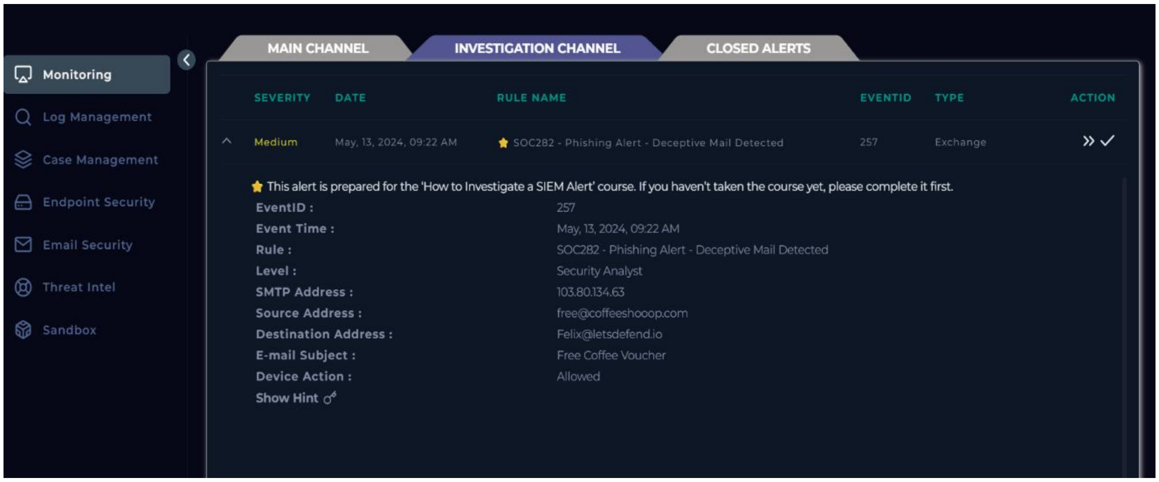
SOC282 - Phishing Alert - Deceptive Mail Detected [Let's Defend – Write-up]

The primary objective of this investigation is to simulate the end-to-end workflow of a SOC Analyst when responding to a high-priority security alert. This exercise focuses on understanding the technical nuances of a phishing attack, executing the predefined Incident Response Playbook, and determining the necessary remediation steps to protect the organizational environment.

| Start Investigation



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	May, 13, 2024, 09:22 AM	★ SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	» ✓

★ This alert is prepared for the 'How to Investigate a SIEM Alert' course. If you haven't taken the course yet, please complete it first.

EventID :	257
Event Time :	May, 13, 2024, 09:22 AM
Rule :	SOC282 - Phishing Alert - Deceptive Mail Detected
Level :	Security Analyst
SMTP Address :	103.80.134.63
Source Address :	free@coffeeshooop.com
Destination Address :	Felix@letsdefend.io
E-mail Subject :	Free Coffee Voucher
Device Action :	Allowed

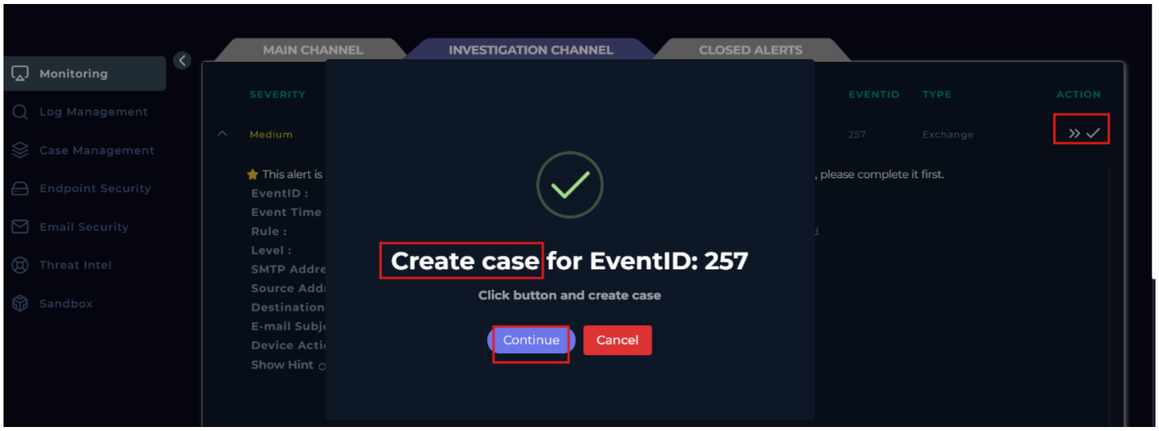
Show Hint

Figure 1: SOC282 - Phishing Alert - Deceptive Mail Detected Alert.

