Bridging the Cybersecurity Talent Gap Through On-The-Job Training

CS6727 Cybersecurity Practicum

Nasar Patrick Dike
School of Cybersecurity and Privacy
Georgia Institute of Technology
Atlanta, Georgia, USA
dike36@gatech.edu

ACKNOWLEDGEMENTS

Special appreciation is extended to the Information Security team at Intercontinental Exchange for their permission to conduct this research within their operations and for their invaluable insights and contributions, which have greatly enriched this study. Additionally, heartfelt thanks to Professor Ahamad and Professor Kuerbis for challenging my initial proposal and guiding me towards a project that ignited a passion within me as my research progressed.

I would also like to express my deepest gratitude to my mother, whose unwavering faith and encouragement have been my anchor throughout this Masters journey. Her belief in my abilities convinced me that I was more than capable of excelling at Georgia Tech, even during times of doubt. I owe all my successes and future achievements to her enduring support and love.

TABLE OF CONTENT

Abstract

The cybersecurity talent gap is a critical issue that threatens both economic stability and global security. This paper addresses the gap by proposing an on-the-job training program designed to bridge the divide between current hiring practices and the industry's evolving needs. Traditional recruitment often overlooks candidates with non-traditional backgrounds who possess transferable knowledge and skills crucial for cybersecurity success. The proposed program focuses on training in incident response as a case study, demonstrating how targeted on-the-job training can effectively develop the necessary skills within the broader cybersecurity field. Detailed implementation and evaluation plans ensure the program's efficacy, incorporating pre- and post-training assessments, performance metrics, and practical exercises. The expected outcomes include significant improvements in participant skills and organizational security posture.

Keywords: Cybersecurity talent gap, on-the-job training, inclusive hiring practices, cybersecurity education, incident response, practical exercises, evaluation

I. INTRODUCTION

In today's digital age, cybersecurity has become a cornerstone of both economic stability and national security. The proliferation of cyber threats and the increasing complexity of cyberattacks have underscored the necessity for a robust cybersecurity workforce. Despite the growing demand, there is a significant gap between the number of available cybersecurity professionals and the needs of the industry. According to the International Information System Security Certification Consortium, (ISC)², Cybersecurity Workforce Study 2023, the global shortage of cybersecurity professionals is at a staggering 4 million. The demand for skilled defenders outpaces the supply, leaving organizations vulnerable to cyber threats [24].

The cybersecurity talent gap is not only a numbers game but also a matter of skills mismatch. Many organizations report that traditional hiring practices and academic programs do not adequately prepare candidates for the real-world challenges they will face. For example, 92% of cybersecurity professionals indicate that their organizations have significant skills gaps, particularly in areas such as cloud security (35%), AI/machine learning (32%), and zero trust (29%). This gap between supply and demand is exacerbated by a rapidly evolving threat landscape, where new skills and knowledge are constantly required. The impact of this workforce gap is profound, leading to increased risk of data breaches, financial losses, and compromised national security. According to the Fortinet 2024 Cybersecurity Skills Gap Global Research Report, 53% of respondents reported that breaches cost their organizations over $1 million in 2023, and 58% of IT decision-makers identified the top cause of security breaches as IT/security staff lacking cybersecurity skills and training [3]. As organizations scramble to protect their digital frontiers, the need for innovative solutions to bridge this gap has never been more urgent.

The primary objective of this paper is to propose a viable solution to bridge the cybersecurity talent gap through an on-the-job training program. This program is designed to address the shortcomings of current hiring practices, which often exclude candidates with non-traditional backgrounds but who possess relevant knowledge and soft skills crucial for cybersecurity success. The same Fortinet report shows that 91% of employers prefer hiring candidates with certifications, yet finding such candidates remains a challenge, with over 70% of organizations struggling to find qualified professionals as the gap increases. By focusing

on incident response training as a case study, this paper aims to demonstrate the effectiveness of targeted on-the-job training in developing the necessary skills within the broader cybersecurity field.

This proposed solution is inspired by insights from Chee H. Tey's analysis, which highlights the importance of diversifying the hiring pool and investing in upskilling of employees [17]. By broadening recruitment to include individuals with varied backgrounds and providing comprehensive training, organizations can effectively fill their cybersecurity gaps.

The scope of this paper includes a detailed analysis of the current cybersecurity workforce, the design and implementation of an incident response training program. It provides detailed implementation and evaluation plans, discusses expected outcomes, potential challenges, and limitations, and suggests future work to scale the initiative.

II. PROJECT DESIGN

Background

In my role as a Senior Cybersecurity Engineer specializing in Digital Forensics and Incident Response (DFIR), I was tasked with training a new cohort of analysts who joined our organization through an acquisition. These analysts had previously focused exclusively on Data Disclosures and Data Loss Prevention (DLP) due to the siloed nature of their former organization. This narrow focus limited their exposure to the broader spectrum of cybersecurity threats and robust incident response protocols.

The goal was to integrate these analysts into our team, equipping them to handle our full incident response plan having little to no prior knowledge of the sort. They needed to learn to triage live alerts and manage real incidents spanning various threat objectives across the CIA Triad (Confidentiality, Integrity, and Availability). This was a significant expansion from their previous roles, which concentrated mainly on confidentiality issues.

This unique situation provided an ideal control group to validate that individuals with essential soft skills and transferable cybersecurity knowledge could be effectively trained on the job to handle broader security challenges. By training these analysts in a diverse range of cybersecurity threats and responses, I was able to demonstrate that targeted on-the-job training could bridge the existing knowledge gaps and significantly upskill the talent available to an organization.

Research

To ensure the training program is aligned with industry guidelines and frameworks, I undertook a comprehensive review of existing standards and best practices. This involved aligning the curriculum with frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the National Initiative for Cybersecurity Careers and Studies (NICE) Cybersecurity Workforce Framework, and relevant ISO standards. This alignment ensures that the training program is not only applicable to our organization but can also be generalized and applied across the industry.

Industry Guidelines and Frameworks:

NIST (National Institute of Standards and Technology): Provides a policy framework for computer security guidance, helping private sector organizations assess and improve their ability to prevent, detect, and respond to cyber-attacks. In particular, the NIST SP 800 series offers detailed guidance on a wide range of cybersecurity topics, including risk

management, incident response, and security operations [8] [9]. NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework: Defines and categorizes cybersecurity work, offering a common lexicon to describe tasks, knowledge, and skills required for various cybersecurity roles [10]. ISO/IEC 27035: Specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system [5]. OWASP (Open Web Application Security Project): Offers extensive guidelines and tools for web application security, providing resources to help organizations understand and improve their application security posture [11]. SANS Institute: Renowned for its comprehensive cybersecurity training and certification programs, SANS provides white papers and guidelines that inform best practices in various areas of cybersecurity [14] [15]. CIS (Center for Internet Security): Provides a set of globally recognized best practices for securing IT systems and data against the most pervasive attacks.

In addition to aligning with these frameworks, I also incorporated feedback from industry experts and peers to ensure the relevance and applicability of the training content. These measures helped ensure that the training program is not only applicable within my organization but can also be generalized and applied across the industry.

Pre-Assessment

To prove the effectiveness of the training and qualify the assumptions of my solution, it was essential first to understand the baseline knowledge of the trainees. I created a pre-assessment skills survey specifically tailored for the Digital Forensics and Incident Response (DFIR) specialization **Appendix A**. The pre-assessment survey was developed based on established guidelines and frameworks alongside our organization's Cyber Incident Response Plan (CIRP). This approach ensured the survey effectively gauged the existing skill levels of the trainees relative to the competencies required to perform their roles successfully.

