The Role of Custom Scripting in APT Incident Response

Raymond Hagen[1], Lasse Øverlier[2], and Kirsi Helkala[3]

[1] DIGITALISERINGSDIREKTORATET-NTNU, Norway
raymond.andre.hagen@digdir.no
[2] Norwegian University of Science and Technology, Norway
lasse.overlier@ntnu.no
[3] Norwegian Defence Cyber Academy, Norway
kirsi.helkala@gmail.com

Abstract. Advanced Persistent Threats (APTs) present complex challenges by employing covert and sophisticated techniques that evade traditional security measures. This study investigates the role of custom scripting in improving incident response capabilities based on interviews with cybersecurity professionals in various sectors. The findings demonstrate that custom scripts bridge critical gaps left by commercial and open-source tools, providing the flexibility and precision to detect and mitigate complex threats. Despite their effectiveness, custom scripts require specialized skills and resources, creating a disparity between large and small organizations in their ability to combat advanced threats. This paper advocates integrating custom scripting within standardized incident management and response, and helping commercial tools address these challenges. Recommendations include targeted training, investment in skill development, and establishing robust policies for script usage and maintenance. Future research should explore the integration of emerging technologies such as artificial intelligence (AI) and machine learning to further enhance scripting capabilities in cybersecurity operations.

Keywords: Advanced Persistent Threats, Incident Response, Custom Scripting, Cybersecurity, Threat Hunting, Security Automation, Cyber Threat Intelligence, Forensic Analysis, Threat Detection, Security Frameworks, Security Orchestration, Digital Forensics, APT Mitigation, Incident Response Tools, Security Skills Gap, Security Operations, Security Policy Development

1 Introduction

In 2023, a financial institution faced an Advanced Persistent Threat (APT) attack that evaded detection for several months due to sophisticated techniques that blended into regular network traffic. The incident response team, aided by an external consulting firm, used custom scripts to analyze logs, identify anomalies, and trace the breach. This anonymized case, collected from the interviews

that form the basis of this study, highlights the vital forms of custom scripting to identify and mitigate APTs when standard tools are insufficient.

Advanced Persistent Threats (APTs) pose a significant challenge due to their stealthy and persistent nature, often bypassing traditional security measures [4]. This study focuses exclusively on the application and impact of custom scripting in incident response activities, specifically to detect, investigate, and mitigate APTs. It does not address incident response practices at large or the use of commercial and open-source tools beyond their interaction with custom scripts.

Despite the availability of sophisticated commercial tools, custom scripting is widely used in various sectors, including large enterprises and specialized consulting firms, to address the unique demands of the APT response [18]. This dependency indicates a critical shortfall in the adaptability of commercial solutions to meet the specific needs of complex threat environments, emphasizing the importance of developing and maintaining robust scripting capabilities.

The following sections will explore the specific role of custom scripting in improving cybersecurity operations against APTs, the unique challenges faced in this context, and the implications for future practice and policy development. This study aims to provide a focused analysis of how custom scripting can be effectively leveraged to fill the gaps left by traditional security tools in the detection and response of sophisticated threats.

2 Related Work

Custom scripting is increasingly crucial for improving the incident response to APTs. Mathew [9] illustrates how scripts automate the detection of Indicators of Compromise (IOCs) and enable rapid adaptation to evolving threats. Abuabid and Aldeij [1] argue that commercial tools often lack flexibility and advocate the integration of custom scripts into standard procedures.

Despite these advances, the practical challenges of implementing custom scripts, such as resource constraints and technical expertise, remain underexplored [12]. This study addresses these gaps through qualitative insights from cybersecurity professionals.

2.1 Manual Scripting and Forensic Readiness

Manual scripting improves forensic readiness by allowing organizations to develop customized tools for data collection, log analysis, and incident response [2]. Scripting languages such as Python and PowerShell facilitate automation and customization, which is crucial to handling unique data formats and automating repetitive tasks [17].

Customization: Scripts enable interaction with proprietary systems and support specific needs that commercial tools cannot address [17].

