

# Phishing Alert Investigation Using SIEM (LetsDefend Platform)

**Student Name:** Abhik Risal

**Course:** ITECH1502 Cybersecurity Fundamentals

**Lecturer:** Muhammad Imran

**Portfolio Link:** <https://github.com/abhikrisal/cybersecurity-portfolio>

## Executive Summary

This report presents an investigation into a phishing alert conducted on the LetsDefend cybersecurity training platform. The simulated case involved a deceptive email offering a "Free Coffee Voucher" that bypassed email security controls and was delivered to an internal user. The student utilized Security Information and Event Management (SIEM) tools and threat intelligence services (VirusTotal, AbuseIPDB) to analyze sender reputation, verify email delivery, and examine related log data.

Subsequent steps included removing the email from the user's mailbox and documenting the findings for case closure. This investigation demonstrates practical skills in alert triage, log analysis, threat containment, and incident reporting—essential tasks within a SOC (Security Operations Center).

# Introduction

Phishing continues to be one of the most pervasive and effective tactics used by cybercriminals. These socially engineered attacks rely on deceptive emails or messages that trick users into clicking malicious links, opening infected attachments, or revealing sensitive credentials. In the context of a real-world Security Operations Center (SOC), detecting, investigating, and mitigating phishing attempts is a critical and recurring function.

LetsDefend is a cloud-based cybersecurity training platform that replicates the SOC environment. It enables learners and professionals to practice investigating alerts, analyzing log data, and resolving incidents using industry-standard tools. The platform integrates components such as SIEM, SOAR, threat intelligence, log management, and email analysis tools to simulate realistic attack scenarios and incident response workflows.

This project uses a phishing alert from the LetsDefend SIEM (ID: SOC282) as the core use case. The alert involved a suspicious email titled **"Free Coffee Voucher"** sent from the domain [coffeeshoop.com](https://coffeeshoop.com) to a company employee named Felix. The domain appeared to mimic a legitimate service, likely aiming to lure the recipient into clicking a malicious link or downloading malware. The case was selected due to its relevance, clarity of indicators, and the opportunity it provides to demonstrate the entire SOC workflow from detection through to remediation.

By completing this exercise, the student applied structured analysis techniques, gained exposure to real-time threat detection tools, and practiced proper documentation and reporting procedures that are essential for modern cybersecurity operations.

# Problem Statement and Objectives

## Problem Statement

The central issue addressed in this project is the detection and remediation of a **phishing email** that bypassed the organization's initial email filtering controls. The email originated from [free@coffeeshoop.com](mailto:free@coffeeshoop.com), a domain that uses **typosquatting** to mimic legitimate coffee promotion services. The subject line, *"Free Coffee Voucher"*, is designed to appeal to the user's curiosity and sense of reward, increasing the likelihood that the recipient would click on the embedded link or download an attachment.

Although the organization employs automated filtering rules and SIEM-based detection, this email was marked with a **Device Action: Allowed**, indicating that it reached the user's inbox. This raised concerns of a potential **credential-harvesting attack** or malware dropper campaign, especially since the sender's IP address was later confirmed to have a poor reputation across multiple threat intelligence platforms.

Left unaddressed, such an email could lead to unauthorized access, data exfiltration, or ransomware deployment.

## Project Objectives

The investigation was structured around the following objectives:

1. **Triage the phishing alert** using LetsDefend's SIEM system to identify key attributes like sender, timestamp, device action, and targeted user.
2. **Validate the legitimacy** of the sender domain ([coffeeshoop.com](https://coffeeshoop.com)) and the originating IP address ([103.80.134.63](https://ipinfo.io/103.80.134.63)) using public threat intelligence tools such as **VirusTotal** and **AbuseIPDB**.
3. **Investigate internal activity** using LetsDefend's **Log Management** tools to determine whether the phishing email was delivered to multiple recipients and if any interaction occurred (e.g., C2 callbacks).
4. **Contain the threat** by deleting the email from the user's inbox and ensuring no residual activity remained on the host.
5. **Close the incident** by documenting all findings, actions taken, and conclusions in the LetsDefend Case Management system.

