Cyb3rd4nc3
TECHNOLOGY

Securing Digital Transformation
for business operation

INCIDENT RESPONSE REPORT

JAN 2025

Prepared By
Daniel Mwendwa

Cybersecurity Analyst / Cloud & Cybersecurity Enthusiast

danielmwendwa234@gmail.com

Table of CONTENTS

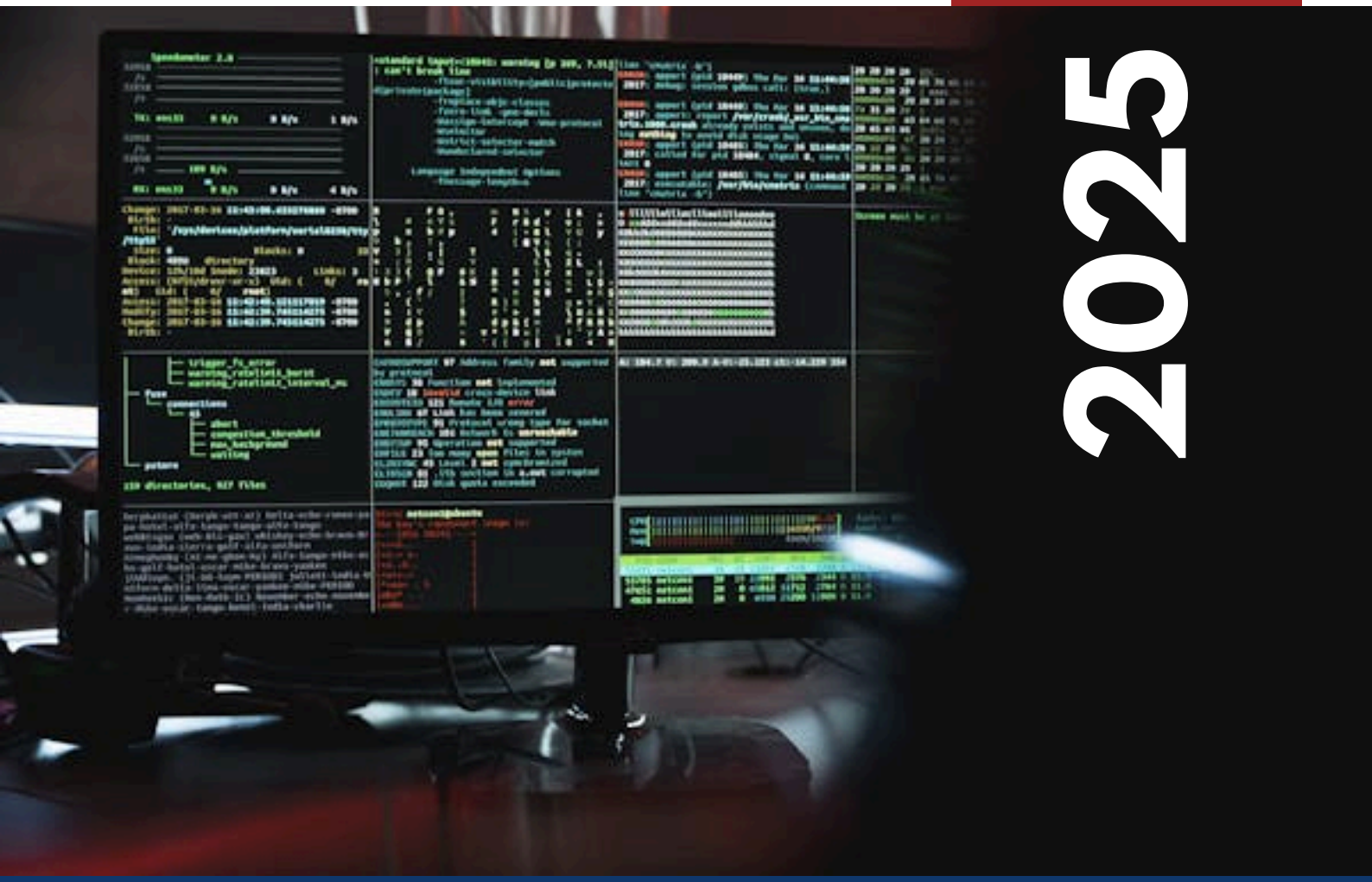
INTRODUCTION

INCIDENT RESPONSE

Incident Response (IR) is the systematic approach organizations use to detect, manage, and resolve cybersecurity threats. It integrates processes and technologies to contain and recover from incidents effectively, minimizing damage and downtime. A well-defined Incident Response Plan ensures teams can swiftly identify, mitigate, and document various attack scenarios, laying a foundation for stronger organizational resilience.