Automation: Automating tasks like log parsing and data correlation increases efficiency and reduces human error [13].

Rapid Response: Scripts can be quickly modified and deployed to counter new threats, providing flexibility in dynamic environments [15].

Challenges in Incident Response Preparedness Despite their benefits, manual scripts require specialized expertise and resources, which can be challenging for smaller organizations [7]. Inadequate policies and the reliance on inflexible commercial tools further hinder effective incident response [9]. Organizations must invest in skill development and integrate custom scripting with standardized frameworks to overcome these limitations.

2.2 Limitations of Commercial and Open-Source Tools

Commercial Off The Shelf (COTS) and open-source tools often lack the adaptability to respond to APT effectively [6]. Issues like siloed logs, inadequate threat intelligence, and a high degree of customization make them insufficient. A balanced approach that combines these tools with custom scripting is essential to address the complexities of APT investigations.

3 Methodology

3.1 Data Collection

Qualitative data was collected through semi-structured interviews [5] with cybersecurity professionals from August to September 2024. Each interview, lasting 1.5 to 2 hours, explored the participants' experiences with APTs, using custom scripts in incident response, and the associated challenges. All interviews were conducted according to the ethical guidelines approved by the Norwegian Agency for Shared Services in Education and Research (SIKT.no (Ref. 530XXX)), and the participants' identities were anonymized for confidentiality.

Table 1. List of respondents, sectors, interview periods, and script usage

Respondent	Sector	Interview Time Period	Uses Script
R1	Consulting Firm A	August 12, 2024	YES
R2	Government Agency	August 5, 2024	YES
R3	Financial Institution A	August 2, 2024	YES
R4	Cybersecurity Consulting B	August 20, 2024	YES
R5	Government Agency B	September 16, 2024	YES
R6	Consulting Firm C	September 2, 2024	YES
R7	Financial Institution B	September 5, 2024	YES
R8	Government Agency C	September 10, 2024	YES
R9	Cybersecurity Consulting D	August 5, 2024	YES
R10	Government Agency D	September 10, 2024	YES

The sample size of 10 cybersecurity professionals was selected using purposive sampling to ensure diverse representation across various sectors and organizations. This number was deemed sufficient as the responses to questions regarding scripting practices reached saturation, meaning no new information or themes emerged. This indicates that the sample size was adequate to comprehensively explore the research questions and validate the consistency of the findings.

3.2 Data Analysis

Thematic analysis [3] was used to identify key themes related to custom scripting in the APT response, which were cross-referenced with the roles and types of organizational threat encountered by the respondents.

3.3 Quantitative Data Analysis and Validation

This study used quantitative data to confirm the consistency of scripting usage among all respondents during the incident response to advanced persistent threats (APT). As shown in Table 2, all 10 respondents affirmed the use of custom scripts as a critical component in their incident response processes. This unanimous agreement provides a robust basis for understanding the prevalence of scripting practices in response to the APT incident.

To statistically validate this finding, we applied a chi-square test [11] for goodness of fit to determine whether the observed data (10 out of 10 respondents using scripts) are consistent with an expected distribution. Assuming the null hypothesis that the proportion of organization is 50% (as might be expected in a population without a strong preference), the chi-square test is calculated as follows:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i}$$

Where:

- O_i is the observed frequency of respondents using scripts (10 out of 10).
- E_i is the expected frequency if only 50% used scripts (5 out of 10).

Substituting the values:

$$\chi^2 = \frac{(10-5)^2}{5} + \frac{(0-5)^2}{5} = 5 + 5 = 10$$

With 1 degree of freedom ($df = 1$), the critical value for χ^2 at a significance level of 0.05 is 3.841. Since the calculated value of 10 is much greater than 3.84, we reject the null hypothesis, confirming that the observed unanimous use of scripting is statistically significant and not due to chance.

This result not only supports the quantitative consistency observed in the qualitative data but also validates the conclusion that scripting is universally employed in responding to APT incidents within the sampled population.