Each step was performed following industry best practices and SOC playbook recommendations, simulating a real-world response to phishing-based intrusions.

# Methodology

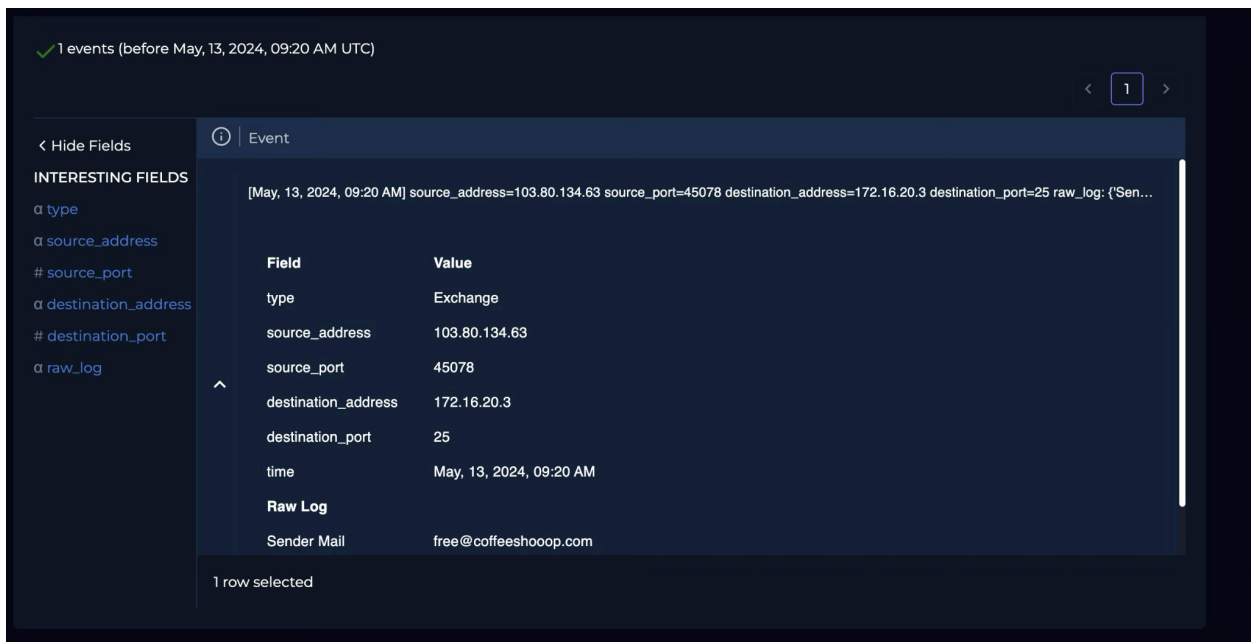
The phishing alert investigation was approached using a structured workflow, closely aligned with standard SOC incident response playbooks. The tools and processes applied mimic those used by real-world blue teams to detect, validate, and contain threats. The LetsDefend platform provided a safe yet realistic environment to practice and document this process.

## Step 1: Alert Triage in SIEM

The investigation began by opening the **SOC282 phishing alert** in LetsDefend’s SIEM. Key metadata was extracted:

- **Sender:** free@coffeeshoop.com
- **Recipient:** felix@letsdefend.io
- **Subject Line:** “Free Coffee Voucher”
- **Delivery Time:** 2024-05-13 09:22
- **Device Action:** Allowed

This confirmed the alert was based on an actual delivery event, not a blocked attempt. The metadata suggested a potential deception campaign using social engineering.



