

ABHIK RISAL

30419133

ITECH1502 Cybersecurity Fundamentals

Week 10 Lab Activities – Exploring SIEM, SOAR, and XDR in Practice

Investigation Case: SOC282 – Phishing Alert (Deceptive Mail Detected)

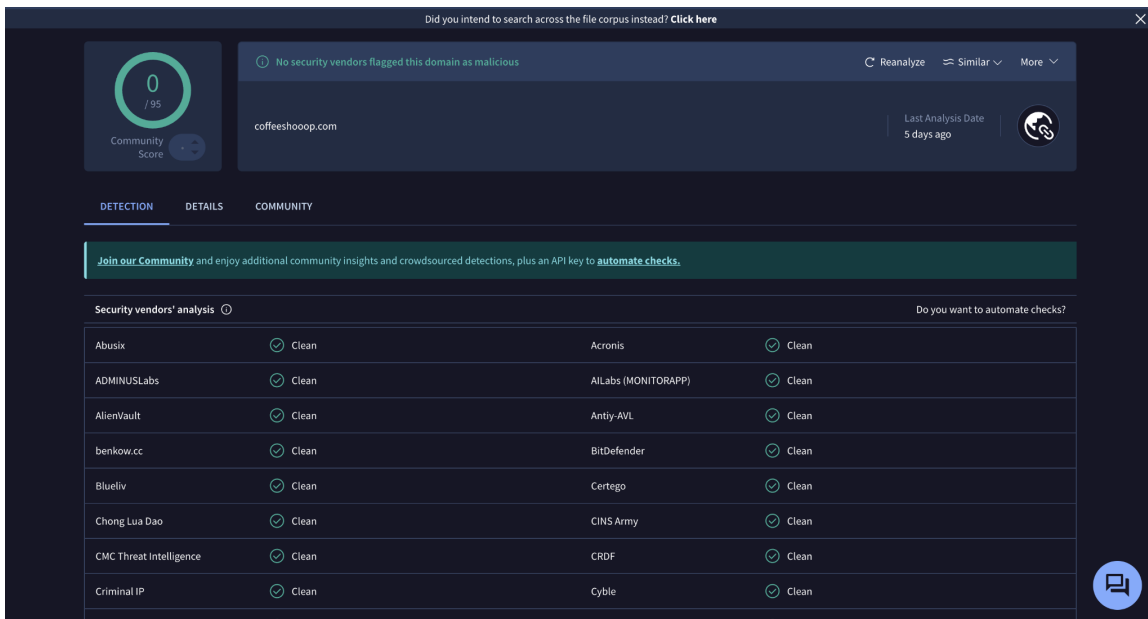
Task Overview

This lab focused on investigating a phishing alert detected in LetsDefend's SIEM environment. The case, labeled SOC282, involved a deceptive email titled 'Free Coffee Voucher' sent from free@coffeeshoop.com to felix@letsdefend.io. The purpose of the exercise was to follow a structured Security Operations Center (SOC) workflow to validate the alert, analyze logs, verify delivery, remove the email, and close the incident.

Evidence (Screenshots)

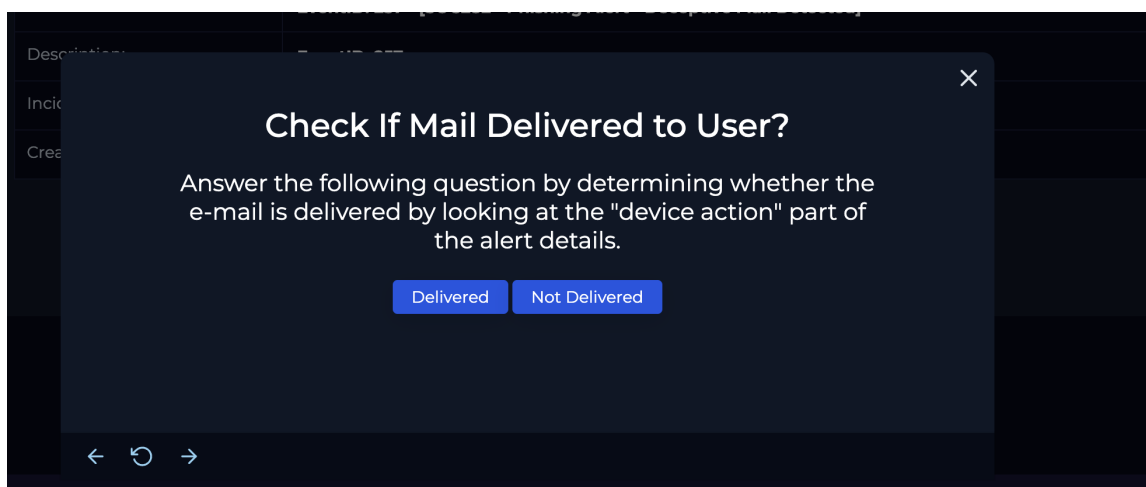
- 1. Screenshot 1 – Initial Alert: SOC282 Phishing Email Detected (Free Coffee Voucher).