The pre-assessment served two main purposes:

1. **Contextualizing the Background of the Control Group:** It was crucial to establish that the new analysts were relatively novice in the realm of Incident Response. This baseline understanding helped frame the training objectives and set realistic expectations.
2. **Informing Curriculum Development:** The results of the pre-assessment were instrumental in shaping the curriculum. By identifying specific knowledge gaps and areas needing improvement, I could tailor the training program to address these deficiencies directly.

Curriculum Design

Developing the curriculum involved establishing clear learning objectives and allocating time to each area based on the pre-assessment results. The learning objectives were informed by our CIRP and aligned with established industry guidelines mentioned in the Project Design section.

These competencies are essential for any analyst to perform their job functions effectively. The curriculum was designed to ensure that trainees developed both foundational and advanced skills necessary for comprehensive incident response. This approach was tailored to address the specific knowledge gaps identified in the pre-assessment, ensuring that more time and resources were dedicated to areas where trainees demonstrated the greatest need for improvement. By combining the internal CIRP requirements with external best practices, the

curriculum aimed to provide a holistic training experience. This ensured that trainees not only met the specific needs of our organization but also acquired skills and knowledge that are broadly recognized and valued across the cybersecurity industry.

The defined learning objectives for each module stem from the core principles of the CIA Triad: Confidentiality, Integrity, and Availability. For example, in the realm of confidentiality, trainees learned to understand and mitigate threats that compromise data confidentiality, such as unauthorized file transfer or sensitive materials being forwarded to a personal email.

The learning objectives closely mirrored these relationships between the CIA Triad and specific threat categories or objectives. They blended pertinent industry knowledge with our internal procedures and instructions, ensuring that trainees were well-equipped to adhere to both general best practices and specific organizational protocols. By focusing on these comprehensive learning objectives, the curriculum aimed to build a robust foundation of skills and knowledge, enabling trainees to effectively manage and respond to a wide range of cybersecurity threats and incidents.

On-the-Job Training Blueprint		
Month	**New Analyst - Cybersecurity DFIR**	
S/N	**Technical Skills and Competencies**	**Training Duration (Month)***
1	**Onboarding/Access Requests**	**1st Month**
2	**General Tools Training**	**1st Month**
3	**Email Analysis**	**2nd Month**
4	**Incident Handling**	**2nd - 6th Month**
5	**Data Loss Prevention (DLP)**	**2nd month**
6	**Host-based Analysis**	**2nd Month**
7	**Network-based Analysis**	**3rd Month**
8	**Endpoint Detection and Response (EDR) / Antivirus**	**3rd - 4th Month**
9	**Threat Intelligence and Detection**	**4th - 6th Month (out of scope for practicum project)**
10	**Tabletop Exercise and Assessment**	**6th Month (After Practicum)**
	Total Duration	**6 Months**

Table 1: Curriculum Design

Appendix 2 outlines the full curriculum. Each module within the curriculum is centered around a specific technical skill or competency of focus with an estimated duration for learning. The curriculum details the knowledge that trainees should achieve by the end of each module, ensuring they understand the theoretical and practical aspects necessary for their roles. Expected abilities are also outlined, specifying the actions that trainees should be able to confidently perform upon completing each module. While the range of application can vary across different organizations, the curriculum provides a useful template, helping trainees understand what tools are available in their

environment and what learning objectives are commonly associated with each tool. Performance evidence, which is covered in depth in the later Evaluations section, serves as a means of assessing how well trainees have understood each module through an applied learnings approach.

The areas in scope for this report include:

- **Onboarding and Access Requests:** In this initial module, the training curriculum emphasizes the importance of familiarizing trainees with our Corporate Information Security Policy (CISP) and the CIRP. These two critical documents were developed in alignment with the NIST framework, providing a robust foundation for our security protocols. This integration helps the new analysts understand their roles within the broader organizational structure and sets clear expectations for their responsibilities in their new roles. By grounding the onboarding process in these key documents, trainees gain an understanding of how their tasks fit into the larger context of the organization's cybersecurity efforts, ensuring they are well-prepared to respond effectively to incidents and uphold the organization's security standards.
- **General Tools Training:** Hands-on training with security information and event management tools and other critical cybersecurity tools.
- **Email Analysis:** Techniques for analyzing email headers, detecting phishing attempts, and handling malicious attachments.
- **Incident Handling:** Procedures for triaging, investigating, and resolving various types of cybersecurity incidents.
- **Data Loss Prevention (DLP):** Strategies for classifying data, handling escalations, and reviewing daily DLP incidents.
- **Host-based Analysis:** Skills for investigating endpoints, performing memory forensics, and understanding adversary tactics.
- **Network-based Analysis:** Methods for analyzing network traffic, detecting anomalies, and utilizing tools like Wireshark for packet capture analysis.
- **Endpoint Detection and Response (EDR):** Techniques for responding to threats on endpoints, performing forensic investigations, and using EDR tools effectively.

Training Plans

Each module was accompanied by a tailored training plan designed to provide foundational knowledge on the learning objectives and a more specific internal use plan that outlines the tools and use cases pertinent to our organization. These training plans ensured that trainees received both a broad understanding of industry standards and the specific procedures and tools used within our organization. Below, I break down the contents of each training document, with corresponding appendices for detailed reference.

Email Analysis

The training plan for the Email Analysis Module, available in **Appendix C**, was created to equip individuals with the necessary skills to effectively identify, analyze, and mitigate inbound email-related threats, such as phishing emails, spam, and spoofing. It provides a detailed guide to understanding email protocols, security measures, and analysis techniques essential for maintaining a secure email communication environment.

The introduction highlights the shift from outbound DLP focus, that the trainees are familiar with, to addressing inbound email threats. It begins with an overview of email basics, explaining key protocols like POP, IMAP, and SMTP, and their secure versions. It emphasizes the importance of understanding these protocols to analyze emails effectively and ensure secure communication.

Following the basics, the document delves into email security protocols such as SPF, DKIM, and DMARC. These protocols are crucial for authenticating emails and preventing domain spoofing. Detailed explanations and examples illustrate how these protocols work and their advantages and limitations in protecting against email threats.

In the email analysis section, the document provides techniques for identifying malicious emails. It outlines indicators of phishing and spam emails, including sender indicators, message content, and suspicious links or attachments. The importance of email header analysis is also discussed, with guidance on examining key components to verify the legitimacy of emails.

The document then covers the email triage process, offering practical steps for handling and responding to different types of malicious emails. This includes verifying senders and domains, investigating message content, analyzing URLs and attachments, and categorizing and mitigating email threats. The emphasis is on a structured approach to ensure thorough investigation and effective response to email-based threats.

Data Loss Prevention (DLP)

The Data Loss Prevention (DLP) training document I developed provides an in-depth overview of strategies and technologies designed to prevent sensitive data from leaving our organization. An excerpt can be viewed in **Appendix D.**

It begins with a definition of DLP, highlighting its role in identifying, monitoring, and protecting data across various states—motion, rest, and use. The document emphasizes the importance of DLP in ensuring compliance and protecting intellectual property, addressing a range of threats from insider threats to data breaches.

Central to the training is data classification, which involves categorizing data based on its sensitivity and confidentiality to ensure appropriate protection measures. This process is crucial for prioritizing resources and implementing tailored security controls. The training also covers email DLP, explaining how to prevent data leaks by monitoring email messages for sensitive content and enforcing security policies to block or flag potential breaches.

Additionally, the document discusses network DLP, which focuses on monitoring and preventing unauthorized data transfers over internal and external networks. This includes inspecting web traffic and file transfers to enforce real-time policies. Endpoint DLP is also addressed, detailing how to secure data at the device level, preventing leaks through unauthorized actions such as USB drive usage or malware infections.