4 Findings

"We have situations where, without our scripts, it would take days to process all the data. We can automate significant portions of the investigation with custom scripts, saving valuable time."

Respondent R5

4.1 Quantitative Data on Effectiveness

An analysis of the effectiveness of custom scripting among respondents is summarized in Table 2. All respondents confirmed using custom scripts in their incident response, highlighting the importance of addressing complex security challenges that commercial tools alone cannot handle.

Table 2. Summary of Custom Script Usage Across Respondents

Respondent ID	Uses Scripts	Script Usage Details
R1	Yes	Custom scripts for identifying user behavior and network traffic anomalies.
R2	Yes	Development of custom detections and scripts for advanced persistent threat (APT) detection.
R3	Yes	Custom scripts for correlating logs and APT activity identification.
R4	Yes	Use of tailored scripts for forensic analysis and data extraction during investigations.
R5	Yes	Scripts will analyze log data for targeted attack detection and threat hunting.
R6	Yes	Custom scripts for integrating and correlating data from multiple sources for comprehensive threat analysis.
R7	Yes	Custom solutions for specific threat analysis focused on advanced persistent threats.
R8	Yes	Scripts are used to refine and automate repetitive security tasks, improving efficiency in incident response.
R9	Yes	Tailored scripts for monitoring and alerting specific suspicious activities in the network.
R10	Yes	Scripts for filtering and prioritizing alerts, threats, and indicators of compromise.

The data indicates that custom scripts are essential for tasks such as log correlation, anomaly detection, and forensic analysis, demonstrating their flexibility and effectiveness in handling advanced threats.

4.2 Interplay Between Interview Insights and Data Analysis

This study demonstrates a strong link between the insights derived from the interviews and the data collected on the use of custom scripting against Advanced

Persistent Threats (APTs). The 10 participants confirmed the use of custom scripts in their security protocols, highlighting the necessity in complex threat landscapes where conventional tools are inadequate.

Throughout the interviews, participants uniformly emphasized the pivotal role of custom scripting in managing APT incidents. For example, Respondent R3 mentioned *"Our custom scripts allow us to automate tasks that would otherwise be impossible to handle with standard tools. This is essential to identify and mitigate complex APT activities."* Similarly, Respondent R7 described scripting as *"the backbone of our incident response strategy, allowing us to respond quickly and effectively to sophisticated threats."* These insights are corroborated by the findings in Table 2, which show complete integration of custom scripts into their incident response workflows by each respondent.

The data in Table 2 reveal that 100% of the participants incorporate custom scripting into their APT response strategies. This unanimous usage highlights the indispensable reliance on scripting for effective threat mitigation. Furthermore, the chi-square test detailed in the methodology section confirms the statistical significance of these findings, suggesting that the results are not just coincidence.

The data and interview insights collectively underscore the critical role of custom scripting in addressing APT incidents. While standard tools provide a basic framework, custom scripts deliver the specific flexibility and precision required to meet the unique challenges of APTs. The uniform adoption of scripting among respondents indicates a broader industry trend toward essential scripting skills in cybersecurity defenses.

The demonstrated correlation supports the extensive implementation of custom scripting in the field and underlines its strategic value in managing sophisticated cyber threats. Future studies should investigate ways to further enhance scripting capabilities to ensure that organizations can adapt to evolving APT tactics.

4.3 Leveraging Custom Scripts for Threat Hunting

Respondent R8's organization employs organizations extensively for threat hunting, automating the detection of indicators of compromise (IOCs), and identifying suspicious patterns. These scripts are crucial for detecting and mitigating threats before they can escalate. For example, custom scripts have been used to correlate file access patterns with log-in attempts, successfully revealing lateral movement activities that had previously gone unnoticed.

Implications for Practice Custom scripts allow proactive threat identification, efficient data analysis, and scalable response capabilities. This approach provides a dynamic mechanism to counter evolving threats by enabling rapid adaptation and response to complex cyberattacks [10].