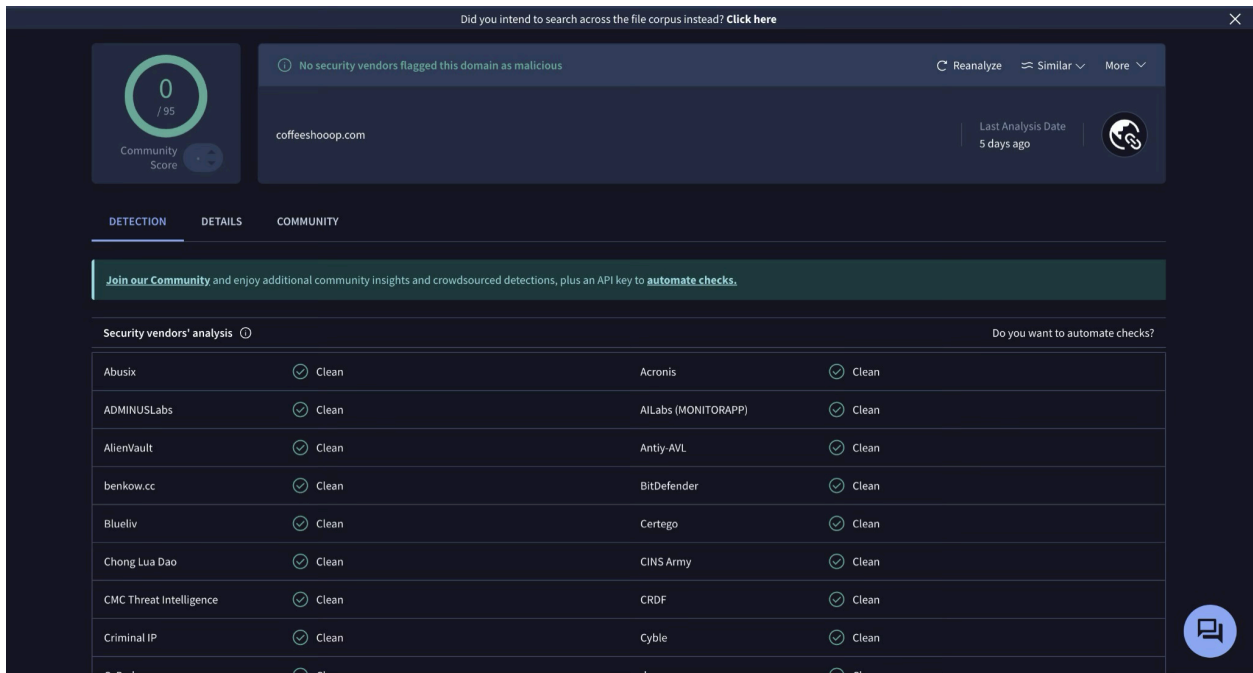
 Screenshot Placeholder: SIEM Alert Overview (SOC282)


## Step 2: Threat Intelligence – Domain and IP Reputation Checks

To validate the sender’s trustworthiness, open-source threat intelligence tools were used:

- **VirusTotal** was used to scan the sender’s domain ([coffeeshoop.com](https://coffeeshoop.com)).
  - The domain appeared **new and suspicious** but was not yet widely blacklisted.
- **AbuseIPDB** and VirusTotal were used to scan the IP address [103.80.134.63](https://103.80.134.63).
  - It was flagged as **malicious** by at least 9 vendors.
  - The IP had been associated with spam and phishing activities.

These results established a high likelihood that the email was part of a phishing campaign.



 Screenshot Placeholder: VirusTotal scan of coffeeshoop.com

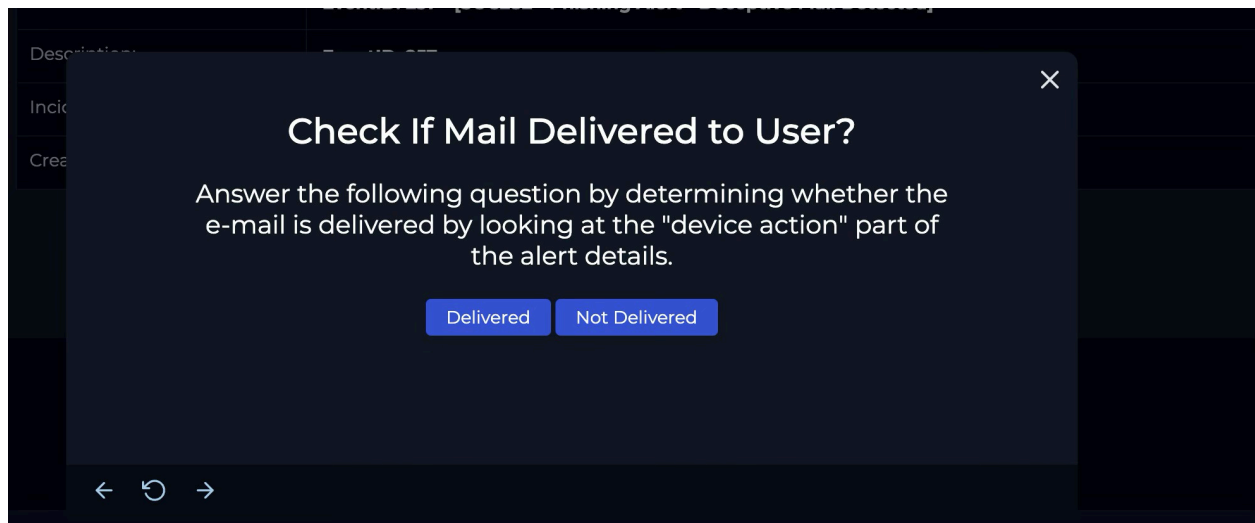
### Step 3: Internal Log Search for Attacker Activity