The document outlines specific responsibilities when investigating DLP incidents as a DFIR analyst. This includes reviewing alerts, verifying user permissions, contacting leadership for authorization, and escalating incidents involving sensitive data leaks. Procedures for handling unblock requests from users are also detailed, ensuring that business justifications are evaluated, and potential risks are assessed.

This section of the training was lighter than others because the test group was already well-versed in the subject matter. The primary focus was on familiarizing them with our internal tools and procedures. However, the scope should be

general enough for adoptability across organizations.

Incident Response

The Incident Response Training document in **Appendix E** provides a detailed framework for preparing analysts to manage cybersecurity incidents effectively. This supplemental learning plan covers Incident Handling, Host-Based Analysis, Network-Based Analysis, and Endpoint Detection and Response (EDR) & Antivirus (AV) learning objectives together. These areas are interlinked, with each section building on the previous one to closer imitate how actual incident response may look in real time, often times a threat may require different domains of analysis to find the root cause and an analyst should know how to pivot from one finding to the next.

The training begins with an introduction to Incident Response, emphasizing the importance of understanding the CIRP and CISP. It outlines the generally accepted lifecycle for responding to incidents, including preparation, detection and analysis, containment, eradication, recovery, and post-incident activity. This structured approach ensures that analysts can effectively minimize the impact of threats within the organization.

Additionally, key takeaways from “FOR508: Advanced Incident Response, Threat Hunting, and Digital" by the SANS Institute have been integrated into the training to enrich the curriculum [14]. The insights on establishing clear communication channels during an incident and the importance of having predefined roles and responsibilities provide practical advice that enhances the preparation phase. The emphasis on the necessity of comprehensive documentation and analysis during the post-incident phase is also included to reinforce the importance of learning from past incidents to improve future response efforts.

Host-based analysis focuses on examining individual systems (hosts) to detect, investigate, and mitigate security incidents. It provides guidance on analyzing system artifacts, log files, and registry settings in Windows operating systems. Various components such as file systems, directories, processes, and user accounts are covered, equipping analysts with the skills to identify and respond to malicious activities on host systems.

Network-based analysis is essential for examining and monitoring network traffic to detect and respond to security incidents. This section covers techniques for analyzing IP addresses, ports, protocols, and services, explaining how to identify normal and abnormal network traffic patterns. Understanding these patterns is crucial for detecting malicious activities like reconnaissance, lateral movement, command and control (C2) communications, and data exfiltration.

The Endpoint Detection & Response (EDR) & Antivirus (AV) section highlights the importance of these tools in modern cybersecurity strategies. EDR solutions provide advanced capabilities for detecting, investigating, and responding to threats that evade traditional antivirus measures. The document details how antivirus solutions use signature-based and behavior-based detection techniques to identify and mitigate malware. Analysts are trained on how to use these tools to quarantine suspicious files, block malicious activities, and conduct threat hunting and deep visibility investigations.

Implementation Plan

Implementation of the training program involved structured training sessions supplemented with the training plan documents. Each session was designed to cover the learning objectives in detail and provide hands-on experience with procedures, analysis techniques, and tools related to the module.

Training sessions were conducted in a collaborative environment, where I would explain the theoretical aspects of each topic followed by a demonstration of practical application. This included working through existing incidents or reviewing closed incidents saved for case study purposes. These practical demonstrations helped trainees understand how to apply their knowledge in real-life scenarios and what was to be expected of them once they began working on issues of the same category.

After covering the introductory training for each module, trainees were assigned alerts that aligned with the learning objectives. This hands-on practice was essential for reinforcing the concepts covered during the sessions. I and other team members were each assigned a trainee to shadow, providing guidance and sharing our experience as the trainees worked through the issues. This mentorship approach ensured that trainees received personalized support and feedback, enhancing their learning experience.

At the end of each module, trainees were expected to handle issues related to that category on their own. This not only tested their understanding and skills but also served as a practical evaluation of their readiness to operate independently. This approach allowed us to assess the effectiveness of the training in a real-world context and provided a clear measure of the trainees' progress.

By reviewing their work and providing constructive feedback in a contiguous manner, we ensured improvement and development of their skills.

III. EVALUATION METHODOLOGY

Live Response

Once a trainee completes a learning objective, they are added to a queue system used by all full-time DFIR analysts. Analysts receive alert tickets throughout their shift, originating from various sources such as monitoring tools, built detections, and employee reported incidents. These alerts are categorized according to the CIA triad as well as subcategories that directly relate to a learning objective. During the initial training period, trainees are kept out of the regular queue. However, as they progress through their training, they are gradually integrated into the queue by alert category, allowing them to gain real-world experience in their expected job functions.

For example, after completing the email analysis section of training, trainees are added to the queue to triage reported phishing alerts; once the trainees have mastered host-based analysis, they can receive alerts that come from Intrusion Detection Systems (i.e. EDRs). This iterative approach allows trainees to apply their newly acquired skills in a controlled, real-world environment, ensuring they can confidently handle incidents related to their training. By the time they complete their training, trainees should be able to independently manage a variety of alerts, demonstrating their readiness to perform as full-fledged Incident Responders.

Peer Review

To maintain high standards of incident response, every alert investigated by an incident responder goes through an anonymous peer review system. This process ensures that the investigation meets the acceptance criteria outlined by the CIRP. Incident Response peers are randomly assigned a collection of alerts to review quarterly, evaluating whether the correct procedures were applied.

The review contains several questions that the reviewer must answer to determine whether the correct procedures were followed. These questions vary depending on the alert but generally cover key aspects of the investigation.

Firstly, reviewers assess whether the appropriate containment actions were taken if applicable. This ensures that any immediate threats were neutralized to prevent further damage, adhering to the containment phase of the incident response lifecycle. For example, if a phishing email was reported, the reviewer checks if the email was quarantined and affected users were notified.

Next, the root cause analysis is scrutinized. Reviewers evaluate if the analyst accurately identified and summarized the root cause of the incident, which is critical for understanding how the incident occurred and preventing future occurrences. This aligns with the detection and analysis phase, where understanding the nature and scope of the incident is crucial.

The review also examines whether the correct business units impacted by the incident were identified and notified. This aspect ensures that all relevant stakeholders are informed, allowing for a coordinated response and recovery. Reviewers look at the work notes to verify that comprehensive exposure checks were performed, ensuring that all potential impacts were assessed and mitigated.

Lastly, the review looks at whether the incident description and work notes provide sufficient detail about the incident, including who was involved and why it occurred. This information is essential for post-incident analysis, helping to improve future responses and refine incident handling procedures.

If the review determines that all these aspects are adequately addressed, it confirms that the proper steps were taken. If not, the reviewer provides feedback to the analyst, detailing what was missing or done incorrectly. This feedback loop is vital for continuous improvement, helping analysts learn from their mistakes and ensuring that future incidents are handled more effectively.

This peer review system not only enforces compliance with internal procedures but also cultivates a culture of accountability and continuous improvement among incident responders. Trainees undergo rigorous evaluations, assessing their competence from incident detection to post-incident analysis. This comprehensive assessment approach guarantees that trainees evolve into skilled and effective responders, well-equipped to tackle the demands of their roles. Moreover, it provides a measurable framework for future implementers of on-the-job training programs to gauge the educational advantages.