Advanced cyber threats require flexible and adaptive responses. Custom scripts are essential for aggregating data across diverse IT environments and correlating complex logs, tasks that standard tools often struggle to achieve. As

Respondent R1 pointed out, custom scripting is necessary to track specific IOCs that commercial tools cannot detect.

The flexibility offered by custom scripts in incident response enables rapid adaptation to unique scenarios. For example, Respondent R5 highlighted that processing critical data could take days without custom scripts, whereas scripting automates substantial portions of investigations, significantly reducing the time required to respond to incidents.

However, notable challenges exist, such as the need for specialized expertise constraints, particularly within smaller organisations; these scripts can be demanding, and errors can complicate investigations.

> *"The challenge I have is balancing priorities and getting the resources to the right team at the right time so they can do what they need to mature the program faster. We have a training issue because we have a small team, and it all stems from staffing and sometimes budget. If you don't have the staff you need, then the people, the small number of people you have, are doing more. And if they're doing more, they have less time. And if they have less time, they cannot train to the level I want to see them trained."* *Respondent R6*

Poorly maintained scripts can also introduce vulnerabilities into the system. Respondent R2 shared an instance where an unmonitored script was compromised, underscoring the importance of script security and regular maintenance.

In addition, smaller organizations develop and maintain custom scripts, putting them disadvantaged when faced with advanced threats. Despite these challenges, custom scripting remains indispensable for effective APT defense, providing the flexibility and rapid adaptability that commercial tools alone cannot offer.

> *"Every advanced cyber threat demands a specific approach, a tailored approach for that. It seems like each one sitting and handling advanced attacks is doing log analysis based on scripts and doing all these types of things. Organizations rely so much on manual scripting because every attack is different."* *Respondent R6*

Custom scripts are particularly useful for handling non-standard data formats and automating context-specific detection rules, filling the gaps left by tools. They allow organizations to make tactics, ensuring effective containment and response during APT incidents.

In addition, custom scripts support proactive defense strategies by automating threat hunting and simulating adversary techniques. This allows organizations to make their abilities before they are exploited. Scripts can also automate real-time alerting, incident response orchestration, and blocking of malicious Internet domains, effectively reducing the dwell time of APT actors.

5 Discussion

5.1 Significance of Custom Scripting in APT Incident Response

The findings of this study affirm that custom scripting plays a crucial role in responding to Advanced Persistent Threat (APT) incidents. Custom scripts allow organizations to enable more precise and effective responses rather than relying solely on commercial tools. This observation aligns with existing research that emphasizes and adapts to the response to cybersecurity incidents [1]. By custom scripting, teams can rapidly adapt to evolving threat landscapes, creating a robust and dynamic defense mechanism against sophisticated attackers.

5.2 Enhancement of Commercial Tools through Custom Scripts

Commercial security tools are often designed with extensibility, offering Application Programming Interfaces (APIs) and integration points that facilitate customization and consolidation of data from diverse sources in complex security environments, which are impractical and time-consuming. Custom scripts address this challenge by enabling seamless data aggregation, standardizing formats, and ensuring accurate time synchronization.

> 'Writing custom scripts is usually the fastest way to standardizable for analysis.' *Respondent R5*

Custom scripts significantly enhance the functionality of commercial tools by enabling precise data queries, advanced event correlation, and the automation of complex analytical tasks. For example, they can automatically parse log files, correlate events across multiple systems, and trigger alerts based on predefined criteria. This integration creates a cohesive and adaptable security ecosystem, improving the overall efficiency of the incident response process and reducing the time to detect and respond to threats [10]. Moreover, custom scripting allows for continuously improving security operations by adapting to new threats as they emerge.

5.3 Challenges and Limitations of Scripting in Incident Response

Despite its benefits, custom scripting in incident response comes with challenges. One of the primary obstacles is the skill gap, particularly in a small organization that develops and maintains scripts effectively [16]. This shortage of skilled personnel can lead to an overreliance on a few key individuals, creating a potential single point of failure.