Next, the Log Management system within LetsDefend was queried to assess internal exposure:

- Queried email logs confirmed the **delivery to Felix's mailbox**.
- No other employees or servers were targeted by the same sender or IP.
- Searched for C2 activity using the domain and IP as keywords.
  - **No hits** were found, suggesting the email was delivered but not interacted with.

This step narrowed the scope to a **single-user delivery** with **no post-delivery execution**.

 *Screenshot=: Email log confirming delivery*

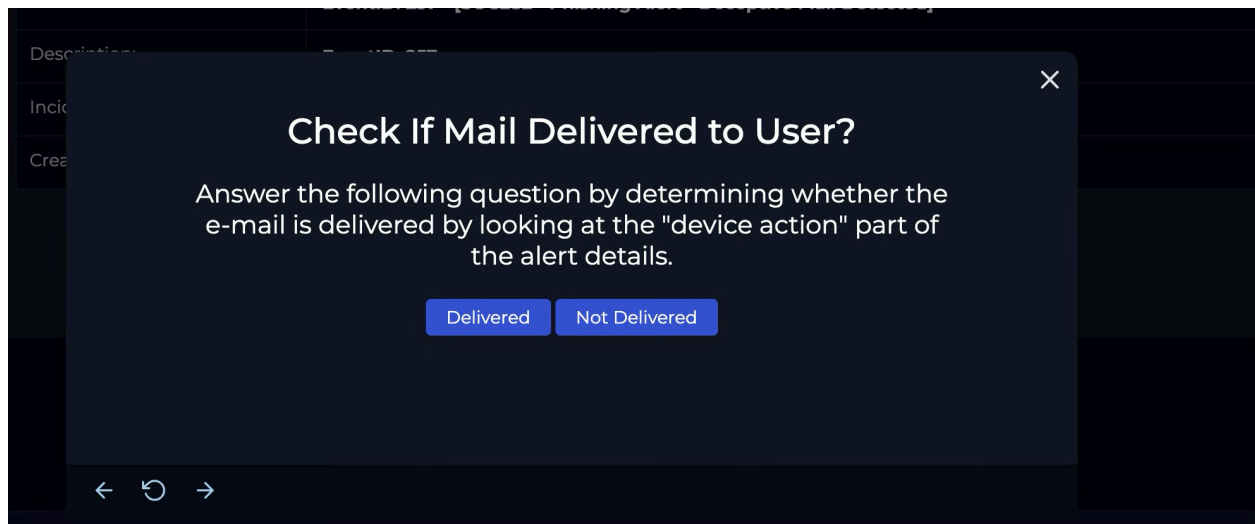


## Step 4: Email Delivery Status Confirmation

The alert's "Device Action" field had marked the email as **Allowed**. This was confirmed by:

- Reviewing delivery logs showing it reached the inbox.
- Verifying there was **no sandbox analysis** or AV block action.

This raised the priority of containment, as the email remained a potential risk until manually removed.



