndtere.

Commented [NJ33]: users are users..

Commented [NJ34]: users focus on the task at hand, not security

Commented [NJ35]: users bypass poor controls

Commented [NJ36]: poor controls

Commented [NJ37]: poor controls due to hardware limitations

[fælles latter]

Det har de forhåbentlig fået udbedret siden, men eksemplet er meget godt. Det næste jeg gjorde var at lave en hash af firmanavn og årstal og se hvor mange konti jeg kunne finde, og det kunne jeg godt.

NB

Skræmmende.

[Fælles latter]

NJ

Ja skræmmende, men det er ikke overraskende.

NB

I forhold til fremtiden for cybersikkerhedstræning, hvor ser du den, og hvad tror du virker? Vi har vendt det her med interaktivitet og undgå præsentationer, men hvor ser du egentlig fremtiden for det?

TK

Jamen jeg tror, altså det er virkelig svært, for selvom vi i det her rum synes sikkerhed er utrolig spændende, så er det jo os der lever af det. Som udgangspunkt ser andre folk sikkerhed som noget man skal gøre, mere end noget der giver værdi. Så det handler i virkeligheden om at få lavet noget, der sikrer at det giver værdi og mening at være sikker. I virkeligheden handler det om at sørge for det giver mening i en arbejdskontekst.

Commented [NJ38]: security as a necessary evil

Commented [NJ39]: make security is seen as valuable / relevant

NB

Så tilbage til det her med relevans?

TK

Ja. [kort pause]

Og så tror jeg også, man kan sige der er noget som handler om hvornår man skal kunne gøre det. Der skal være en portion af fleksibilitet. Når man har awareness og cybersecurity træning, så skal man kunne gøre det på et tidspunkt hvor det passer ind i ens hverdag. Det kan godt være man synes det er spændende, og at man godt ville, men hvis der kommer noget ind fra højre med en besked om at det skal gøres nu her til formiddag, så får det modstand. Giver det mening? Altså at man opnår noget fleksibilitet i hvornår træningen skal være.

Commented [NJ40]: flexibility in timing

NB

Ja, det er en proces, man kan ikke nødvendigvis sætte en slut dato på.

TK

Ja det er den ene del af det. Man kan sige de fleste virksomheder har også træning i forbindelse med onboarding. Dermed sagt at alle medarbejdere har gennemført træning inden for et eller andet tidsrum. Der jeg var i The Big Four havde du et eller andet tidsrum til at få det gjort, mandag morgen er motivationen for at lære om den amerikanske børns ret lav, lav just saying.

**Commented [NJ41]:** time window, flexibility

**Commented [NJ42]:** flexibility in timing, monday morning blues

NB

OK, så det her med motivation har også betydning, det giver jo også god mening. Vi er faktisk ved at være færdige, så jeg vil høre, er der andet vigtigt du føler vi ikke har talt om?

TK

Jeg mangler at høre om, hvad jeres speciale i virkeligheden handler om.

NB

Jamen det vil vi meget gerne fortælle om. Vi samarbejder med Campfire Security og laver noget materiale til dem i forhold til at undervise i insider threats. Vi laver et kursus med moduler som skal på deres hjemmeside. Det består af læringsmateriale og challenges ved siden af som vi skal have prøvet af. Det er egentlig det, som det handler om.

TK

Spændende. Men det er jo også netop der, hvor man har det der online komponent og det interaktive. Har i set den der fra PET omkring insider træning?

**Commented [NJ43]:** PET perspective

NB og NJ

Nej

TK

Det ligger inde på deres youtube, og er faktisk god. I bør lige prøve google PET insider.

**Commented [NJ44]:** PET perspective



NJ

Ja, jeg noterede det faktisk også ned da du nævnte det, at det skal vi lige have kigget på. Jeg har et enkelt spørgsmål. Det er mere på et organisations perspektiv, hvor ikke alle måske synes sikkerhed er spændende, hvilket jeg ikke forstår. Hvis man nu udbredte træning om insider trusler, hvor forestiller du dig at det bedst forankres i en organisation som f.eks. Statens It eller anden organisation?

TK

Jamen jeg tror, hvis vi nu siger f.eks. for Statens It er beskyttelse mod insidere til dels forankret i Koncern HR, for det er ligesom dem der stiller krav til at du skal have en sikkerhedsgodkendelse. Og så ligger det selvfølgelig også i vores center med sikkerhed og compliance, hvor vi dels har verifikation på at du har fået en HEM godkendelse [HEM = Hemmelig red.] og holder styr på HEM godkendelser.

Commented [NJ45]: anchor in HR and organization

TIMESTAMP: 24:25

[utydelig bid på ca. 10sek.]

TK

Awareness delen i vores organisation er at stille kursus til rådighed. Hvis vi er enige om at, det her er et godt kursus behøver vi jo ikke være dem som udbyder det, det kan lige så godt ske gennem dem som almindeligvis arbejder med kursus. Det vigtige er at i en typisk organisation har man platforme til det. Staten har det som hedder Campus, hvor man, hvis man havde tiden, kunne bruge flere uger af sit liv på at tage forskellige kurser. Men folk har jo oftest en hverdag, så det er organisationen tilpasser de forskellige kurser som folk skal igennem, der skal være noget om sikkerhed, krænkende adfærd, de nye arbejdstidsregler og andet interessant. Jeg tror i virkeligheden det jeg forsøger at sige er, at dem som laver kurser i forvejen det skal gøre det. Man skal ikke gøre som vi gjorde i 90'erne hvor man lavede et specielt felt fordi det er sikkerhed, vi skal lave undervisningen sammen med dem som laver undervisningen i organisationen.

Commented [NJ46]: e-learning platform

Commented [NJ47]: Course saturation, add value

Commented [NJ48]: Learning / teaching is not done in silo's

NB

Så det netop bliver skræddersyet til dem.