'In my own case, using my own financial capability and budget to have, and trying to update these capabilities, I don't have the time and the budget to even to try to perform my own SOC, because in this moment, I have my own mini

SOC, I have my own server and equipment, but even it's not, really speaking, we don't have the capabilities to confronting a biggest attack in this moment. Perhaps in my case, yes, because I'm a Linux user, but even when you're working or even what you're talking with other people, or when you're talking with other CISOs or CTOs, they mention the same. Most of companies or most of professionals working in Latin America don't have the capabilities or they don't have even the technical knowledge to confronting these major cyber attacks.'

Respondent R7

5.4 Strategies for Overcoming Scripting Challenges

Organizations have comprehensive training programs to address these challenges and improve their security teams. Having regular and standardized code reviews can mitigate the risks of poorly maintained scripts. [8] Furthermore, integrating scripting efforts with broader security operations and DevSecOps practices can enhance collaboration and ensure that scripts are developed and maintained in alignment with the organization strategy [14].

> *"We approach it the same way that we do with detections, because we create detections and we don't want them going stale or breaking without our knowledge, because there was a change made to the logs, the log structure or something. And that is that we mandate as a team, a security operations team, we mandate a periodic review of all of our playbooks and all of our detections. And we go through one by one, we break them up as a team and say, okay, this team member will focus on these 20, next one will do the next 20 and so on. And we try to review them sorting by criticality, we'll do the critical ones first. And then once we get through all of them and review and make sure that they're still applicable, including changes to our environment and so on, then we'll either update it then or we'll delete it if it's no longer applicable, we're no longer using this system or whatever. We'll get rid of those playbooks"* *Respondent R7*

Table 3, provides a comparative analysis of custom scripting versus commercial tools used in the incident response to advanced persistent threats (APT). The comparison draws directly from data and insights gathered through interviews, the same interviews that form the basis of Table 1 and the entire study. These discussions with cybersecurity professionals have highlighted their experiences and insights on various aspects such as efficiency, customization, deployment time, skill requirements, and maintenance of both approaches. Each criterion in Table 3 reflects key themes that were recurrent in these interviews, clearly illustrating the trade-offs between flexibility and operational ease in security environments.

Table 3. Comparison of Custom Scripting vs. Commercial Tools in APT Incident Response

Criteria	**Custom Scripting**	**Commercial Tools**
Flexibility	High	Moderate
Customization	Extensive,	Limited to API capabilities
Time to Deploy	Longer (development needed)	Shorter (pre-built functionality)
Skill Requirement	High	Moderate
Maintenance	Ongoing (requires expertise)	Vendor-supported

5.5 Future Directions

Future research should further explore the role of custom scripting in enhancing automation and orchestration in incident response. Furthermore, developing frameworks and best practices for script management and integrating AI and machine learning could provide valuable insight into optimizing operations. Addressing these areas can lead to more effective and resilient security postures, particularly in the face of increasingly sophisticated threats.

This study contributes to the growing body of literature on cybersecurity incident response by highlighting the significant advantages and challenges of custom scripting. Organizations can improve customer security operations by understanding these dynamics and responding more effectively to APT incidents.

6 Limitations of the Study

This study examines the role of custom scripting in responding to Advanced Persistent Threats (APTs). However, several limitations must be considered when interpreting its findings, which may affect the generalizability of the results.

6.1 Focus on Scripting in APT Incident Response

The primary emphasis of this study is on custom scripting, which can overlook other essential components of incident response. The limitations include:

- **Coordination and Communication:** The study provides limited insight into how organization departments, such as legal, management, and technical units, during an incident response. This gap suggests that the collaborative dynamics of incident management have not been fully explored.
- **Integration with Frameworks:** There is a lack of in-depth analysis on how custom scripting is integrated into established security frameworks like the National Institute of Standards and Technology (NIST) NIST SP 800-61 or ISO 27001. Understanding this integration is crucial for standardizing
- **Use of Commercial Tools:** The interaction between custom scripts and commercial tools has not been comprehensively addressed. As organizations utilize commercial solutions, further exploring their integration could provide valuable insights.