Performance Metrics

The evaluation of trainees' performance relied heavily on the peer review process. This is integral to proving the efficacy of my proposed training plan because it provides a quantitative measure of their ability to apply learned skills in real-world scenarios. Based on the correctness of actions taken during their alert reviews, trainees were given a score out of 100, similar to academic assessments. Each peer review consists of 5-10 questions, and a score of 100 indicates that all questions are answered correctly.

Collecting the metrics for the trainees, detailed in **Appendix F,** yielded overwhelmingly positive results. An analysis of over 100 alerts handled by the trainees showed that they received perfect scores on 97% of their closed alerts.

Moreover, 31.6% of these correctly triaged alerts were true positives for malicious activity. This statistic is significant as it indicates that trainees not only handled false positives but also successfully identified and responded to actual security threats. This experience allowed trainees to follow the complete lifecycle of incident response multiple times, reinforcing their learning and building confidence in their skills.

The data convincingly demonstrates that the training program met its original objectives. Trainees displayed high performance metrics and proficiently managed true positive alerts, indicating that the program successfully prepared individuals with little to no prior experience for roles in cybersecurity. This achievement highlights the importance of incorporating hands-on, real-world experiences into the training curriculum and supports the strategy of progressively expanding trainees' responsibilities throughout the program as they onboard to a new cybersecurity role.

Post-Assessment

Building on the insights from the pre-assessment, the post-assessment was conducted to measure the growth in trainees' knowledge and skills after completing the training. This assessment was crucial in demonstrating the advances made by trainees in key DFIR competencies, highlighting both the areas of significant improvement and those requiring further attention. The post-assessment also included a feedback mechanism, enabling trainees to express their views on the training's impact, areas of strength, and potential improvements. This feedback is invaluable in refining future iterations of the training program to better meet the evolving needs of the cybersecurity field.

The following is a summary of observations from the Post-Assessment survey, the link with visualizations is available in **Appendix G**

Organizational Understanding

Initially, only 57.1% of respondents were at intermediate or higher levels. Post-training, this number increased to 71.4%, demonstrating a 14.3% improvement in understanding organizational structures.

Incident Response Life Cycle

Confidence in managing the incident response life cycle saw a remarkable increase. Pre-training, no respondents rated themselves as advanced; post-training, this changed to 28.6% of respondents feeling confident at an advanced level.

SIEM/Log Analysis

Proficiency in SIEM/log analysis showed substantial growth. Initially, only 28.6% felt confident at an intermediate level or above; post-training, this rose to 57.1%, reflecting a more than double increase in proficiency. This was a major focus in both the General Tools Training and Host/Network-Based Analysis.

Email Analysis

For the task of analyzing email headers, there was an impressive jump from 28.6% of trainees feeling at least intermediate pre-training to 71.4% post-training, indicating enhanced capabilities in identifying email-based threats.

DLP Incident Handling

There was a notable leap in handling DLP alerts, with those feeling advanced in their skills increasing from 28.6% to 85.7%. This stark improvement underscores the transferable knowledge yielding immediate results within a new security capacity.

Feedback Summary

The feedback from trainees on the training session was predominantly positive, highlighting the structured and comprehensive nature of the content. Participants particularly appreciated the Data Loss Prevention (DLP) section for its clear and practical approach, noting it as a standout feature that set this

training apart from previous experiences. The training was commended for its organization and adaptability to different skill levels, ensuring all participants could engage effectively. However, some participants mentioned difficulties with the frequent use of acronyms and technical jargon, suggesting the inclusion of a glossary or database might help in clarifying these terms. Additionally, there was a consensus on the need for more practical exercises, which, while the theoretical aspects were well-addressed, would provide beneficial hands-on experience to solidify the trainees' learning before adding them to the queue for live response to active alerts.

Impact

The evaluation conclusively demonstrates that on-the-job training is a powerful solution to bridging the cybersecurity talent gap. By integrating real-world experience, this method ensures that trainees are not only theoretically knowledgeable but also practically skilled. The success of this approach hinges on selecting individuals with foundational knowledge, transferable skills, and a strong ability to learn and adapt.

This program has shown that engaging, iterative, and practical training can effectively transform these individuals into competent incident responders. The overwhelmingly positive results underscore the potential of on-the-job training to address skill shortages in the cybersecurity field, ultimately contributing to a workforce capable of responding to cyber threats. This approach validates the initial proposal that with the right foundational prerequisites, on-the-job training can bridge the cybersecurity talent gap effectively and sustainably.

IV. LIMITATIONS

The scope of my project was specifically focused on Incident Response (IR). While the overarching aim is to present a case for on-the-job training across all realms of cybersecurity, IR is a particularly challenging specialization that demands extensive domain knowledge. This project did not place significant emphasis on other cybersecurity disciplines such as application security (AppSec), governance, risk, and compliance (GRC), red team activities, or penetration testing, aside from their relevance to organizational structure and interactions with our team. Despite this, the training template proposed can and should be adapted for other cybersecurity domains, with individual management determining the specific areas of focus. This limitation should not detract from the broader commentary on the industry's need for comprehensive on-the-job training to bridge a gap in the talent.

Part of my proposed solution involves expanding the background of candidates for open cybersecurity roles. However, my test group consisted solely of cybersecurity professionals with varying levels of experience. Ideally, I would have conducted my own hiring process to include individuals from non-traditional backgrounds, demonstrating the viability of training those without prior cybersecurity experience. Unfortunately, such an approach would be beyond the scope and authority granted to conduct this research. Nonetheless, the test group, which previously focused only on DLP, approached other domains with minimal prior exposure, thus providing a valid context for evaluating the training program's effectiveness.

Access requests and resource constraints impacted the execution of some planned simulated exercises. Coordinating organizational onboarding and aligning with the individual schedules of trainees affected the proposed curriculum timeline. Despite these

logistical challenges, all the primary learning objectives set out in the curriculum were successfully covered.

The training program was heavily based on our organization's Cyber Incident Response Plan, which follows NIST and NICE frameworks. This focus presented a challenge in making content relevant to both our specific organizational practices and the larger cybersecurity industry. While I rooted the training in shared standards and frameworks to mitigate bias, some degree of organizational specificity remained.

Additionally, there was a bias towards Windows operating systems within the training content. This focus aligns with our organization's primary operating environment but may not be as applicable to environments that predominantly use other operating systems.

In conclusion, while the project successfully demonstrated the efficacy of on-the-job training within the context of Incident Response, broader application across all cybersecurity domains will require further adaptation and validation. The limitations identified highlight areas for future research and development, reinforcing the need for flexible and comprehensive training programs tailored to the diverse needs of the cybersecurity industry.

V. FUTURE WORKS

Looking ahead, there are several key areas where this training program can be refined and expanded to maximize its impact and applicability across the broader field of cybersecurity. I plan to take detailed feedback from both the training sessions and the post-assessment evaluations, as well as constructive input provided by my peers throughout the creation of this curriculum and refine the curriculum and materials of the training program. Outside of the confines of this project scope I can work on improving both breadth and depth in areas identified as lacking. By continuously iterating and enhancing the training content, I can ensure it remains relevant and impactful.

I also aim to make this training model adoptable across various cybersecurity disciplines. To achieve this, I will research other specializations within cybersecurity and collaborate with domain experts to tailor the training plan to different fields while retaining the core approach demonstrated in this project. This will involve creating specialized modules for areas such as application security, governance, risk and compliance (GRC), red teaming, cloud security, automation, SecOps, ensuring a comprehensive training solution for all cybersecurity roles.

The dissemination of this training model is crucial for its scaling and adoption. I plan to submit proposals to both local and global security conferences, such as RenderATL, BSides ATL, and HushCon, to present this training model to a wider audience. At the time of writing this report, my company is encouraging submissions to Black Hat's call for papers, and if selected, submitters can host a briefing at BlackHat USA to present their topic.