TK

Nej. Så at de har overblik over hvad for et udbud der er, og kan sikre at det passer ind. For når hver enkelt afdeling har deres egen lille ynglings ting og samtidig skubber den ud til den enkelte bruger, som desperat sidder og kæmper med deadlines i Campus. Så du skal bruge den organisation du har, og være tro mod den. Og så lade være at følge dit instikt med bare at gøre det selv, nu gør min afdeling det, nu gør mit center det. Man skal bruge den organisation man har, og sige, hey! Vi har forresten nogen som arbejder med at de relevante kurser er til rådighed og de skal bare have at vide, her er et relevant kursus, sørg for det kommer til rådighed.

Commented [NJ49]: anchor in HR and organization

Commented [NJ50]: avoid DIY silo's in organizations

Commented [NJ51]: use the organization you have

NJ

I forhold til det med at lave relevant kursus, man kan jo lave kursus på forskellige niveauer, og det er netop noget af det vi kigger lidt ind i. Man kan både have, hvordan gør du detection engineering målrettet mod intentional insider trusler, men man kan også godt have en awareness agtig træning. Der skulle fungere lidt som de to dokumenter du nævner ved ansættelse, så sige du har også et insider trussel kursus du skal igennem, om ikke andet for at skabe bevidsthed om at det er noget vi kigger på og synes er relevant. Nu har jeg lidt afsløret vores tanker og hvad vi tænker at gøre, men hvad tænker du om den tilgang, altså netop at undervise på laveste niveau også for at skabe opmærksomhed på det? Du nævner selv MICE, vi har mest selv kigget i CISA's definitioner, men ja nu blev det et langt spørgsmål. Har du nogen tanker du kan dele?

TK

Jamen jeg synes godt om at gøre det differentieret. Der er ikke noget værre hvis du sidder i en sikkerhedsafdeling og skulle igennem et online kursus i sådan opdager du en phishing mail, som måske i virkelighed er et kursus rettet til bogholderne.

Commented [NJ52]: differentiated training levels

NJ

Nick har du flere ting på listen?

NB

Jeg tror det eneste vi vil snakke mere om var om der var noget nyere teknologi som kan ændre på landskabet?

TK

Ja. AI.

[Fælles latter]

NJ

Ja det var oplagt måske, men hvordan?

TK

Når men pointen er jo at insider threat er noget der sker med en social interaktion. Vi mennesker er jo biologisk kodet til at tro på det vi ser og hører. Jeg ved det er dig Nick, da jeg kan se skiltet, og Nikolaj at han kender dig og kalder dig det samme, og Nikolaj stoler jeg på, så du er sgu nok Nick. Hvis jeg ser en avatar eller digital repræsentation af dig, som kan blive ret gode efterhånden, så vil jo sige hmm, hvis du så laver et teams kald med mig om en uge med opfølgende spørgsmål, så vil jeg jo sige jo, og man vil så bygge videre derfra, men jeg kan jo rent faktisk ikke vide om det er dig.

Commented [NJ53]: AI impersonation

NB

Bestemt ikke. Der var også en, apropos, der var en journalist som var med i et radio program hvor han lavede en AI model på hans stemme, så de havde en repræsentation af ham. De ringede til hans mor, og hun gav alle oplysninger som han, eller som computeren spurgte om. Derefter ringede de hende op og fortalte, mor du har faktisk ikke talt med mig men med computeren. Det var bare en sjov historie jeg kom i tanke om.

Commented [NJ54]: AI impersonation

TK

Har du set den de har lavet, for det gælder jo så også begge veje, er det British Telecom der har lavet den her Granny robot? Har du set den?

NJ

Ja der findes jo også youtubere dedikeret til netop anti-scramming med AI.

TK

Ja. Granny Robot, den tager imod de her Microsoft support service opkald og så spilder den bare deres tid.

**Commented [NJ55]:** AI impersonation, for the "good guys"

NJ

Det er fantastisk.

TK

Det er genialt. Det virker begge veje.

**Commented [NJ56]:** AI impersonation works both ways!

NB

Ja vi har jo lidt talt om det på en negativ måde, men nu er der også noget positivt. Hvordan teknologi kan du ved blive brugt både angrebs- og forsvars-mæssigt. Det med at spille tid er jo en god måde at gøre det på. Tænker du at der er andet end det her?

TIMESTAMP: 31:13

TK

[Tekst bid fjernet efter ønske fra Thomas red.]

NJ

Ja præcis, unintentional så.

TK

Ja.

NJ

Insider trusler er et stort emne, så vi kan selvfølgelig ikke dække det hele, men er der noget hvor du tænker, hvorfor har vi ikke snakket om dette?

TK

Jeg tænker, men det er måske mere en PET ting. For i virkeligheden tænker jeg mere i relation til spionage.

Commented [NJ57]: framing in relation to espionage

NJ

Ja, jeg synes godt man kan fornemme du kommer fra UM med den måde du går til insider trussel emnet

TK

Jo jo, men jeg har også været i to tjenester jo.

NB

Ja du nævner jo det her med, hold kæft ikke, man kan bruge information. Normalt når man tænker både intentional eller unintentional insiders vil mange tænke phishing emails eller disgruntled employees, men der har du et andet perspektiv, hvilket gør det meget interessant. Netop det her med espionage retningen, som man også bør overveje.

TK

Ja og også det her med universiteter, case in point.

Commented [NJ58]: espionage against universities

NJ

Ja der er det også meget udbredt

NB

Espionage?

TK og NJ

Ja.

NB

OK. Det har jeg hørt lidt om men ikke meget.

Det sidste der er, om vi må række ud hvis der er opfølgende spørgsmål?

TK

Ja selvfølgelig.

NB

Vi sender transskribering når vi er færdige med den.