NIST VS. SANS FRAMEWORKS

The **NIST Framework** outlines four phases: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity, emphasizing continuous improvement. The **SANS Framework** divides the combined steps of containment, eradication, and recovery into separate phases, creating a six-step process: preparation, identification, containment, eradication, recovery, and lessons learned.



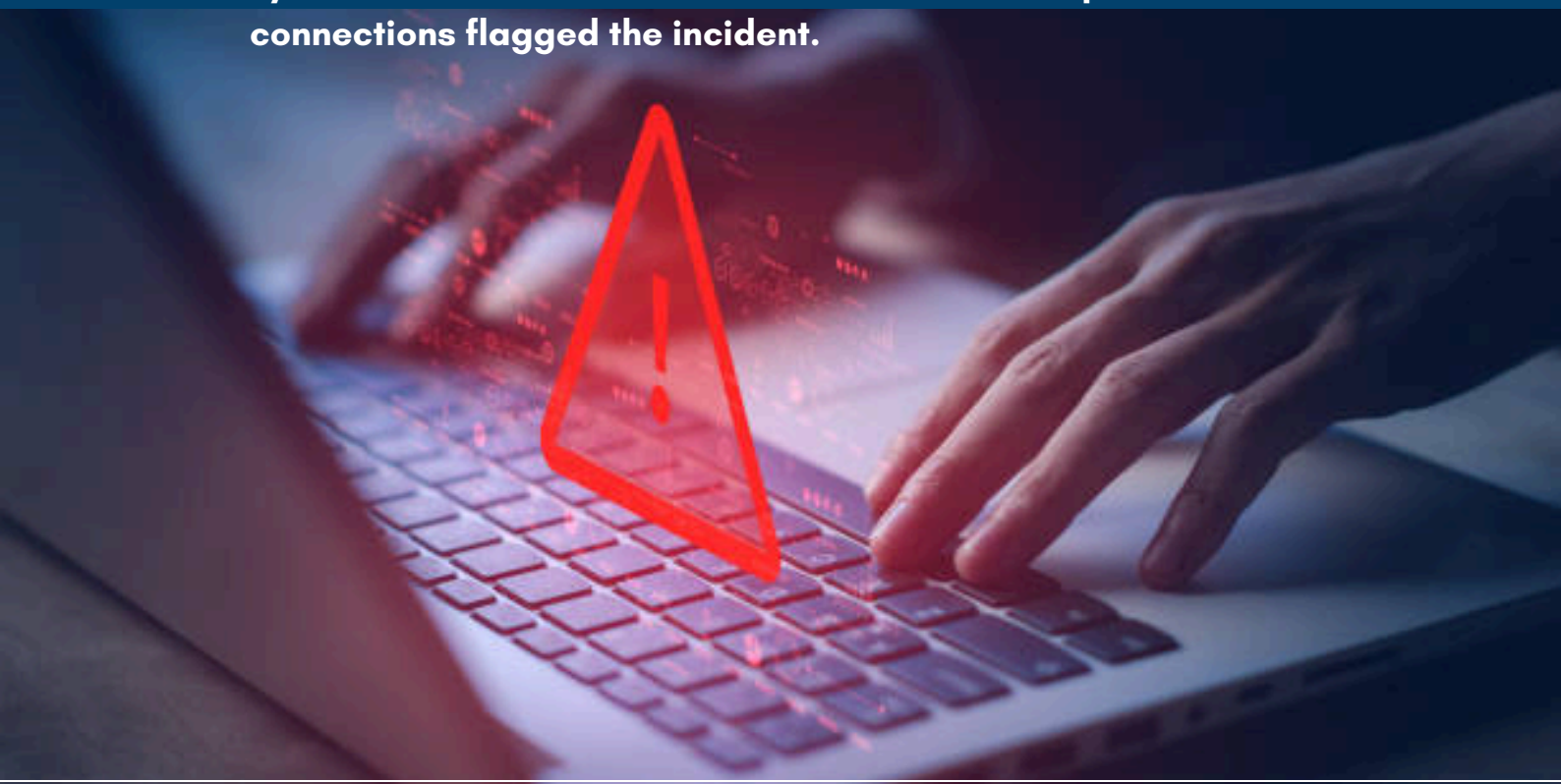
PREPARATION

Preparation lays the foundation for effective incident response by establishing policies, procedures, and tools to handle potential threats. Key elements include creating an Incident Response Plan (IRP), defining access controls, implementing data backup strategies, and ensuring regular patch management. Proactive measures like team training, threat intelligence gathering, and deploying tools such as SIEM and EDR systems enhance readiness. By identifying risks and conducting simulations, organizations minimize vulnerabilities and ensure swift responses. This ongoing process builds resilience, reduces incident impact, and strengthens overall cybersecurity, enabling teams to detect, respond to, and recover from threats efficiently.

Detection And Analysis

- **Scenario**: In this lab, I act as member of the Incident Response Team (IRT) investigating a potential incident on a Windows workstation. The incident was escalated to the Security Operations Center (SOC) team after a user reported performance issues on their Laptop.

- **Detection**: Detection is the process of identifying potential security incidents through monitoring and analysis. It relies on tools like SIEM systems to analyze logs, detect anomalies, and generate alerts for unusual activity. By identifying Indicators of Compromise (IOCs), such as unauthorized access or irregular traffic patterns, organizations can respond promptly to threats. In this case, the user's report of unusual system behavior and the SOC's observation of repeated outbound connections flagged the incident.



Analysis

Analysis refers to the process of examining and evaluating data from a security incident to understand what happened, how it happened, and the impact it had. This helps determine the cause and how to prevent future incidents.