Something I am most excited about is my recent acceptance into the Cyber Security Experts Association of Nigeria (CSEAN). This provides another platform for showcasing this research. Their annual summits offer an opportunity to present on approved topics, and I aim to prepare my project for such a presentation in a country that suffers a direct impact of the gap in cybersecurity talent.

VI. CONCLUSION

I interviewed Dan Paltiel, Director of Cyber Threat Intelligence at Intercontinental

Exchange, who exemplifies how non-traditional backgrounds can be an asset in the cybersecurity space [12].

Dan started his academic journey as a history major at a liberal arts school in Boston, Massachusetts, and further enriched his education studying Arabic in Jordan. His professional career began with an internship at a think tank in Washington, DC, where he tracked global militant organizations and their funding streams. This work was heavily research-oriented, involving extensive analysis, monitoring, and reporting.

Dan's burgeoning interest in security led him to seek opportunities in the field. He eventually joined an IT policy program where he would research and maintain record of ongoing policy issues. His experience in tracking policy issues and his deep research skills were directly applicable to threat intelligence and his role increasingly shared responsibilities with that of a cyber threat intelligence analyst. When a financial institution had an opening on their Threat Intel team, Dan’s unique combination of skills made him a strong candidate, ultimately leading to his first cybersecurity role.

Despite lacking the traditional technical education typically associated with a career in threat intelligence, Dan's on-the-job training allowed him to acquire the necessary technical skills. His ability to apply his research expertise and understanding of IT policy facilitated his growth and success in the role.

Dan's journey demonstrates how skills acquired in any industry or background can be effectively applied to a security profession. His experience highlights the need to broaden the hiring pool to include individuals with diverse, non-traditional backgrounds. By assessing their unique talents and investing in on-the-job training programs modeled after my research, organizations can cultivate skilled security professionals. This approach not only meets the immediate demand for cybersecurity personnel but also helps develop a talented and qualified workforce capable of addressing future challenges. Investing in diverse talent and practical training is a viable solution to bridging the cybersecurity talent gap and ensuring long-term industry stability and security. The training plan detailed in this paper serves as a model for how such programs can be structured and implemented effectively, demonstrating the potential for widespread adoption and success.

REFERENCES

[1] Center for Internet Security (CIS). (2020). *CIS controls version 7.1*. Retrieved from https://www.cisecurity.org/controls/cis-controls-list/

[2] Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Incident response training*. Retrieved from https://www.cisa.gov/resources-tools/programs/Incident-Response-Training

[3] Fortinet. (2024). *2024 cybersecurity skills gap report*. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

[4] Infosec Institute. (n.d.). *Email Analysis*. Retrieved from https://resources.infosecinstitute.com/topic/analyzing-smtp-traffic/

[5] International Organization for Standardization (ISO). (2023). *Information technology — Security techniques — Information security incident management* (ISO/IEC 27035:2023). Retrieved from https://www.iso.org/standard/78973.html

[6] Microsoft. (n.d.). *Recognize and Avoid Phishing Attacks*. Retrieved from https://www.microsoft.com/en-us/security/business/security-101/avoid-phishing-scams

[7] Mwila, K. A., & Phiri, J. (n.d.). Data Loss Prevention. Unpublished manuscript, University of Zambia, Lusaka, Zambia.

[8] National Institute of Standards and Technology (NIST). (2012). *Computer security incident handling guide* (Special Publication 800-61 Revision 2). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[9] National Institute of Standards and Technology (NIST). (2007). *Guidelines on electronic mail security* (Special Publication 800-45 Version 2). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45v2.pdf

[10] National Initiative for Cybersecurity Careers and Studies. (n.d.). *NICE Framework*. Cybersecurity & Infrastructure Security Agency. Retrieved from https://niccs.cisa.gov/workforce-development/nice-framework

[11] Open Web Application Security Project (OWASP). (n.d.). *OWASP Email Security Testing Guide*. Retrieved from https://owasp.org/www-project-email-security-testing-guide/

[12] Paltiel, D. (n.d.). Interview by N. P. Dike. Retrieved from https://github.com/DK36/CS6767-Cyber-Sec-Practicum/blob/main/Interview with Daniel Paltiel Intercontinental Exchange.m4a

[13] SANS Institute. (2012). *Incident handler's handbook*. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

[14] SANS Institute. (2023). *FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics* [Course Material]. SANS Institute.

[15] SANS Institute. (n.d.). *Email Security*. SANS Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/email-security

[16] Techopedia. (n.d.). *Hardest cybersecurity jobs to fill and essential certifications*. Retrieved from https://www.techopedia.com/hardest-cybersecurity-jobs-to-fill-and-essential-certifications

[17] Tey, C. H. (2022). *Examining the cybersecurity workforce gap: An analysis of the disconnect between industry and academia* (PUBP 6727). Georgia Institute of Technology.
[18] World Economic Forum. (2024). *Strategic cybersecurity talent framework 2024*. Retrieved from https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf
[19] Anti-Phishing Working Group (APWG). (n.d.). *Phishing Activity Trends Report*. Retrieved from https://apwg.org/trendsreports/
[20] Attack Mitre. (n.d.). Retrieved from https://attack.mitre.org/
[21] Cyber Kill Chain. (n.d.). Try Hack Me Cyber Kill Chain Write Up. Retrieved from https://medium.com/@kumarishefu.4507/try-hack-me-cyber-kill-chain-write-up-d076d323fdc8
[22] Trellix. (n.d.). What is Endpoint Detection and Response. Retrieved from https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-detection-and-response/
[23] XPLG. (n.d.). Windows Server Security Events List. Retrieved from https://www.xplg.com/windows-server-security-events-list/
[24] ISC². (2023). *ISC² Cybersecurity Workforce Study 2023*. Retrieved from https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e&hash=CE6762D811935593F5C04AAB49DF33DF

Appendix A: Pre-Training Skills Assessment

https://docs.google.com/forms/d/1AwoyBFdBBIc9XAZPqIyuBziGoznMwVYlf6Mzb58Xwao/viewanalytics

Appendix B: Training Curriculum Outline

On-the-Job Training Blueprint		
Month	**New Analyst - Cybersecurity DFIR**	
S/N	**Technical Skills and Competencies**	**Training Duration (Month)***
1	**Onboarding/Access Requests**	1st Month
2	**General Tools Training**	1st Month
3	**Email Analysis**	2nd Month
4	**Incident Handling**	2nd - 6th Month
5	**Data Loss Prevention (DLP)**	2nd month
6	**Host-based Analysis**	2nd Month
7	**Network-based Analysis**	3rd Month
8	**Endpoint Detection and Response (EDR) / Antivirus**	3rd - 4th Month
9	**Threat Intelligence and Detection**	4th - 6th Month (out of scope for practicum project)
10	**Tabletop Exercise and Assessment**	6th Month (After Practicum)
	Total Duration	6 Months