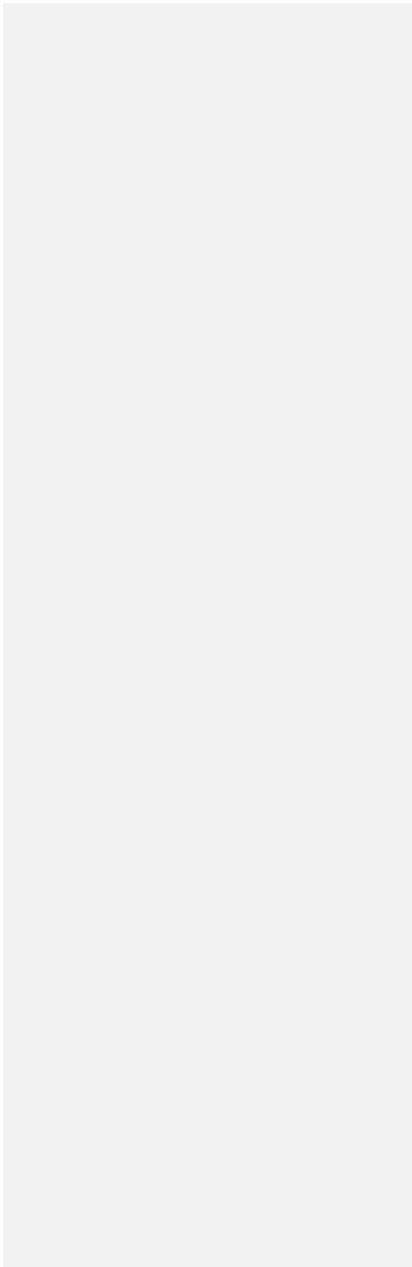
NJ

Og citater kører vi lige forbi dig inden vi bruger dem. Og vi anonymiserer dig ikke i opgaven?

TK

Nej det fint.

[Interviewet afsluttes]



## **A.8 Interview Guide**



Theme/Focus	Rationale	Sample questions	NOTES
1. Introduction & building rapport	Opening the "drama" and setting the stage. Establish interviewee as the knowledgeable actor	<ul style="list-style-type: none"> <li>- What is your current role and responsibilities?</li> <li>- Why is Insider Threats an important topic?</li> </ul>	
2. Defining Insider Threats	Explore the interviewee's frame and vocabulary for Insider Threats	<ul style="list-style-type: none"> <li>- How do you personally define Insider Threat?</li> <li>- Is there anything lacking in the common conceptualization of the term?</li> <li>- What sorts of indicators/behaviors do you associate with Insider Threats?</li> <li>- What would you have liked an earlier version of yourself to know about Insider Threats?</li> </ul>	
3. Cybersecurity training in general	Open the "stage" and allow interviewee to "perform"	<ul style="list-style-type: none"> <li>- How do you conduct cybersecurity training in Statens IT?</li> <li>- How do you feel good cybersecurity training looks like?</li> </ul>	
4. Cybersecurity training in practice	Steer the "performance" towards challenges identified	<ul style="list-style-type: none"> <li>- When conducting cybersecurity training, who are the most likely target audience?</li> <li>- From your experience, what makes good cybersecurity training? what makes the knowledge stick?</li> </ul>	
5. Future needs	Open the "stage" once more and allow for interviewee to give advice	<ul style="list-style-type: none"> <li>- How do you envision the future of cybersecurity training to look like? What would have the most impact?</li> <li>- Which emerging tools or methods (AI-based analytics, user behavior monitoring) might transform insider threat detection?</li> </ul>	
6. Closing	Exit from the "stage" and explain next steps. Ask for follow-up and snowball	<ul style="list-style-type: none"> <li>- Is there anything crucial about insider threats we haven't covered?</li> <li>- Would it be okay to reach out if we have additional clarifications?</li> </ul>	

## **A.9 Coding Process**

Categories	1. Nature and motivation of insider threat	2. Organizational governance and safeguards	3. Designing effective awareness and training in general	4. Cultural and contextual factors
	socio-guilt hook	locate critical information first	target audience selection based on ROLE?	public understanding is a bad intent actor
	intimidation, MICE	risk of geolocation data	Answer 'what's in it for me?'	Trust based society
	PET perspective	employer's responsibility / duty	Define the goal as behavior change	trust based requires responsibility
	PET perspective	poor controls	relevance as a driver for retention	Trust based society
	framing in relation to espionage	poor controls due to hardware limitations	relevance as a driver	Earn the trust
	espionage against universities	security as a necessary evil	real and recent examples	Sec as a necessary evil
	MICE "button"	anchor in HR and organization	interactive / hands on learning	AI is double edged
	voluntary vs. involuntary insiders   note term mis-match compared to CISA?	Learning / teaching is not done in silo's	PowerPoint = Failure	
	voluntary insider	anchor in HR and organization	compliance fatigue	
	involuntary insider	avoid DIY silo's in organizations	compliance fatigue	
	identity fraud	use the organization you have	users are users..	
	elicitation as a CRAFT	AI impersonation	users focus on the task at hand, not security	
	MICE "motivations"	AI impersonation	users bypass poor controls	
	MICE to affect	AI impersonation, for the "good guys"	make security is seen as valuable / relevant	
	Evil intent =voluntary	AI impersonation works both ways!	flexibility in timing	
	Insiders as a social, interpersonal phenomenon	cybersecurity awareness folder	time window, flexibility	
		onboarding ritual as a signal	flexibility in timing, monday morning blues	
		a ritual "with teeth"	e-learning platform	
		tech-workforce	Course saturation, add value	
		security clearance required	differentiated training levels	
		follow up, Post-hire re-screening	Define what you protect	
		"security officer" alerts	Behavior change as goal	
		Clearance as a tool	Use relevance and examples	
		Continuous fight	Get your hands dirty	
		Rituals makes it "real"	Flexibility and, on participants schedule	
		Users vs. org	Differentiate learning	
		Allow motivation to drive		
		Use the org		
<b>Concepts</b>				
	Insider risk is a motivation + opportunity phenomenon			
	Security is an organisational obligation operationalised through governance rituals			
	Behaviour changing training hinges on: relevance, interactivity and contextual fit			
	Trust culture and emerging technologies create a double edged landscape			