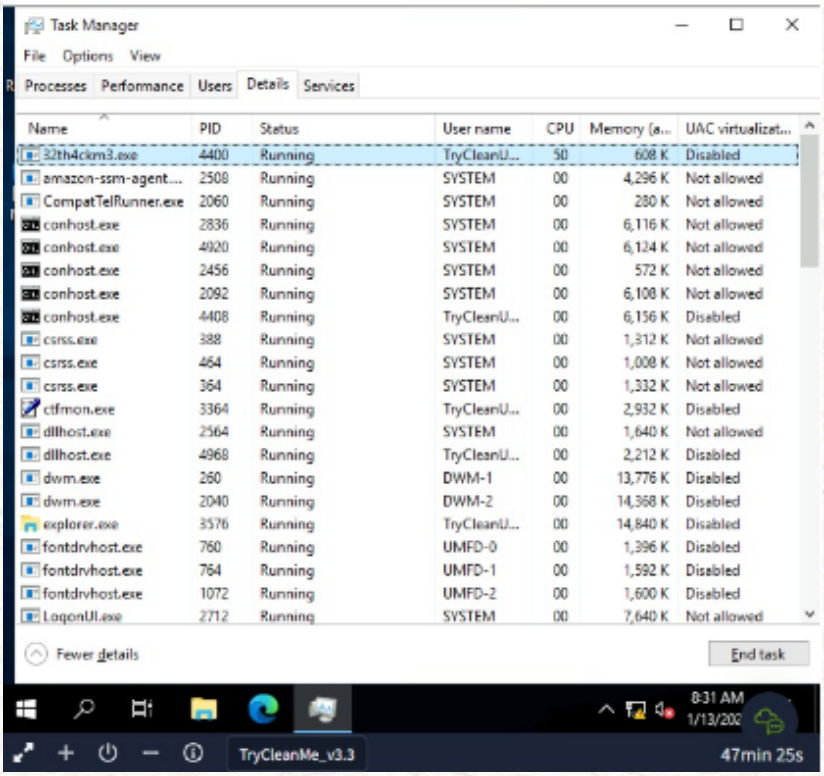
Now let's get our hands dirty

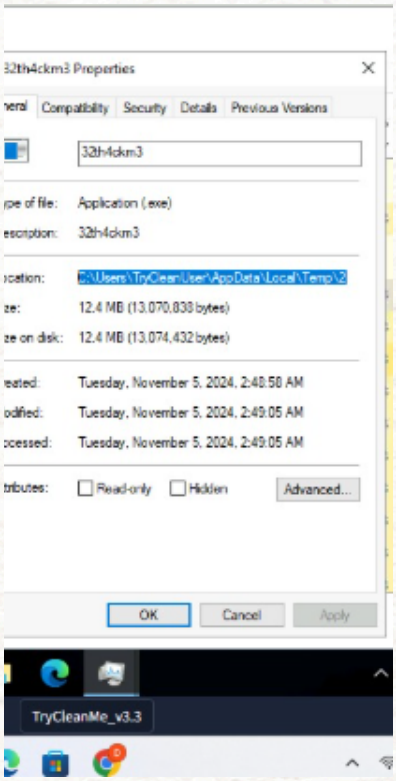
The analysis involved connecting to the machine, verifying the anomaly, identifying the malicious process, and understanding the infection vector.
Steps Taken:
1. Identifying the Threat
- Opened Task Manager to check for processes consuming high CPU resources.
  - Observed an unusually named process (3d33es454e.exe) consuming high CPU.
  - Process location: C:\Users\IRUser\AppData\Local\Temp.
  - PID 4400
- Verified the process's outbound connections to a C2 server:
  - Used the following command:
  - netstat -aofn | find "4400"
  - Identified repeated outbound connections to a suspicious IP (45.33.32.156:42424).