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
1	**Onboarding/Access Request**	• Organizational Structure • Roles and Responsibility • Incident Response Life Cycle • Incident Response Plan • Incident Escalation Procedure • Key Stakeholder group	• Familiar with incident management and response procedure for detection, reporting and handling of incidents • Familiar with remediation and resolution of cyber incidents at organizational level • How to communicate incidents to different critical stakeholders • Cross-region communicate and collaboration	• Incident and Case Handling • Incident Response Procedure/playbook • Email Notification/Response Template • Cross-region handover • Different accounts	1st Month	• Able to identify various SME • Complete CISP and CIRP • Familiarity with CMDB tool
2	**General Tools Training**	• [SIEM Tools] • CMDB service • Email Security Appliance • Email Archive • Domain Name Server resolution service	• Able to access and use org tools	• Cyber Dashboard with tools • Tool Documentation(s)	1st Month	• Able to access org tools
3	**Email Analysis**	• Lifecycle of an email (SMTP) • Analyze message headers and gauge email authenticity using SPF and DKIM • Extract and review document metadata present • Merge event logs and perform advanced filtering to easily get through large events • Malicious attachment analysis • Phishing Response Tool	• Perform log analysis • Case writeup and handling • Phishing email analysis • Identify if any email clickers • Analyze email header and authenticity • Malicious attachment analysis • Malicious url analysis • Blocking of C2/phishing Domains • Email removal/quarantine • Ticket queue	• Phish email analysis tool • Case management • Malware file or link analysis • Email releases • ticket	2nd Month	• Able to manage Email Triage Queue • Able to triage Phish Report Incidents without assistance • Able to triage tickets

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
4	**Incident Handling**	• Phish Report Triage • Ticket handling • Incident handling	• Handles phish reports • Basic ticketing and cyber-Incident investigation	• varies	2nd month – 6th month	• Able to triage cases/ cyber incidents without assistance
5	**DLP**	• Classification of Data • Escalation • Review Daily DLP	• Able to work on DLP daily triage	• DLP tool(s)	2nd month	• Able to work on DLP Daily triage Incidents
6	**Network-based Analysis**	• Network protocol analysis • Hypertext Transfer Protocol (HTTP) • Domain Name Service (DNS) • File Transfer Protocol (FTP) • Server Message Block (SMB) and related Microsoft protocols • Simple Mail Transfer Protocol (SMTP) • Log collection, aggregation, and analysis • Pcap/wireshark analysis - etraining	• Analyze network traffic • Architecture and core functionality • Tunneling • Fast flux and domain name generation algorithms (DGAs) • Logging methods • Amplification attacks • Filtering network activity to identify indicators of compromise • Assessing encrypted network traffic with multiple data sources • Identifying compromised host beaconing with proxy server logs	• Packet Capture Analysis • Wireshark • Network investigations cases • SIEM tools - log analysis ○ Syslog ○ Windows Event ○ HTTP server logs ○ Firewalls, Intrusion Detection Systems (IDS), ○ Network Security Monitoring (NSM) Platforms ○ Log collection, aggregation, and analysis ○ Web proxy server examination	3rd month	• Able to triage network-based cases/ cyber incidents without assistance • Able to review packet capture using wireshark *

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
7	**Host-based Analysis**	• Incident Response and Intrusion Forensics Methodology • Advanced Incident Response and Threat Hunting Tactics and Procedure • Cyber-kill chain strategies • ATT&CK - MITRE • Web Browser Forensics • Windows Artifact Analysis • Registry Analysis, Application Executions • Memory Forensics • Timeline Analysis • Advanced Adversary & Anti-forensics Detection • Living of the land techniques • scenario	• Track a suspect's activity in browser history and cache files and identify local file access • Examine which files a suspect downloaded • Determine URLs that suspects typed, clicked on, bookmarked, or were merely re-directed to while web browsing • Investigate browser auto-complete • Identify artifact and evidence locations to answer crucial questions, including ○ application execution, ○ file access, ○ data theft, ○ external device usage, ○ device geolocation, ○ Browser history, ○ file download, ○ anti-forensics, ○ detailed system, ○ and user activity ○	• Endpoint Detection and Response (EDR) console and agents • ATT&CK - MITRE's Adversarial Tactics, Techniques, and Common Knowledge	2nd & 3rd Month	• Able to triage host-based cases/tickets without assistance
8	**Endpoint Detection and Response (EDR) / Antivirus**	• Hands-on exercise modeled after real-world attack • Parent Child Processes • Common process	• Respond, detect, scope, and stop intrusions and data breaches. • Identify compromised and affected systems • Perform damage/compromise assessments, such as:	• Endpoint Detection and Response (EDR) console and agents • ATT&CK - MITRE's Adversarial Tactics, Techniques, and Common Knowledge • Kill process	• 3rd – 4th month	• Threat Hunt • Investigate Host • Able to perform forensic investigation on given host

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
			○ Identity attack mechanism ○ Identify and track malware beaconing to C2 ○ Memory analysis ○ Registry analysis ○ Privilege escalation ○ Lateral movement analysis ○ Deep-dive timeline creation and analysis ○ Detect anti-forensics and hiding techniques ○ Data exfiltration • Contain and remediate incidents • Organize findings for use in ○ incident response, ○ internal investigations, ○ intellectual property theft inquiries, ○ and civil or criminal litigation.	• Quarantine host		
9*	**Threat Intelligence and Detection**	• Cyber intelligence • Emerging threats, perpetrators, doctrines, and methods of operations	• Gather intelligence with OSINT platforms and tools • Manage the research, analysis, and data integration across wide variety of information sources/ intel feeds • Determine tactics, techniques and procedures used for intrusions and attacks • Articulate significance of evolving cyber security threats to global cyber team, critical decision	• Cyber intelligence feeds • Regulator/Gov • 3rd Party Intel Vendor • Incident response and threat hunting	• 4^{th} - 6^{th} month	• Threat assessment and case write up

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
			makers and senior management in organization • Present impact assessment			
10	**Tabletop Exercises***	• Full Incident Response Life Cycle Walkthrough	• Be able to Respond to a simulated breach and follow the incident response life cycle all the way through: ○ Mainly **Identification** ○ **Containment** ○ **Eradication** ○ **Recovery** ○ And **Lessons Learned**	• Varies	• 3rd month and again on 6th month	• No missed alerts • Indicators of Compromise identified • Root cause identified • Threat contained and eradicated where applicable

* out of scope of practicum project

Appendix C: Email Analysis Training Plan (excerpt)

Full Training plan available at: https://github.com/DK36/CS6767-Cyber-Sec-Practicum/blob/main/Email%20Security.pdf

INDICATORS OF MALICIOUS EMAILS

Most diligent users will report emails that they were not expecting to receive. Here are a few indicators to investigate and determine whether these emails may be malicious. The general term for these is "Phishing Emails." A phishing email is a fraudulent attempt by malicious actors to deceive individuals into divulging sensitive information such as passwords, credit card numbers, or personal data. These emails often appear to be from legitimate sources like banks, government agencies, or well-known companies. They typically urge recipients to click on links, download attachments, or provide information through forms designed to steal personal or financial information.

…

EMAIL TRIAGE

Not all malicious emails can be handled the same way, but here is a brief guide, that will give you an idea of what steps you need to take to successfully mitigate an email threat.

1. CHECKING THE SENDER/DOMAIN

Verify the authenticity of the sender and the domain from which the email was sent looking out for indicators mentioned in the previous section.

- **Check Domain Reputation:**
    - Use tools to check the reputation of the sender's domain, there are open-source tools like phishtank or VirusTotal in addition to tools unique to each organization.
    - Look for domains known to be associated with spam or malicious activity.
- **SPF, DKIM, and DMARC:**
    - Ensure the email passes SPF, DKIM, and DMARC authentication checks.
    - Verify whether the sender is internal, trusted 3rd party, a supplier, client etc.
    - Leverage Email archiving tools (for ex. Global Relay) to review historical communications from the sender.

2. INVESTIGATING THE MESSAGE

Analyze the content of the email for signs of phishing or other malicious intent.