## A.10 HTML Emails

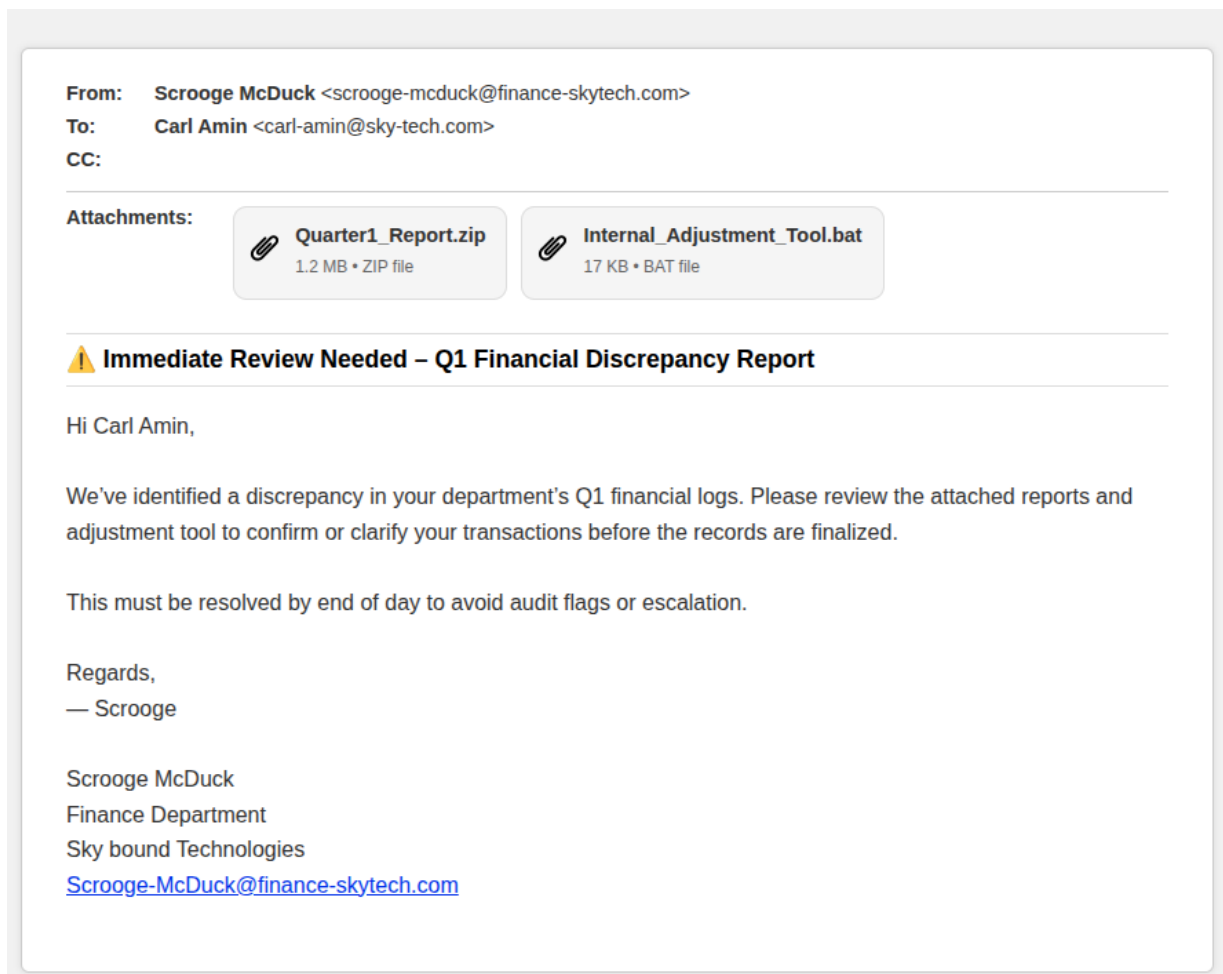


Figure 64: The 4th task out of 7 in the 3rd challenge - "Is This a Phishing Email... ?". This is the only email presented with attachments.