6.2 Additional Limitations

The study's focus on custom scripting suggests saturation in this area, implying that further interviews may yield diminishing returns regarding new insights. However, several topics were underexplored:

Resource Allocation and Training The study does not adequately address the allocation of resources and the training required for practical scripting in incident response. These factors are critical in understanding the full impact and potential of custom scripting in an organization.

Potential Data Bias Participants might have been hesitant to share sensitive information, particularly in areas where their organization is based. This reluctance could lead to potential biases in the data, affecting the study's findings and conclusions.

Geographical and Organizational Scope The research predominantly includes North American and European participants, focusing on medium to large organizations, and the experiences and challenges of smaller entities or organizations in regions with diverse resources and response processes.

Technological Scope Although emerging technologies such as artificial intelligence (AI) and machine learning are mentioned, the study does not detail their specific impact on custom scripting. More exploration of how these technologies can enhance scripting practices in APT responses is necessary.

Regulatory and Ethical Considerations The study does not address the regulatory and ethical implications of using custom scripts, particularly regarding data privacy and compliance with international standards. These considerations are critical for organizations' industries and must be evaluated in future research.

7 Conclusion and Implications

This study highlights the pivotal role of custom scripting in responding to Advanced Persistent Threats (APT). Through more than 30 hours of interviews with cybersecurity professionals, it became evident that custom scripts often surpass commercial and open source tools in delivering precise and adaptable responses to complex threats. The ability to rapidly adjust to the shifting tactics of APT actors underscores the value of scripting as a superior solution over conventional approaches.

7.1 Summary of Findings

Commercial and open source tools are fundamental in the response to APT, yet they frequently lack the flexibility for effective mitigation. Custom scripting fills this void by enabling security teams to:

- **Handle Non-Standard Data:** Custom scripts can parse and analyze unique data that standard tools cannot process.
- **Automate Detection Rules:** Scripts allow custom rules, enhancing the ability to spot incident specific IoCs
- **Enhance Proactive Defense:** Scripts facilitate automated threat hunting and simulate adversary techniques, strengthening defensive capabilities.

7.2 Unexpected Advantages of Scripting

Contrary to initial expectations, custom scripting offers more efficient and timely responses than many commercial tools. Rapid prototyping and adaptation capacity of custom scripts provides a strategic advantage in reactive and proactive defense. These findings suggest a strong case for increased investment in internal scripting capabilities within cybersecurity teams.

7.3 Implications for Practice and Policy

For organizations, the following actions arise:

- **Investment in Training:** Organizations should prioritize personnel skilled in scripting. Training programs focused on scripting can significantly enhance an organization's scripting capabilities.
- **Balancing Tools and Scripts:** A robust response strategy should complement commercial tools with custom scripts. This hybrid approach can effectively address a broader range of threats and vulnerabilities.
- **Proactive Strategies:** Scripting should be integrated into threat hunting and automated intelligence efforts. This approach can lead to earlier threat detection and a more agile response to emerging threats.

7.4 Recommendations for Future Research

To build on the findings of this study, future research should consider the following.

- **Broaden the Scope:** Expand the research to include various incident response activities beyond custom scripting, such as coordination, communication, and commercial tools.
- **Quantitative Methods:** Incorporate quantitative methods to complement qualitative findings, offering a more balanced perspective on the effectiveness of custom scripting.
- **Integration with Tools and Frameworks:** Investigate how custom scripts can be effectively integrated with commercial tools and established frameworks like NIST and ISO 27001.
- **Emerging Technologies:** Explore the role of AI and machine learning in enhancing custom scripting practices and improving incident response strategies.

– **Regulatory and Ethical Challenges:** Address the regulatory and ethical implications of custom scripting, particularly about data privacy and compliance with international standards.

By addressing these areas, future research can provide a more comprehensive understanding of the complexities and nuances of APT incident response.