2. Identifying the Infection Vector
- Opened browser history in Microsoft Edge to identify suspicious downloads.
  - URL: edge://downloads/all
  - Found suspicious file: invoice n. 37484567 (1).docm downloaded from http://172.234.25.65.
- Opened the suspicious macro-enabled Word document.
  - Observed instructions prompting the user to visit a fake website.

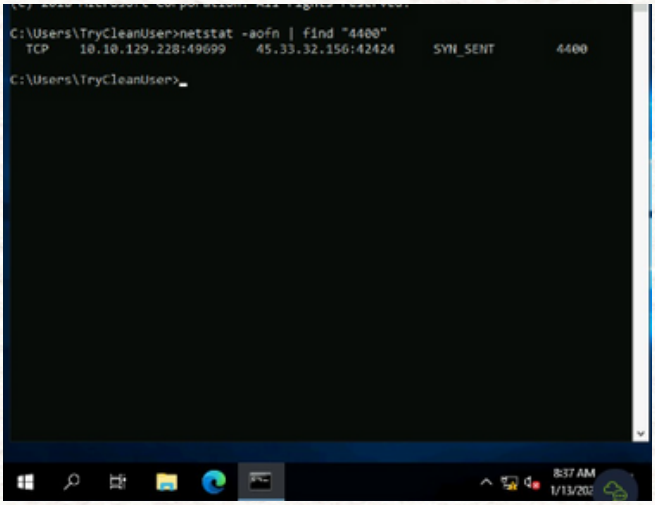
3. Analyzing the Macro
- Accessed macros within the document:
  - Menu: View > Macros > Edit.
- Reviewed VBA code, confirming malicious behavior:
  - Code referenced execution of the suspicious file 3d33es454e.exe.

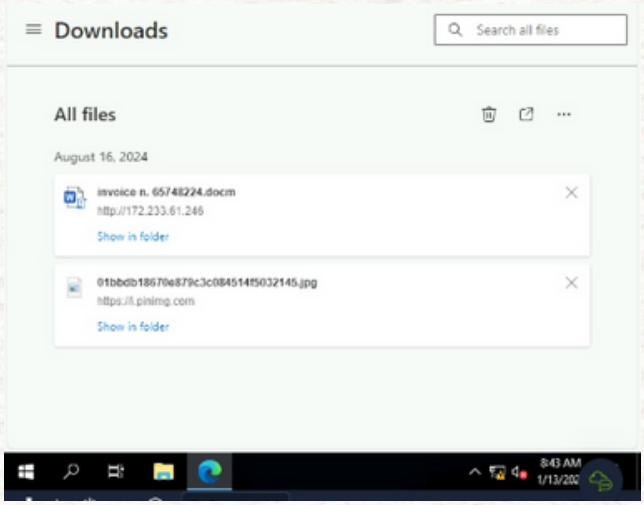
How About some screenshots?
Here's to the Next page

