student name: yasindu randika de silva peduru hewa

Student No.: 30438862   
Course Code: ITECH1502

course name: cybersecurity fundamentals



Automated Incident Response Using LetsDefend SOAR Platform

2025

Table of Contents

[Executive Summary 2](#_Toc211726085)

[Introduction 2](#_Toc211726086)

[Problem / Challenge 3](#_Toc211726087)

[Objectives / Project Goal 3](#_Toc211726088)

[Methodology 4](#_Toc211726089)

[Results and Outcomes 6](#_Toc211726090)

[Reflection 8](#_Toc211726091)

[References 9](#_Toc211726092)

# Executive Summary

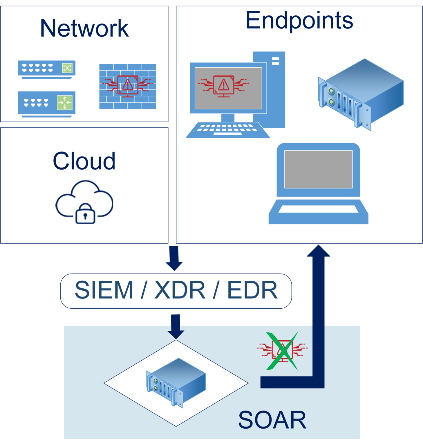
The LetsDefend Security Operations Center (SOC) platform was used to simulate automated incident response across two critical cybersecurity scenarios: a malware exploitation case (SOC336 – Windows OLE Zero-Click RCE) and a phishing-based data exfiltration case (SOC338 – Lumma Stealer). These simulations were designed to strengthen understanding of the NIST Cybersecurity Framework (CSF 2.0) domains, including detection, response, and recovery.

Alerts were examined through integrated SIEM and SOAR functions to identify, contain, and mitigate threats. Evidence such as malicious attachments, phishing URLs, and command-and-control (C2) indicators were verified using VirusTotal and log correlation tools. Endpoint containment and remediation were conducted via Endpoint Detection and Response (EDR) controls, ensuring proper isolation of affected systems.

Each incident was closed following the documentation of Indicators of Compromise (IoCs) and analyst notes. The exercise demonstrated proficiency in digital forensics, incident management, and threat analysis, reflecting the essential competencies required for real-world SOC operations (LetsDefend, 2025; NIST, 2024).

# Introduction

LetsDefend functions as a cloud-based SOC simulation platform designed to train analysts in real-time incident response, forensics, and threat intelligence workflows. It integrates SIEM, SOAR, and XDR functionalities to streamline the automation of alert triage and remediation actions. The exercises conducted correspond with Week 9–10 lecture topics on SOAR automation, incident containment, and log-based threat hunting.



***Figure 1:*** *Simplified workflow showing how SIEM gathers and detects security events, SOAR automates response actions, and XDR extends detection across multiple systems (Airbus Protect, n.d.).*

This diagram contextualizes the incident management process used across both investigations. The practical engagement enabled application of theoretical models discussed in lectures, particularly the NIST CSF phases: Identify, Protect, Detect, Respond, and Recover (NIST, 2024).

# Problem / Challenge

Phishing and malware-based attacks remain the most prevalent cyber threats globally, accounting for over 70 percent of initial intrusion vectors (Verizon, 2024). The challenge addressed was how automated incident response platforms can effectively detect, contain, and mitigate these threats using structured workflows. Within LetsDefend, each incident required identification of the malicious vector, verification of indicators through threat-intelligence sources, and appropriate response within the SOAR playbook.  
A screenshot of a computer

AI-generated content may be incorrect.

***Figure 2:*** *LetsDefend Case Management dashboard showing two analyzed incidents (SOC336 and SOC338) and one prior tutorial case (LetsDefend, 2025).*

This evidence demonstrates completion of multiple investigations under a unified SOC environment, validating system proficiency in automated response.

# Objectives / Project Goal

The exercise aimed to:

1. Apply NIST CSF 2.0 functions (Detect, Respond, and Recover) in practical SOC operations.
2. Demonstrate technical skills in phishing triage, malware containment, and forensic artefact documentation.
3. Evaluate the role of automation in improving incident-handling efficiency.