Acknowledgment of Participant Contributions

We sincerely thank all participants for their valuable insights and contributions, which form the foundation of this study and enhance our understanding of custom scripting in incident response.

References

1. Abuabid, A., Aldeij, A.: Cyber security incident response. Journal of Information Security and Cybercrimes Research (Online) **7**(1), 29–50 (2024)
2. Bankole, F., Taiwo, A., Claims, I.: An extended digital forensic readiness and maturity model. Forensic science international. Digital investigation (Online) **40**, 301348 (2022)
3. Cernasev, A., Axon, D.R.: Research and scholarly methods: Thematic analysis. JAACP : Journal of the American College of Clinical Pharmacy **6**(7), 751–755 (2023)
4. Cole, E.: Advanced persistent threat : understanding the danger and how to protect your organization. Yngress, USA, 1. edn. (2013)
5. Galletta, A.: Mastering the semi-structured interview and beyond : from research design to analysis and publication (2012)
6. Kuzuno, H., Yano, T., Omo, K., van der Ham, J., Yamauchi, T.: Security risk indicator for open source software to measure software development status. In: Information Security Applications, Lecture Notes in Computer Science, vol. 14402, pp. 143–156. Springer Nature Singapore, Singapore (2024)
7. Lee, M.: Cyber threat intelligence (2023)
8. Lukyanovich, I., Blinkova, L., Sableuski, U.: Effective tools and technologies for creating and maintaining web resources based on javascript libraries. Cyber-Physical Systems: Design and Application for Industry 4.0 pp. 443–452
9. Mathew, A.J.: Unscripted practices for uncertain events: Organizational problems in cybersecurity incident management. Science, technology, human values **49**(4), 827–850 (2024)
10. Muggler, M., Eshwarappa, R., Cankaya, E.C.: Cybersecurity management through logging analytics. In: Advances in Human Factors in Cybersecurity. pp. 3–15. Springer International Publishing, Cham
11. Pandis, N.: The chi-square test. American journal of orthodontics and dentofacial orthopedics **150**(5), 898–899 (2016)
12. Patil, R., Muneeswaran, S., Sachidananda, V., Gurusamy, M.: E-audit: Distinguishing and investigating suspicious events for apts attack detection. Journal of systems architecture **144**, 102988 (2023)

13. Rahman, A., Rahman, M.R., Parnin, C., Williams, L.: Security smells in ansible and chef scripts: A replication study. ACM transactions on software engineering and methodology **30**(1), 1–31 (2021)
14. Sadovykh, A., Truscan, D., Mallouli, W., Cavalli, A.R., Seceleanu, C., Bagnato, A.: CyberSecurity in a DevOps Environment: From Requirements to Monitoring. Springer, Cham, 1 edn. (2023)
15. Shinde, N., Kulkarni, P.: Cyber incident response and planning: a flexible approach. Computer fraud security **2021**(1), 14–19 (2021)
16. Siegel, C.A.: Cyber strategy : risk-driven security and resiliency (2020)
17. Tonhauser, M., Ristvej, J.: Cybersecurity automation in countering cyberattacks. In: Transportation research procedia (Online). vol. 74, pp. 1360–1365 (2023)
18. Xiang, G., Shi, C., Zhang, Y.: An apt event extraction method based on bert-bigru-crf for apt attack detection. Electronics (Basel) **12**(15), 3349 (2023)

Appendix: Interview Guide for Semi-structured Interviews

The following interview guide was used for the semi-structured interviews conducted in this study. The interviews covered several topics related to incident response and cybersecurity practices. In this article, questions focusing on custom scripting in the APT incident response are the only data used.

1. Introduction and background

2. Investigation of APT Attacks

3. Client Expectations and Communications (If Interviewing an Advisor)

4. Tools, Processes, and Gaps

5. Victim's perspective (if interviewing a victim of an APT attack)

6. Future Directions and Recommendations

7. Closing questions

This interview guide was part of a broader study on incident response practices. While this paper focuses on custom scripting in APT incident response, the complete guide is included here for completeness and to provide context on how the discussions were structured.