At the beginning of the analysis, I reviewed the alert details and identified the following information:

- **Alert Type:** Phishing Alert - Deceptive Mail Detected.
- **Event ID:** 257.
- **Event Time:** May 13, 2024, 09:22 AM.
- **Sender (Source Address):** free@coffeeshooop.com.
- **Receiver (Destination Address):** Felix@letsdefend.io.
- **E-mail Subject:** Free Coffee Voucher.
- **SMTP Address:** 103.80.134.63.
- **Device Action:** Allowed.

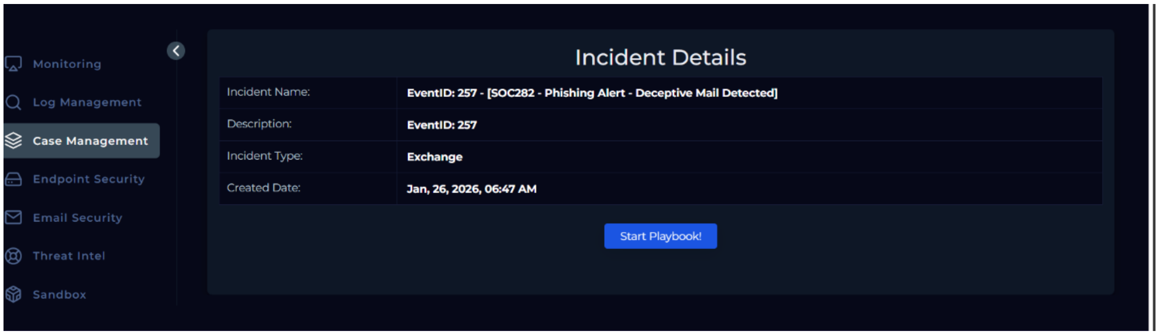
This information will help me during the analysis to track the origin and impact of the threat. Therefore, I want to take action on it and link the alert by selecting Create Case. This action transitions the investigation from a pending alert to an active incident, allowing for formal documentation and playbook execution.



Create case for EventID: 257

Click button and create case

Figure 2: Create case.

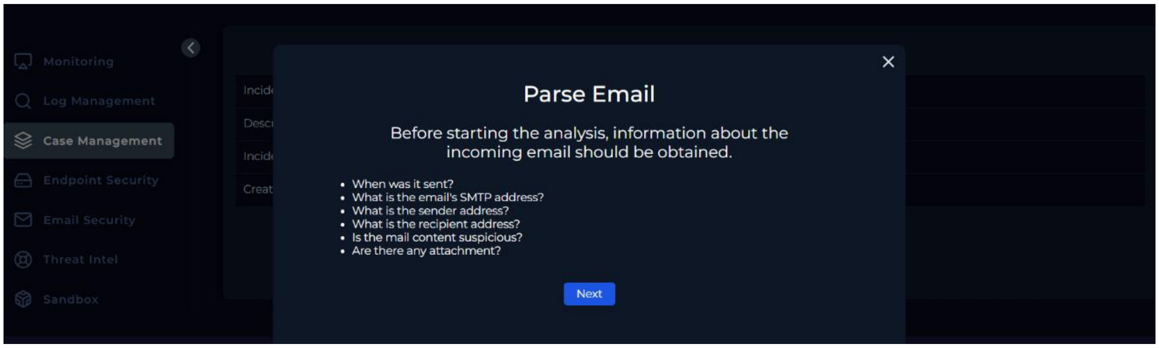


Incident Details

Incident Name:	EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]
Description:	EventID: 257
Incident Type:	Exchange
Created Date:	Jan, 26, 2026, 06:47 AM

Figure 3: start investigation using Playbook.