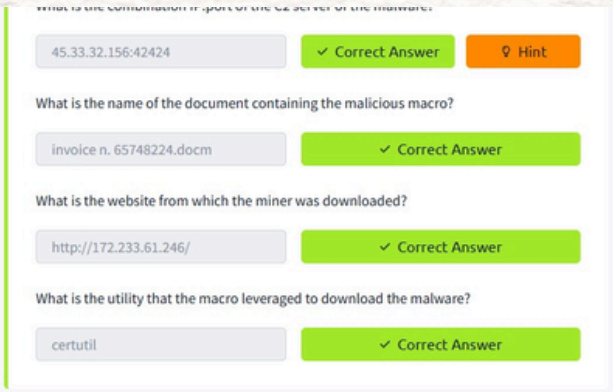


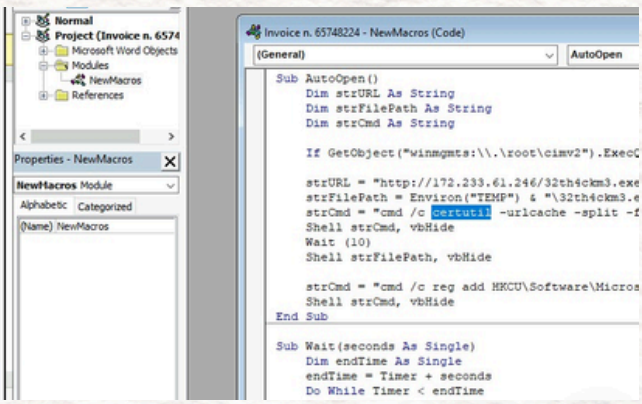


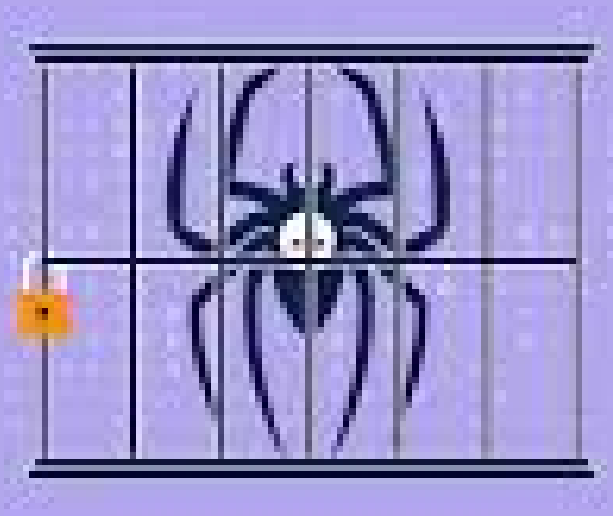
SCREENSHOTS











Containment, Eradication, and Recovery

Containment

I started by isolating the infected machine from the network to prevent the malware from spreading. Then, I identified the malicious process in Task Manager and ended it by selecting End Task. Next, I compiled the Indicators of Compromise (IoCs), including the C2 server IP, malicious URLs, and file hashes. Using tools like SIEM and EDR, I scanned the network and blocked any occurrences of these IoCs to contain the threat across the organization.