## A.11 Other Pages.

Index Page

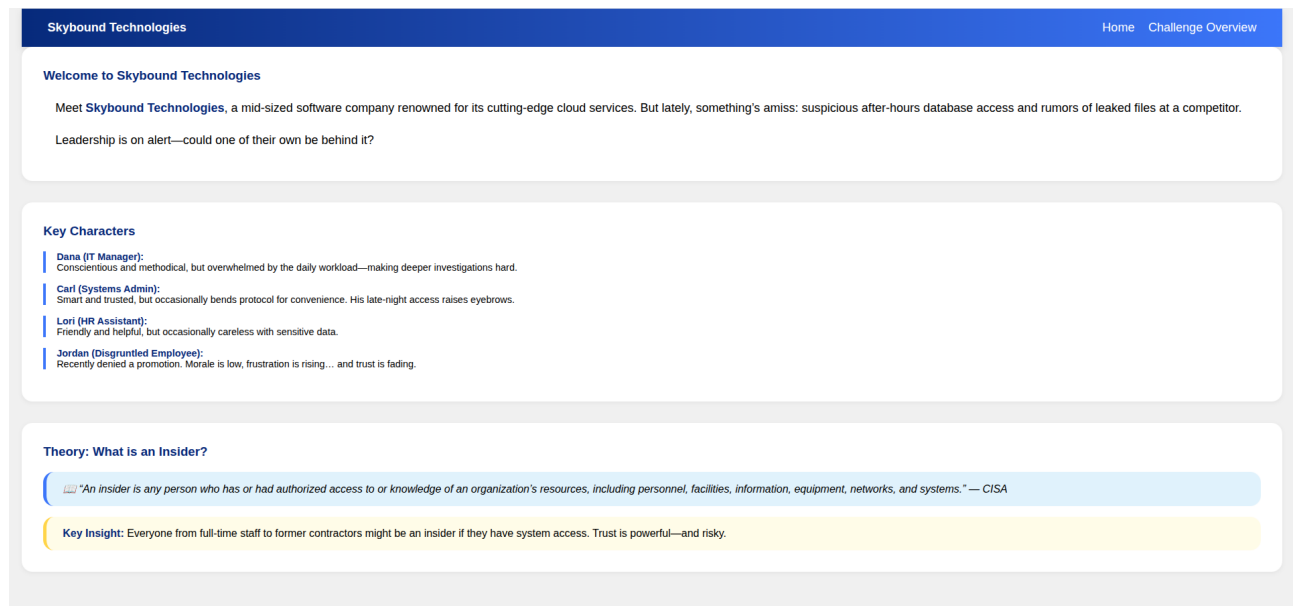


Figure 65: The Index.html

## Challenge Overview Site

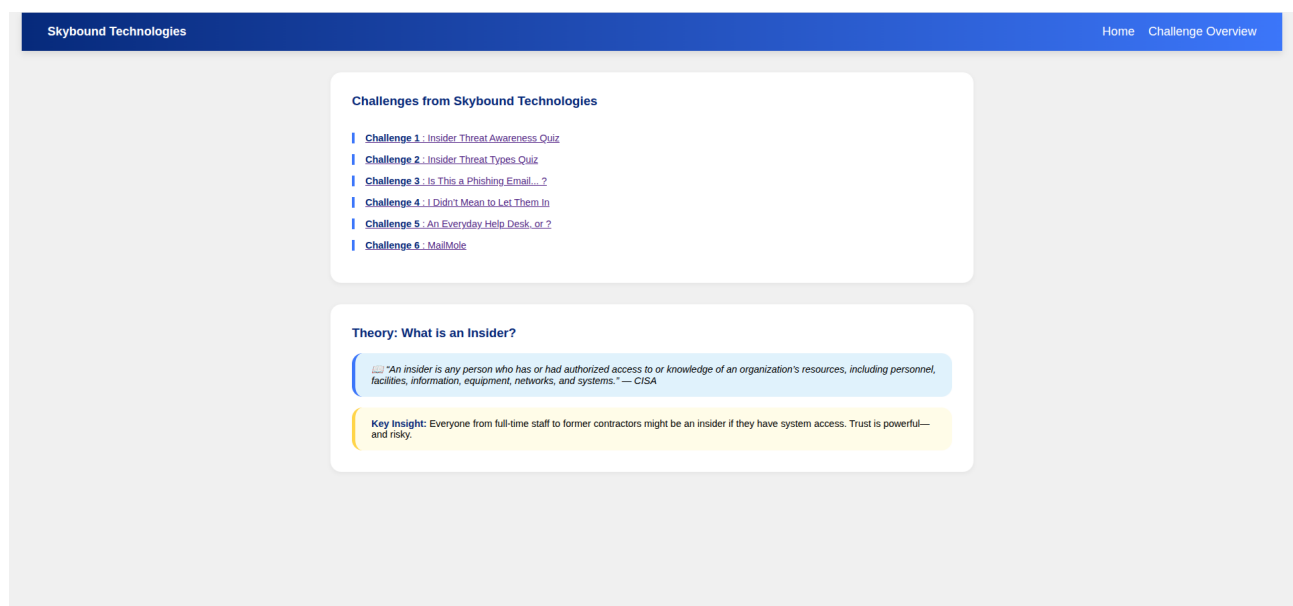


Figure 66: The ChallengeOverview.html

## Malicious Site

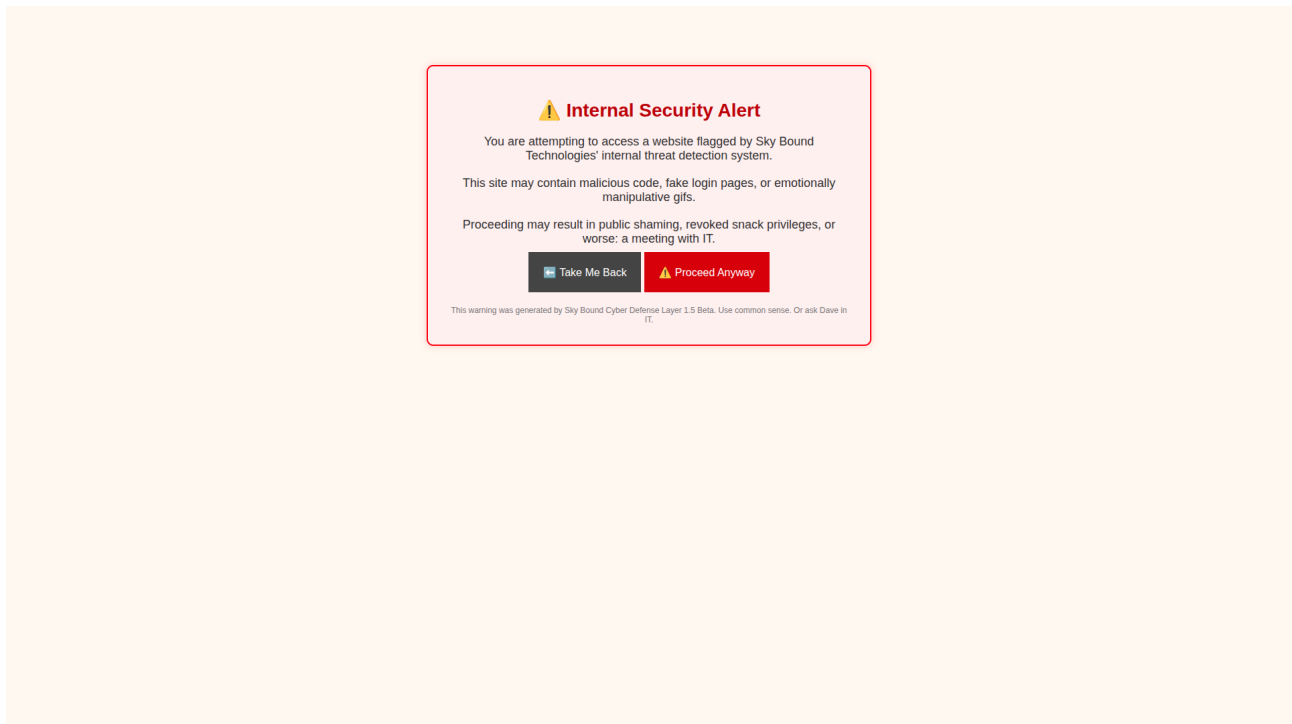


Figure 67: The MaliciousSite.html, When clicking the link a new window