These objectives directly align with the course outcomes for Cybersecurity Fundamentals, focusing on technical, analytical, and ethical practice within cyber-defence domains.

# Methodology

A structured incident-response approach was adopted in the SOC336 case, which involved analyzing a critical malware alert generated by the LetsDefend Security Operations Center (SOC) platform. The investigation began by taking ownership of the alert within the *Monitoring* dashboard and reviewing the event details, including sender and destination addresses, timestamp, and attachment hash. The suspicious email originated from projectmanagement@pm.me and contained an RTF attachment named *mail.rtf*.

The attachment hash (df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184) was analyzed using VirusTotal, which confirmed detection of the *CVE-2025-21298* exploit. This vulnerability targeted Microsoft OLE components through a malicious RTF file capable of remote-code execution (RCE). Evidence correlation between LetsDefend logs and external scanning tools verified the exploit as genuine and critical.

Following verification, the malware status was assessed within the LetsDefend *Playbook*. The file was confirmed as not quarantined, triggering the containment workflow. Log Management and Endpoint Security modules were then examined to ensure no further propagation occurred. All relevant indicators of compromise (IoCs), including the source IP 84.38.130.118 and email artefacts, were recorded for later reporting.

A screenshot of a computer

AI-generated content may be incorrect.

***Figure 3:*** *LetsDefend event summary for SOC336 showing sender, destination, and malicious RTF attachment linked to CVE-2025-21298 (LetsDefend, 2025).*

A screenshot of a computer

AI-generated content may be incorrect.  
***Figure 4:*** *VirusTotal analysis confirming the malicious RTF file exploiting CVE-2025-21298 (LetsDefend & VirusTotal, 2025).*  
A screenshot of a computer

AI-generated content may be incorrect.

***Figure 5:*** *Indicators of Compromise (IoCs) recorded for SOC336, including file hash, malicious sender, domain, possible C2 address, and internal investigation link (LetsDefend, 2025).*

In the SOC338 incident, a DLL side-loading attack was detected through the LetsDefend Security Operations Center (SOC) platform. The alert indicated malicious activity originating from the domain windows-update.site, associated with the Lumma Stealer malware family. Following the SOAR playbook, the email header, sender identity, and embedded URL were systematically analyzed to determine the source and method of compromise.

The command-and-control (C2) address 132.232.40.201 was identified in the incident log, confirming communication between the attacker’s host and the internal machine 172.16.17.216. This correlation verified that the infected endpoint had interacted with the external C2 server. The Endpoint Detection and Response (EDR) dashboard was then accessed to isolate the affected host and prevent further lateral movement within the network (National Institute of Standards and Technology (NIST, 2024).

A screenshot of a computer

AI-generated content may be incorrect.

***Figure 5:*** *Log Management showing connection between internal host 172.16.17.216 and C2 server 132.232.40.201 before containment (LetsDefend, 2025).*

A combination of forensic verification and dynamic URL analysis was performed using VirusTotal and other sandbox tools, confirming the malicious payload behavior. After all Indicators of Compromise (IoCs) including sender email, domain, C2 IP, and file hash were recorded, the incident was formally closed through the integrated SOAR automation workflow. This structured process demonstrated alignment with the NIST Cybersecurity Framework (CSF 2.0) functions of *Detect, Respond,* and *Recover*, ensuring a complete and traceable incident-response lifecycle (NIST, 2024; LetsDefend, 2025).

# Results and Outcomes

Both investigations were successfully completed within the LetsDefend SOC environment. In the SOC336 (Zero-Click RCE Exploit) case, the malicious RTF file *mail.rtf* was identified as exploiting CVE-2025-21298. The attachment hash, sender domain, and IP address were validated through sandbox and VirusTotal analysis. The email was removed from the recipient’s inbox, and the event was confirmed as a True Positive, demonstrating accurate incident detection and containment aligned with the *Respond (RS.AN)* and *Recover (RC.CO)* subcategories of the NIST CSF 2.0 (NIST, 2024).