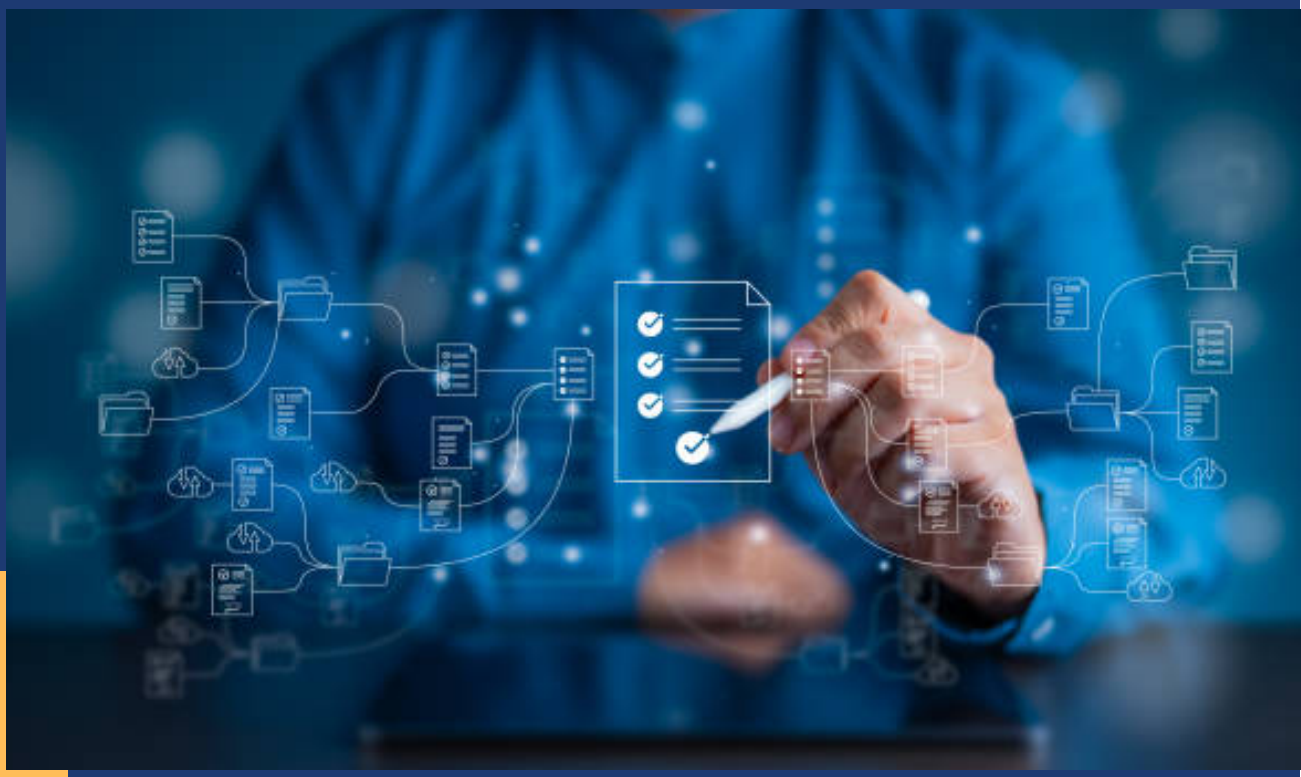
Eradication

I proceeded to delete the malware from the temporary folder where it was running. I also removed the Word document containing the malicious macro from the downloads folder and cleared the browser's download history to avoid accidental reactivation. To eliminate persistence, I accessed the Windows Registry Editor, navigated to the Run registry key, and deleted the malicious entry.

Recovery

After completing the cleanup, I verified that no persistence mechanisms or additional malware artefacts were present. I restored the system to a clean state and ensured it was fully functional.

Its Time for Documentation



Post-Incident Activity

Post-incident activities focus on evaluating the response process, identifying lessons learned, and implementing improvements to enhance organizational security and resilience. These activities ensure readiness for future incidents by addressing gaps and reinforcing defenses.

Summary of Key Steps:

- Documentation: Record a comprehensive incident report detailing actions taken, timelines, IoCs, and the incident's impact.
- Lessons Learned: Hold a review with stakeholders to identify successes, shortcomings, and areas for enhancement.
- Policy and Procedure Updates: Update security policies, playbooks, and response procedures based on insights gained.
- Tool Optimization: Refine tools like SIEM and EDR with updated IoCs to prevent similar threats.
- Employee Training: Share lessons learned with staff and reinforce cybersecurity best practices.
- Testing and Validation: Perform penetration tests and simulations to validate the effectiveness of new or improved security measures.

Conclusion

Incident response is not just about addressing the now—it's about building a stronger tomorrow. Every incident is a stepping stone, offering lessons that shape a more resilient security posture. By continuously refining strategies, enhancing tools, and empowering teams, we prepare for an ever-changing threat landscape. Stay tuned for more insights and tips to fortify your defenses because the journey doesn't end here—it evolves.
And remember, the Cyb3rd4nc3 flag for today:
Cyb3rd4nc3{Th3_r34l_s3cur1ty_jOurn3y_n3v3r_3nds!} 🚩 Keep learning, keep adapting, and keep growing. See you in the next phase!

ABOUT AUTHOR

Daniel M. Mwithui

Daniel M. Mwithui is a Certified Cybersecurity Analyst and IT Specialist with a strong foundation in IT support, cybersecurity, and network management. With certifications such as SOC Analyst, HCIA Security, and Google Cybersecurity Professional, Daniel brings over two years of expertise in securing IT infrastructures, investigating incidents, and conducting penetration testing.

A Bachelor of Computer Science graduate, Daniel is also an accomplished trainer and keynote speaker, sharing insights on cybersecurity best practices. His passion for learning and commitment to excellence make him a trusted voice in the cybersecurity space.

Connect with Daniel

- LinkedIn: linkedin.com/in/daniel-mwendwa-bsc-a475311b7/
- GitHub: github.com/daniel-mwendwa