will open with the this html. When pushing "Take Me Back" retrieves to the index.html, "Proceed Anyways" closes the window with Malicious-Site.html

## A.12 Challenge 6 Emails

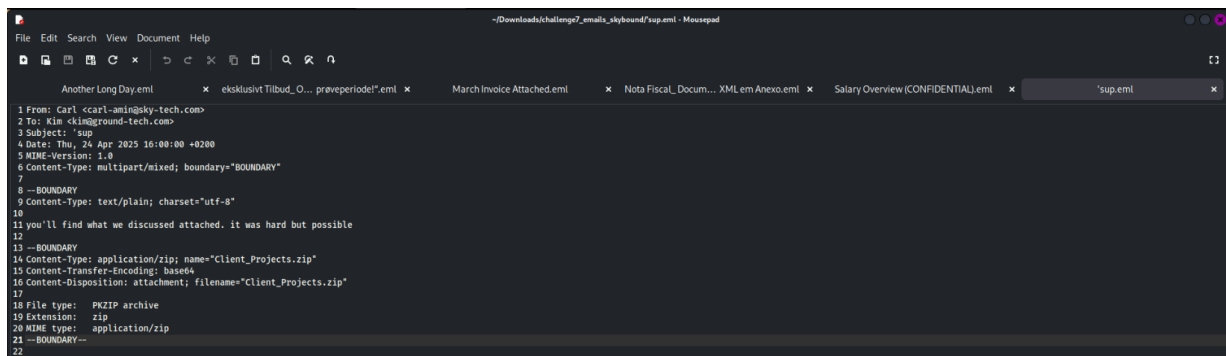
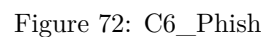
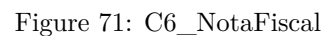
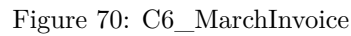