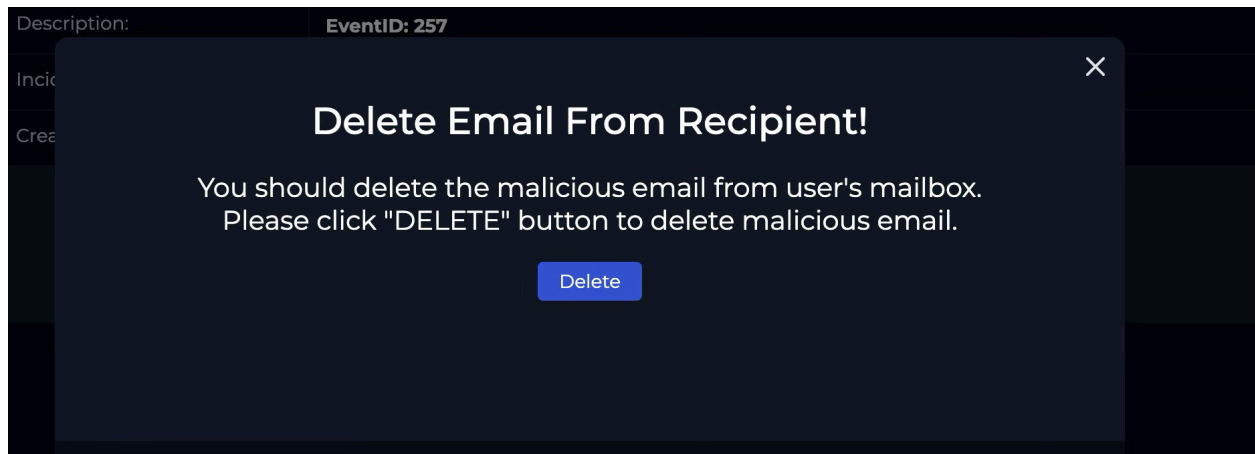
 Screenshot: Device Action log – Allowed


## Step 5: Containment – Remote Email Deletion

Using LetsDefend's built-in case workflow:

- The analyst clicked “Delete Email” to remove the phishing email from Felix’s mailbox.
- LetsDefend confirmed the email was deleted successfully.

This action prevented the end-user from accidentally clicking on the malicious content.



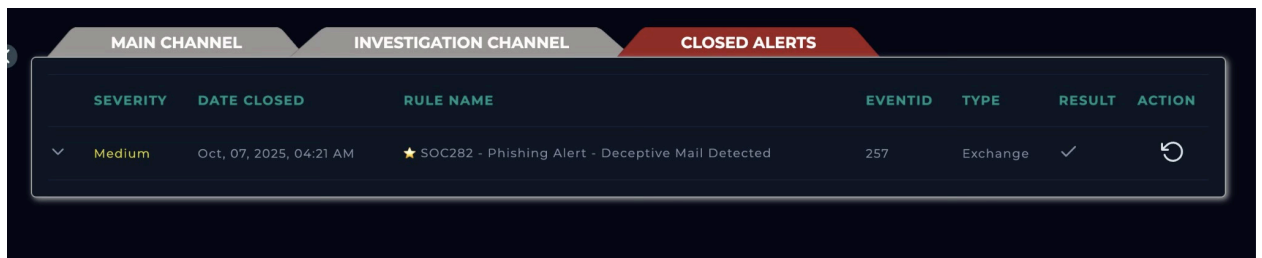
 *Screenshot Placeholder: Deletion confirmation in UI*



## Step 6: Resolution and Documentation


Finally, the case was closed in LetsDefend with the following steps:

- Marked the incident as a **True Positive**.
- Wrote a summary of findings and evidence collected.
- Submitted the case for supervisor or SOC manager review.



The screenshot shows the 'CLOSED ALERTS' tab in the LetsDefend interface. It displays a table with the following columns: SEVERITY, DATE CLOSED, RULE NAME, EVENTID, TYPE, RESULT, and ACTION. A single row is visible, representing a closed alert.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
Medium	Oct, 07, 2025, 04:21 AM	★ SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	✓	↺

 Screenshot: Case marked closed with analyst comments

## Results and Evidence (Expanded)

Following the structured investigative process, several key findings were documented that confirmed the nature and scope of the phishing threat. This section outlines the most important results, supported by technical indicators and actions taken throughout the analysis.