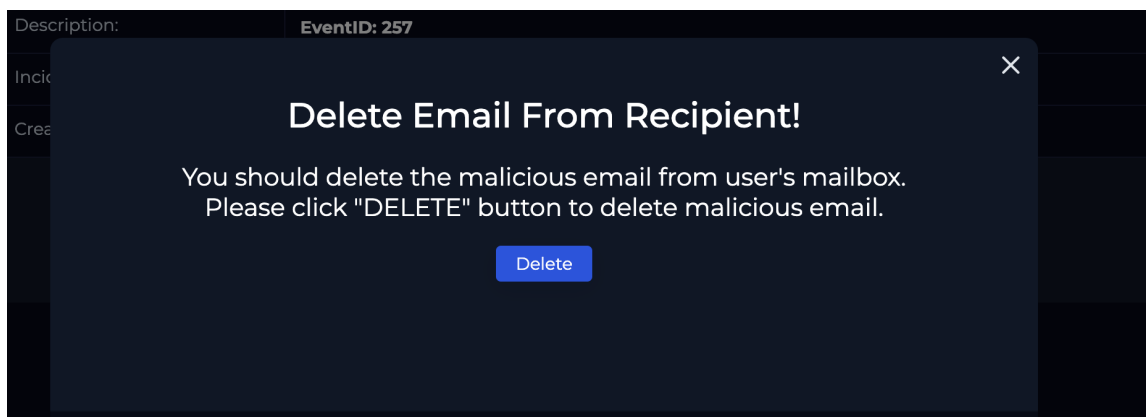
[Insert corresponding screenshot here]

2. Screenshot 3 – Log Management: Source IP 103.80.134.63 Exchange communication

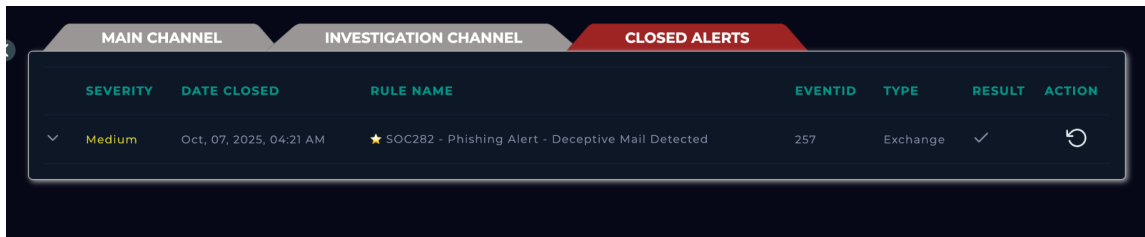


evidence.

3. Screenshot 4 – Mail Delivery Verification: Device Action indicates email delivered.



4. Screenshot 5 – Email Deletion Confirmation: Malicious email removed from user mailbox.
5. Screenshot 6 – Closed Alert: SOC282 case marked as resolved and mitigated.



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

Artifacts Collected

The following Indicators of Compromise (IOCs) were identified and documented during the investigation:

- Sender Email: free@coffeeshooop.com
- Recipient Email: felix@letsdefend.io
- Source IP: 103.80.134.63
- Domain: coffeeshooop.com
- Email Subject: Free Coffee Voucher

These artifacts were added to the case management record for correlation and future intelligence reference.

Reflection

This Week 10 lab provided a complete hands-on experience in analyzing phishing incidents using SIEM tools. The exercise demonstrated the workflow from alert detection to containment and case closure. Initially, the SOC282 alert identified a phishing email attempting social engineering through a fake voucher offer. Using VirusTotal, the sender domain was verified as non-malicious, which confirmed the alert as a low-severity or training scenario. The investigation still followed a standard incident-response flow: checking delivery, deleting the message, and validating that no malicious connections occurred.

The final steps included confirming that the message was delivered (Device Action: Allowed), performing deletion, and verifying in log management that the malicious domain

was not accessed (no C2 traffic). After these steps, the case was closed as mitigated. This exercise highlighted the importance of verification and documentation in SOC operations. It also reinforced how SIEM tools streamline incident analysis, provide visibility, and integrate with SOAR and XDR frameworks for rapid response and improved accuracy.