Figure 68: C6\_'sup



Figure 69: C6\_AnotherLongDay



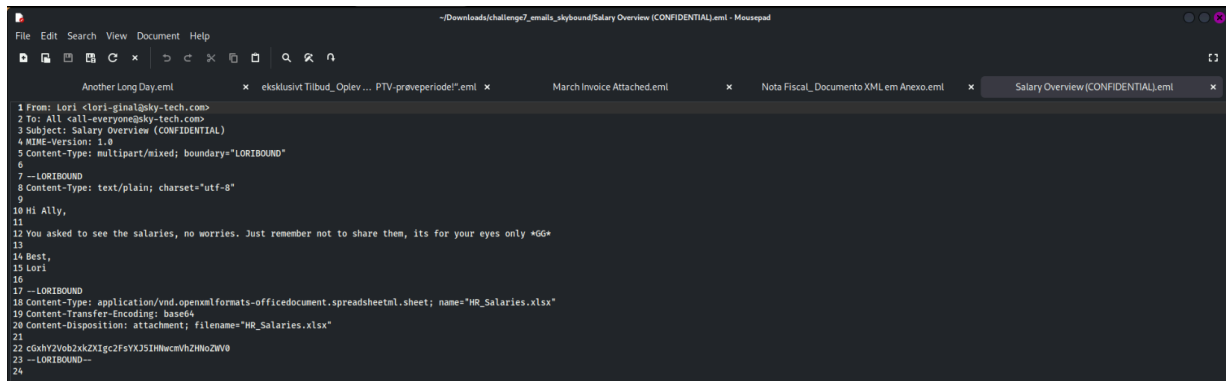


Figure 73: C6\_SalaryOverviewUnintentional

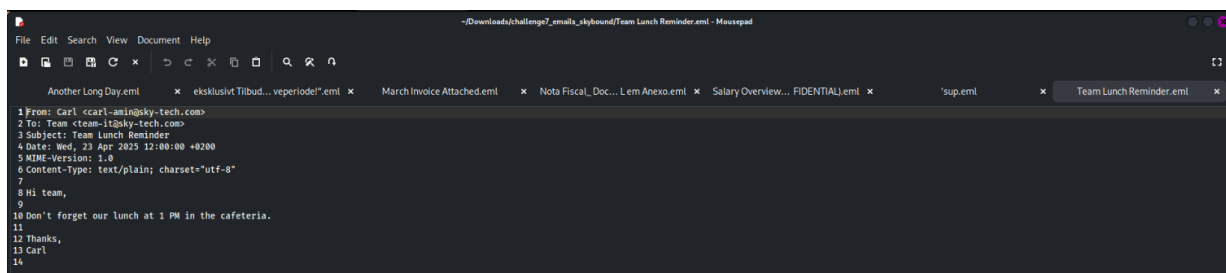


Figure 74: C6\_TeamLunch

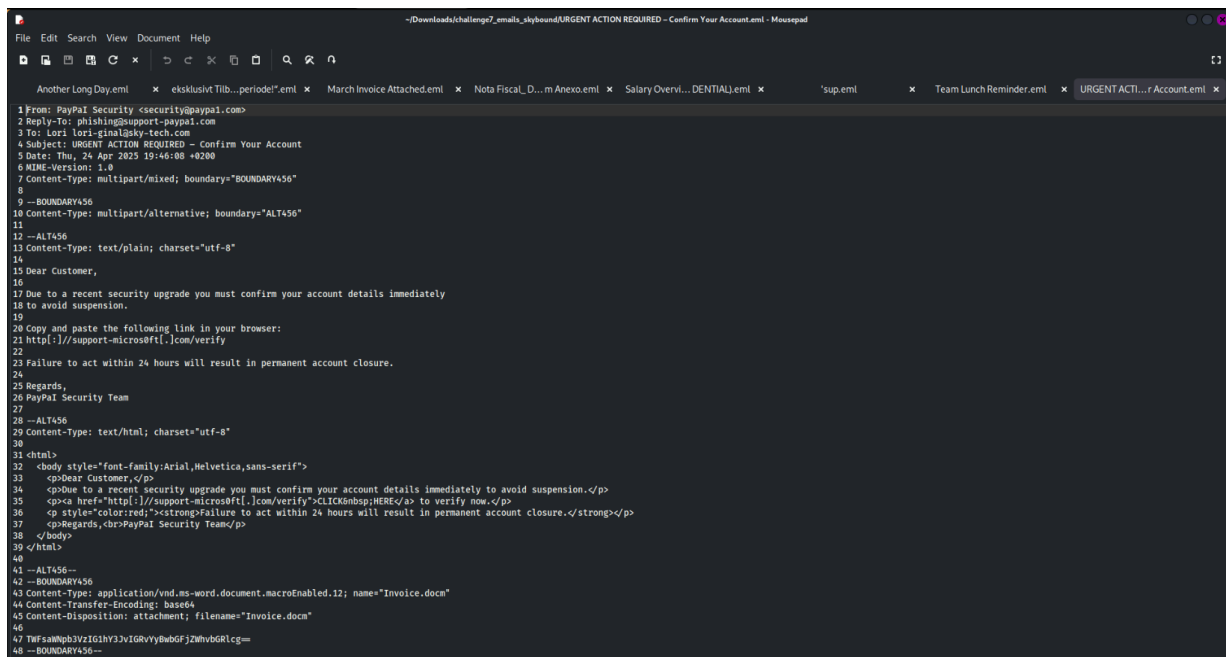


Figure 75: C6\_UrgentPaypalPhish



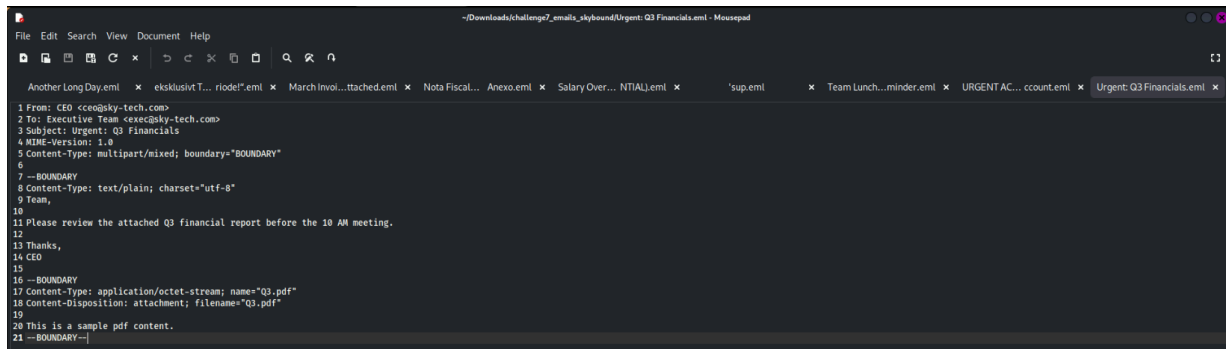


Figure 76: C6\_UrgentQ3Finance

## A.13 Questionnaire data

ID	Your current Role/Job/Position	Approximate years of professional experience (number of years)	Prior cybersecurity experience	Have you previously participated in a CTF?	I lost myself in this experience.	The time I spent using "Insider Threat Course" just slipped away.	I was absorbed in this experience.	I felt frustrated while using this "Insider Threat Course".	I found this "Insider Threat Course" confusing to use.	Using this "Insider Threat Course" was taxing.	This "Insider Threat Course" was attractive.	This "Insider Threat Course" was aesthetically appealing.	"Insider Threat Course" appealed to be visual senses.
1	Graduate	10	Basic awareness	No	Agree (4)	Neither agree nor disagree (3)	Agree (4)	Neither agree nor disagree (3)	Agree (4)	Disagree (2)	Neither agree nor disagree (3)	Disagree (2)	Disagree (2)
2	Graduate (IT-medarbejder)	5	None	No	Disagree (2)	Neither agree nor disagree (3)	Neither agree nor disagree (3)	Strongly Disagree (1)	Disagree (2)	Strongly Disagree (1)	Agree (4)	Strongly Agree (5)	Agree (4)
3	Graduate	0	15 erts kurse i netværk og cybersecurity fra SDU (Datalog)	Yes	Agree (4)	Agree (4)	Agree (4)	Disagree (2)	Disagree (2)	Neither agree nor disagree (3)	Neither agree nor disagree (3)	Neither agree nor disagree (3)	Neither agree nor disagree (3)
4	Analytiker	3	Intermediate/hands-on	Yes	Disagree (2)	Disagree (2)	Disagree (2)	Neither agree nor disagree (3)	Disagree (2)	Disagree (2)	Agree (4)	Neither agree nor disagree (3)	Neither agree nor disagree (3)