- **Content Analysis:**

    - Look for language that creates a sense of urgency or uses pressure tactics.
    - Identify spelling and grammar mistakes that are uncharacteristic of legitimate senders.
- **Request for Sensitive Information:**
    - Be cautious of emails requesting personal, financial, or login information.
- **Attachments and Links:**
    - Analyze any attachments or links for potential threats (detailed in subsequent sections).

3. INVESTIGATING URLS AND LINKS

Determine the safety and legitimacy of URLs and links included in the email.

- **Hover Over Links:**
    - Hover over any links to see the actual URL and ensure it matches the context of the email.
- **URL Reputation:**
    - Use tools to check the reputation of URLs (VirusTotal, urlscan.io).
    - Look for known malicious domains or newly registered domains.
    - Use sandbox environments to analyze the behavior of URLs without risking your main system (browserling.com is a free online option).

4. INVESTIGATING ATTACHMENTS

Safely analyze email attachments for malicious content.

- **Attachment Handling:**
    - Use secure methods to handle attachments, such as opening them in a sandbox environment.
- **Static and Dynamic Analysis:**
    - Perform static analysis to inspect the attachment without executing it.
    - Use dynamic analysis in a controlled environment to observe the behavior of the attachment.
- **Check for Macros:**
    - Be cautious of attachments prompting you to enable macros, which can execute malicious code.

5. CATEGORIZING EMAIL

Correctly categorize the email to determine the appropriate response.

- **Phish:**
    - Emails that attempt to steal sensitive information or deliver malware through deceptive tactics.

- **Spam:**
    - Unsolicited emails that are typically promotional or irrelevant but may not be directly harmful.
- **False Positive:**
    - Legitimate emails that were mistakenly flagged as suspicious.

6. CONTAINING THE THREAT

Objective: Take appropriate actions to mitigate the impact of malicious emails.

- **Exposure Check**
    - Determine whether the phish was an isolated incident or a campaign against multiple users. Determine who else may have received the email but hasn't reported it to identify the scope of your mitigation actions.
- **Quarantine the Email:**
    - Isolate suspicious emails to prevent further spread.
- **Contain threats**
    - For URL links, your organization should have firewalls or domain filtering tools available. A means of controlling destinations a user can visit online. (OpenDNS for example is a Domain Filtering tool by Cisco that allows you to block dns destinations for identities and control policy for various entitities)
    - Attachments that are malicious should be "blacklisted" using antivirus tools, this means that the hash of the file should be blocked with another security control across the network. If other users received the same email, they wouldn't be able to execute the malware once it's been blocked.
- **Block Sender/Domain:**
    - Block the sender or domain to prevent future emails from the same source.
- **Alert Relevant Parties:**
    - Notify the relevant teams or individuals about the threat to take further action.
- **Document and Report:**
    - Record your findings and actions taken in your incident management system for future reference and analysis.

Appendix D: Data Loss Prevention (DLP) Training Plan (excerpt)

Full Training plan available at: https://github.com/DK36/CS6767-Cyber-Sec-Practicum/blob/main/DLP%20Training.pdf

Data Classification

Data classification is the categorization of data based on its sensitivity, importance, and confidentiality to ensure appropriate protection measures are applied. This process assigns labels or tags to data sets, defining how they should be handled, accessed, and protected throughout their lifecycle. Typically, data is classified into categories such as public, internal use, confidential, and restricted, each with varying levels of access control and security requirements. Effective data classification enables organizations to prioritize resources and implement tailored security controls.

Domains

DLP solutions are typically categorized into several domains or types, each focusing on protecting data at different points within an organization's IT infrastructure. At a high level they can be categorized as follows:

Email DLP

DLP for email systems helps prevent sensitive data from being lost, leaked, misused, or accessed by unauthorized individuals. Email DLP solutions monitor

endpoints and exfiltrates data without authorization (often the starting point of another type of DLP like Network or Email).

DFIR Analyst DLP Responsibilities

When investigating DLP incidents the role of an analyst is to conduct the following:

1. Review the alert triggered by the DLP system.
2. Check the user's permissions or confirm if they received explicit permission from their leadership for the action.
3. Contact the user's leadership to confirm whether the activity was previously authorized; if authorized, log the justification.
4. If not authorized, contact the user to delete or otherwise remove sensitive materials.
5. Escalate the incident to the appropriate teams or stakeholders, especially when the leaked data involves Personally Identifiable Information (PII)...

Appendix E: Incident Response Training Plan (excerpt)

Full Training plan available at: https://github.com/DK36/CS6767-Cyber-Sec-Practicum/blob/main/Incident%20Response%20Training.pdf

INCIDENT RESPONSE TRAINING

INTRODUCTION TO INCIDENT RESPONSE

This training plan is intended for analysts who have completed review of our Cyber Incident Response Plan (CISP) and Corporate Information Security Policy (CISP).

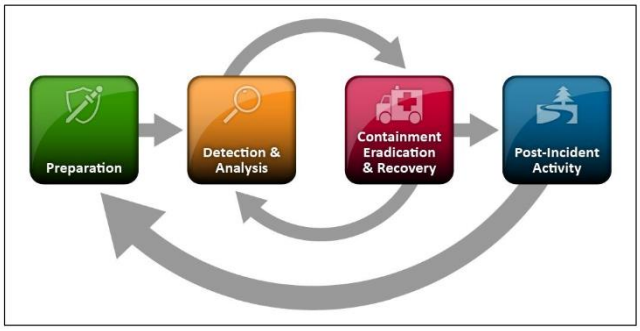
The generally accepted lifecycle for responding to incidents is structured into several key phases[1]:

1. **Preparation**: This phase involves establishing an IR policy, defining the team's roles and responsibilities, and identifying critical assets and potential threats. It includes creating incident detection and reporting procedures, as well as ensuring resources are available for effective response.

2. **Detection and Analysis**: In this phase, incidents are detected through monitoring and analysis of network traffic, system logs, and other sources. Once detected, incidents are categorized based on severity and impact, and a preliminary assessment is conducted to understand the nature and scope of the incident.

3. **Containment, Eradication, and Recovery**: The focus here is on containing the incident to prevent further damage, eradicating the threat from affected systems, and restoring operations to normalcy. This phase involves executing mitigation strategies, applying patches or fixes, and restoring data from backups if necessary.

4. **Post-Incident Activity**: After the incident is contained and systems are restored, post-incident activities include documenting the incident, conducting a lessons learned review, and updating incident response procedures based on identified weaknesses or improvements.



DIRECTORIES:

- **C:\Windows:** The directory where the Windows operating system files are stored.

- **C:\Users:** Contains user profiles and associated data.
- **C:\Program Files & C:\Program Files (x86):** Default directories for installed applications.
- **C:\ProgramData:** Contains application data that is shared among users.
- **C:\Windows\System32:** Critical system files and drivers necessary for Windows functionality, protected against unauthorized modifications.
- **C:\Windows\Temp (or %Temp%):** Used for temporary storage, frequently targeted by malware for hiding and executing malicious code.

FILES:

- **Pagefile.sys:** A file used for virtual memory, which can contain fragments of memory.
- **Hiberfil.sys:** A file used when the system hibernates, which can contain the contents of RAM.
- **Prefetch Files:** Located in C:\Windows\Prefetch, these files help speed up application launch times and can provide information about program execution.

REGISTRY HIVES:

- **HKEY_LOCAL_MACHINE (HKLM):** Contains system-wide settings.
- **HKEY_CURRENT_USER (HKCU):** Contains settings for the currently logged-in user.
- **HKEY_CLASSES_ROOT (HKCR):** Stores information about registered applications.
- **HKEY_USERS (HKU):** Contains user-specific settings for all users on the system.

PROCESSES

Processes are instances of executable programs running on a computer system, each with its own memory space and resources.