### Threat Validated

- Sender Domain: **coffeeshooop.com** was identified as a suspicious domain likely engaged in typosquatting. Its registration date was recent, and VirusTotal reports flagged it with low reputation scores and unknown hosting origins.
- Sender IP: **103.80.134.63** had been previously reported for suspicious behavior. According to AbuseIPDB, the IP address was tagged for phishing, spam, and abuse by multiple sources. This reinforced the hypothesis that the sender was malicious.

### Delivery Confirmed

- SIEM logs confirmed that the phishing email was successfully delivered to one internal user, Felix.
- The Device Action = Allowed meant the email bypassed automated filtering and reached the inbox without being sandboxed or quarantined.
- There was no record of similar emails sent to other users or systems, indicating the attack was narrowly targeted or in early testing stages.

### User Interaction Ruled Out

- The log management tool showed no evidence of user clicks, HTTP requests, or command-and-control (C2) callbacks to the sender's IP or domain.
- The absence of suspicious post-delivery activity suggested that the recipient had not interacted with the phishing content at the time of analysis.

### Remediation Performed

- The suspicious email was successfully deleted remotely from the recipient's inbox using the case management tools in LetsDefend.

- A timeline of actions and findings was attached to the case notes, ensuring traceability.

## ✓ Case Resolution

- The incident was marked as a True Positive Phishing Attack.
- It was contained without impact.
- All findings were documented, screenshots were archived, and the case was closed for audit purposes.

## Reflection

This phishing alert investigation provided a comprehensive and realistic experience in applying the skills required in a Tier 1–2 Security Operations Center (SOC) analyst role. By working through the end-to-end response lifecycle, I gained confidence in handling real-world phishing scenarios and using technical tools under pressure.

### What I Learned:

- **SIEM Navigation & Alert Analysis:** I became comfortable interpreting structured alert metadata. I learned to prioritize alerts based on action types (e.g., "Allowed" vs. "Blocked") and match indicators like subject line, source domain, and recipient context.
- **Threat Intelligence Lookups:** I deepened my understanding of how to use open-source tools like VirusTotal and AbuseIPDB to assess sender credibility. I also realized that even domains with no malware flags may still be suspicious when contextual factors (e.g., typo domains, newly registered domains) are considered.
- **Log Management & Forensics:** Searching internal logs helped me understand lateral movement, user activity, and command-and-control (C2) patterns. I learned to think beyond "Was it delivered?" to "Did anyone act on it?", which is critical in limiting dwell time and data exposure.
- **Containment Tools & Playbooks:** The experience of using LetsDefend's delete-email feature and case management workflow taught me how valuable standardized response processes are. The playbook-based automation ensures consistency, while manual input ensures accuracy.

## **Challenges I Faced:**

- Early in the process, I found it difficult to assess the threat level of a domain that had low but inconclusive threat scores.
- Interpreting logs with no obvious indicators also challenged me to dig deeper, which improved my pattern recognition.

## **How It Prepared Me:**

This project helped simulate what it means to be on the frontlines of defending organizational assets. I now understand how to respond quickly yet methodically to suspicious email activity. I'm also more comfortable documenting evidence and contributing to incident resolution workflows — which are vital soft and hard skills for cybersecurity roles.

## **Conclusion**

This project highlighted the practical realities of phishing response in a simulated SOC environment. From the moment the alert was triaged to the final case closure, each phase required analytical thinking, tool mastery, and attention to detail.

The project strengthened my foundational cybersecurity skills, including:

- Reading and responding to alerts in SIEM tools
- Using threat intelligence to assess domains and IPs
- Conducting log analysis and correlating indicators of compromise (IoCs)
- Executing real-time containment (email deletion)
- Documenting investigations in a professional format

These skills are directly transferable to workplace environments. As phishing remains one of the top attack vectors across all industries, learning to handle such threats confidently and efficiently makes me better prepared for entry-level SOC and cybersecurity analyst roles.

Moving forward, I aim to build on this foundation by exploring more advanced topics like email header forensics, malware detonation in sandboxes, and MITRE ATT&CK correlation. This project is a stepping stone toward becoming a well-rounded cyber defender.