Sheet3

Using "Insider Threat Course" was worthwhile	My experience was rewarding.	I felt interested in this experience.	How was the overall difficulty of the challenges	Any notes on the overall difficulty of the challenges	I prefer this style of learning compared to traditional methods ?	Did the story telling influence your experience?	Any notes on how the story telling influenced your experience	Did the storytelling affect your engagement	Any notes on how the story telling affected your engagement?	Do you believe you could explain at least one concept or technique from the course to a colleague ?	Any notes, or elaboration on why, or why not.	Feel free to provide additional feedback
Agree (4)	Neither agree nor disagree (3)	Strongly Agree (5)	(3) Neither easy nor difficult	Den sidste opgave var svært godt? Jeg kunne ikke finde det sidste ord på navnet af emailen, hvilket gjorde det svært. Bortset fra det, var spørgsmålene nemme at forstå og ikke så svære at folk uden baggrund i sikkerhed ville kunne forstå dem.	(5) Strongly Agree	Uncertain	overflødig tekst. Når først man fangede det mønster, at den info ikke blev brugt til noget, og blev ved med at komme i de senere quizzer, kunne man godt have tendens til at springe den del over.	No	Yes	I just had a Cours in security	man havde ikke nok tid eller sørgte for at give dem alle tid eller droppe det. Dermed sagt så var det en fint oplevelse men designet af hvor teksten er og hvordan man skal løse det hænger ikke sammen. Hvad var grundlaget til at bruge en ekstern server, der jo intet i den der er skadeligt.	
Agree (4)	Agree (4)	Strongly Agree (5)	(2) Easy	It's sikkerhed ryder meget i min hverdag for tiden og mange af begreberne er front of mind i min hverdag for tiden, så på den måde føltes, specielt de første opgaver, meget lette. Den sidste opgave med mailene var mere udfordrende.	(5) Strongly Agree	Uncertain	En smule rollespil er altid godt for at blive draget mere ind i en oplevelse.	Uncertain	Yes	Det var nogle fine forklaringer, som gjorde det jordnært.	Svært at fokusere når folk taler omkring en. Man kan godt komme til at føle sig presset til ikke at læse tingene grundigt igennem.	
Agree (4)	Agree (4)	Agree (4)	(2) Easy	Some of the questions is could be interpreted as "trick questions", which could be more precise.	(5) Strongly Agree	Yes		Yes	Yes	Specielt de gange hvor jeg svarede forkert, havde jeg god grund til at reflektere over, hvorfor jeg svarede som jeg gjorde.		
Agree (4)	Disagree (2)	Neither agree nor disagree (3)	(2) Easy		(3) Neither disagree nor agree	Uncertain		No	Yes			

## A.14 Questionnaire graphs

### 5. Questions Focused Attention

● Strongly Disagree (1) ● Disagree (2) ● Neither agree nor disagree (3) ● Agree (4) ● Strongly Agree (5)

I lost myself in this experience.

The time I spent using "Insider Threat Course" just slipped away.

I was absorbed in this experience.

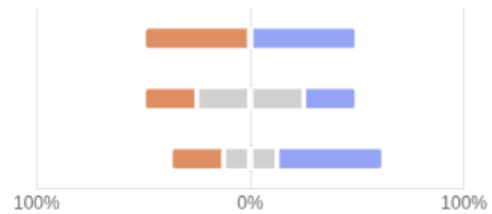


Figure 77: UES-SF Focused Attention

### 6. Questions Perceived Usability

● Strongly Disagree (1) ● Disagree (2) ● Neither agree nor disagree (3) ● Agree (4) ● Strongly Agree (5)

I felt frustrated while using this "Insider Threat Course".

I found this "Insider Threat Course" confusing to use.

Using this "Insider Threat Course" was taxing

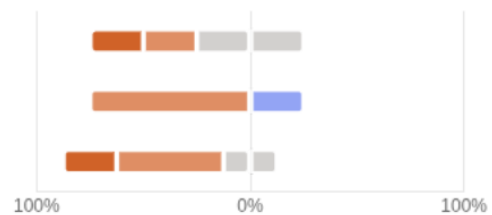


Figure 78: UES-SF Perceived Usability

### 7. Questions Aesthetic Elements

● Strongly Disagree (1) ● Disagree (2) ● Neither agree nor disagree (3) ● Agree (4) ● Strongly Agree (5)

This "Insider Threat Course" was attractive

This "Insider Threat Course" was aesthetically appealing

"Insider Threat Course" appealed to be visual senses.

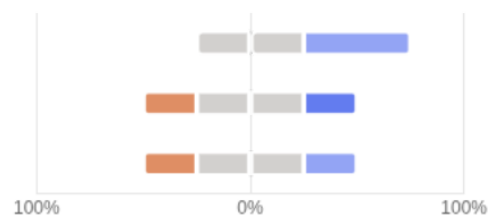


Figure 79: UES-SF Aesthetic Elements

8. Questions Reward Factor

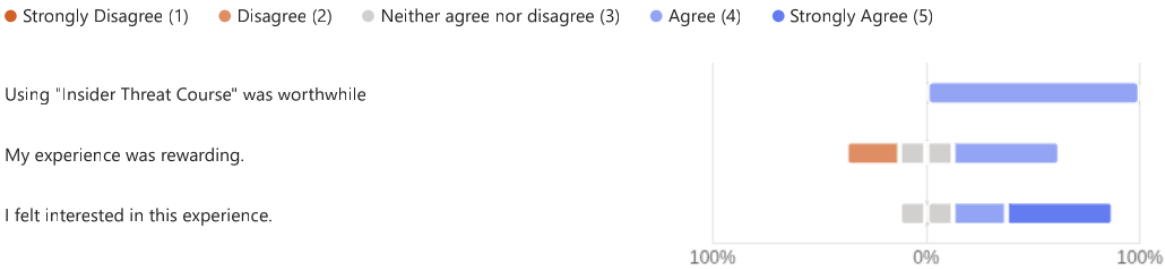


Figure 80: UES-SF Reward Factor