In Windows, processes can spawn other processes, creating a parent-child relationship. Understanding this hierarchy is essential for tracing the execution flow of malicious activities.

1. **Parent Process:** The original process that initiates another process. For example, a command shell (cmd.exe) launching a script.
2. **Child Process:** The process that is initiated by another process. For example, a PowerShell script (powershell.exe) started by cmd.exe.

HASHES

Hashes are cryptographic representations of data and are used to verify the integrity of files. In forensics, hashes help ensure that evidence has not been tampered with.

1. **File Hashes:** Used to uniquely identify files. Common algorithms include MD5, SHA-1, and SHA-256.
2. **Process Hashes:** Hashes of executable files that help identify known good or malicious files. Comparing hashes against databases of known malware (e.g., VirusTotal) can quickly determine if a file is malicious...

PORTS, PROTOCOLS, AND SERVICES

Ports are endpoints used by computers for communication over a network. They enable different applications and services to interact with each other by providing a specific channel through which data is transmitted. Ports facilitate the transmission and

reception of data between computers and devices. Each port is associated with a specific protocol or service, enabling computers to distinguish between different types of network traffic.

Protocols are standardized sets of rules that determine how data is transmitted between different devices over a network. They define the procedures for formatting, sending, and receiving data across network connections, ensuring that devices—regardless of their underlying architectures—can communicate effectively. Protocols operate at various layers of the OSI (Open Systems Interconnection) model, each layer addressing specific aspects of network communications.

The foundational protocols for the internet and major focus in network-based analysis are TCP and IP (Transmission Control Protocol &Internet Protocol). TCP ensures data is sent and received accurately, while IP handles the addressing and routing of packets to their destination as explained in the previous section. DNS is another important protocol used to translate human-readable domain names into IP addresses. This enables users to access websites using easy-to-remember names instead of numerical addresses (i.e google.com IP is 8.8.8.8).

Services, in a network context, refer to specific applications or processes that utilize network protocols to perform useful functions or provide functionalities to user applications. Services are often associated with specific protocols at the application layer of the OSI model, and they enable diverse network functionalities such as web browsing, file transfer, email communication, and more.

Here are a few common examples of Protocols/Services and the ports that are frequently used:

HTTP and HTTPS (Web Browsing)

- **Protocol:** HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure)
- **Port:** Typically, HTTP uses port 80, and HTTPS uses port 443.
- **Service:** Web browsing

  When you type a website URL into your browser, the browser uses HTTP or HTTPS to request the webpage from a server. HTTPS includes encryption with SSL/TLS to secure the communication. The server listens on ports 80 (HTTP) or 443 (HTTPS) to respond to these requests, delivering web pages back to the browser.

FTP (File Transfer)

- **Protocol:** FTP (File Transfer Protocol)
- **Port:** Commonly uses ports 20 and 21; port 21 for control (commands) and port 20 for data transfer.
- **Service:** Transferring files between computers

  FTP allows users to upload and download files from a server. A client connects to the server using port 21 to send commands, and the actual file data transfers through port 20.

SSH (Secure Remote Access)

- **Protocol:** SSH (Secure Shell)
- **Port:** Typically uses port 22.
- **Service:** Secure remote administration

  SSH is used for securely logging into remote machines, allowing administrators to manage systems via a secure channel. All data, including login credentials, is encrypted to prevent eavesdropping.
  SSH is not native to Windows Operating Systems and can often be an indication of suspicious activity.

RDP (Remote Desktop Protocol)

- **Protocol:** RDP (Remote Desktop Protocol)
- **Port:** Generally uses port 3389.
- **Service:** Remote desktop access

  RDP lets users connect to a remote computer and use the Windows graphical interface over a network connection. This service is crucial for accessing a workstation or server from a remote location.

DNS (Domain Name System)

- **Protocol:** DNS
- **Port:** Uses port 53.
- **Service:** Resolving domain names
- DNS translates human-readable domain names (like google.com) into IP addresses (like 8.8.8.8). When you enter a URL in your browser, your computer uses DNS to find the corresponding IP address of the server you're trying to reach.

SMB (Server Message Block)

- **Protocol:** SMB (Server Message Block)
- **Port:** Typically uses TCP ports 139 and 445.
- **Service:** Windows file sharing and inter-process communication

  SMB is used for providing shared access to files, printers, and serial ports among network devices. It's also used in Windows for network file system operations...

EDR

EDR represents an evolution in endpoint security. EDR systems provide advanced capabilities to detect, investigate, and respond to threats that evade traditional antivirus measures. EDR tools continuously monitor endpoint activities, capturing detailed information about system behaviors and network interactions. This real-time monitoring enables the identification of suspicious activities and potential breaches through behavioral analysis and anomaly detection.

DETECTION

A key aspect of EDR solutions is the ability to create detections based on defined threat indicators. Creating effective detections in involves defining rules and conditions that trigger alerts when suspicious activities are detected on endpoints. The process begins with understanding the specific environment and establishing a baseline of normal behavior, which includes typical applications, user activities, network connections, and processes. This knowledge is essential for accurately identifying deviations that may signal potential threats. After we baseline the normal, the next step is identifying Indicators of Compromise (IOCs), such as suspicious file hashes, IP addresses, domain names, URLs, registry keys, and unusual process behaviors. These IOCs help in crafting precise detection rules.

Let’s say, for example, our EDR tool has an alert that searches for non-standard applications creating network connections and it is alerting on the process `calc.exe`

(Windows Calculator application) attempting to initiate an SSH connection.

As an analyst, the alarms should be sounding off in your head as this behavior is highly

unusual and could indicate a process injection attack, where an attacker uses a legitimate process to execute malicious actions, bypassing traditional security measures. Now you can readily identify a threat in the environment and start stepping through the response plan. You may ask yourself:

“Should I blacklist (block) this hash or disconnect the workstation from the network? “

“What is the destination IP address this process is communicating with?”

“Does the hash for this process match for the known native calculator app?”

“Who or what initiated this process?”
“Are there any suspicious processes in the ancestry that led to this?”

EDR can help us answer these questions as well as take quick action. One of the immediate steps is to isolate the infected host from the network. Network isolation prevents the potential spread of the threat and limits the attacker's ability to communicate with the compromised device, thereby containing the threat. This action allows analysts to perform a more detailed investigation without the risk of further contamination or data exfiltration.

EDR solutions also offer capabilities to collect artifacts and perform file fetch operations. Analysts can remotely retrieve files, logs, and memory dumps from the affected system for forensic analysis. This helps in understanding the nature and extent of the compromise, identifying any malicious payloads, and gathering evidence for further investigation. The collected artifacts can be analyzed to determine how the attack occurred and what steps need to be taken to remediate the system fully...

Appendix F: Trainee Performance Metrics

Reviews Completed: The true percentage indicates the number of alerts the trainees completed that have been reviewed by a peer. The total for reviewed at the time of data collection was 112

Alert Categories: These are the general categories an alert may fall into; the lease level of specificity. Learning objectives were formed around these categories.

Alert Severity: The level of severity an alert was assigned according to CIRP. Informational was investigated and determined a false positive, meaning the conditions that triggered the alert did not actually indicate a security threat. Anything above informational is treated as a threat or violation of policy.

This scatter plot indicates the scores trainees received from peer reviewed alerts on a scale of 100%. On Average, trainees were meeting their acceptance criteria to total satisfaction.

Appendix G: Post-Training Skills Assessment

https://docs.google.com/forms/d/1aItj1R_MLk_lzM5u-BjNtgrUOUV3wNp0wzJjQlySDb8/viewanalytics