In the SOC338 (Lumma Stealer – DLL Side-Loading Attack) case, the investigation achieved a 55 percent score and a 44 percent playbook success rate. Although there were minor deviations from the guided workflow, full containment of the compromised endpoint was achieved through EDR isolation. The C2 IP (*132.232.40.201*) was verified in log management, confirming outbound communication from the infected host. All Indicators of Compromise (IoCs), including sender address, malicious URL, and MD5 file hash, were recorded to assist ongoing monitoring and forensic analysis (LetsDefend, 2025).

A screenshot of a computer

AI-generated content may be incorrect.

***Figure 6:*** *SOC336 case closure summary showing full playbook completion and artefacts recorded during phishing email analysis (LetsDefend, 2025).*

A screenshot of a computer

AI-generated content may be incorrect.

***Figure 7:*** *SOC338 investigation summary showing playbook accuracy, score, and response time during malware containment process (LetsDefend, 2025).*

The investigations demonstrated the ability to identify, analyze, and mitigate both malware and phishing threats while ensuring the integrity of digital evidence. These findings reflected proficiency in using SIEM, SOAR, and EDR tools to execute automated response procedures aligned with the *Detect–Respond–Recover* phases of the NIST Cybersecurity Framework 2.0.

The full playbook reports, including the analyst notes, can be viewed using the following links for further validation and evidence:

* SOC336 Report Summary: <https://app.letsdefend.io/case-management/casedetail/yas0509/257>
* SOC338 Report Summary: <https://app.letsdefend.io/case-management/casedetail/yas0509/316>

# Reflection

The practical activities significantly strengthened both technical and analytical capabilities in cybersecurity operations. Through the investigations of phishing and Lumma Stealer incidents, a deeper understanding of SIEM log correlation, malware artefact analysis, and endpoint containment procedures was developed. The structured playbook approach provided clarity on the stages of the NIST CSF lifecycle, particularly in the areas of detection, response, and recovery.

The most valuable learning outcome was the improvement in interpreting complex log data and identifying malicious indicators such as MD5 hashes, C2 IPs, and suspicious email domains. At the beginning, some difficulty was encountered when linking playbook steps with real-time log evidence. However, repeated investigation practice enhanced accuracy, analytical reasoning, and decision-making confidence.

The exercises also highlighted how automation within SOAR tools reduces manual workload and improves response efficiency during live incidents. The hands-on experience demonstrated how threat intelligence, automation, and forensic verification complement each other in an operational SOC setting.

Future improvement will focus on gaining proficiency in vulnerability scanning, advanced threat-hunting, and forensic documentation to strengthen investigation depth and reporting quality. This experience has provided a solid foundation for developing into a more effective and structured cybersecurity analyst capable of managing real-world incidents.

**A screenshot of a computer

AI-generated content may be incorrect.**

***Figure 8:*** *GitHub portfolio webpage displaying the uploaded LetsDefend artefacts, case study summaries, and reflective analysis as part of the Automated Incident Response project.*

<https://yasindurandika.github.io/cybersecurity-portfolio/>

# References

Australian Cyber Security Centre (ACSC). (2024). *Essential Eight Maturity Model v4.* <https://www.cyber.gov.au/>  
National Institute of Standards and Technology (NIST). (2024). *NIST Cybersecurity Framework 2.0 Core.* <https://www.nist.gov/cyberframework>  
Verizon. (2024). *2024 Data Breach Investigations Report (DBIR).* <https://www.verizon.com/business/resources/reports/dbir/>  
LetsDefend. (2025). *SOC Simulation Platform [Computer software].* <https://app.letsdefend.io/>

Airbus Protect. (n.d.). *MDR, SOC, EDR, XDR, SOAR and SIEM – what does it mean?* Airbus Protect. Retrieved October 16, 2025, from <https://www.airbusprotect.com/insights/mdr-soc-edr-xdr-soar-siem-what-does-it-mean/>