After clicking Start Playbook, I will address the series of investigative questions provided to complete the analysis based on the established playbook.



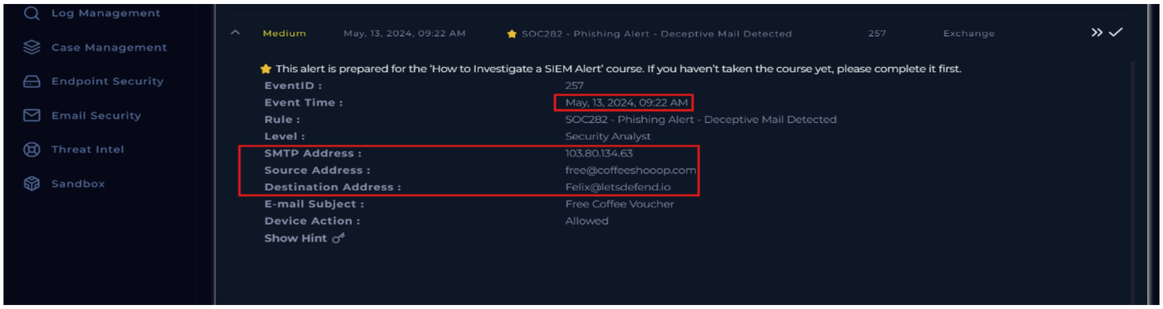
Parse Email

Before starting the analysis, information about the incoming email should be obtained.

- When was it sent?
- What is the email's SMTP address?
- What is the sender address?
- What is the recipient address?
- Is the mail content suspicious?
- Are there any attachment?

Figure 4: First Questions.

The answers to the first four questions are found directly within the alert notice:



Medium May, 13, 2024, 09:22 AM SOC282 - Phishing Alert - Deceptive Mail Detected 257 Exchange

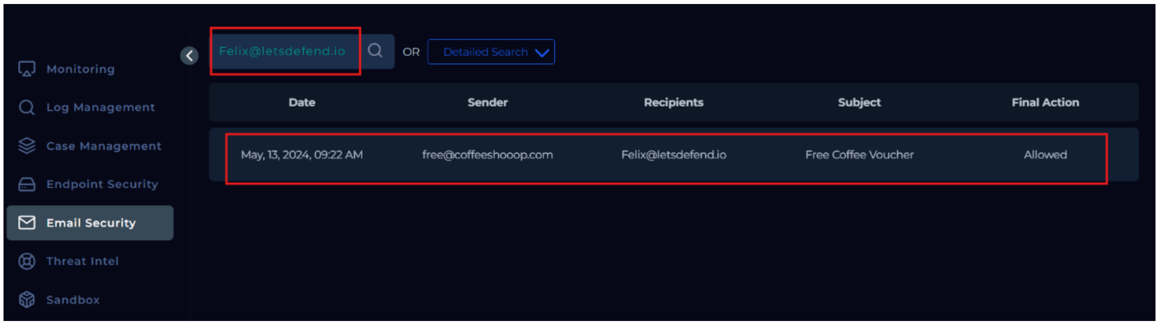
This alert is prepared for the 'How to Investigate a SIEM Alert' course. If you haven't taken the course yet, please complete it first.

EventID :	257
Event Time :	May, 13, 2024, 09:22 AM
Rule :	SOC282 - Phishing Alert - Deceptive Mail Detected
Level :	Security Analyst
SMTP Address :	103.80.134.63
Source Address :	free@coffeeshooop.com
Destination Address :	Felix@letsdefend.io
E-mail Subject :	Free Coffee Voucher
Device Action :	Allowed
Show Hint	

Figure 5: The answers.

1. When was it sent?
   - **Sent Date:** May 13, 2024, 09:22 AM.
2. What is the email's SMTP address?
   - **SMTP Address:** 103.80.134.63.
3. What is the sender address?
   - **Sender Address:** free@coffeeshooop.com.
4. What is the recipient address?
   - **Recipient Address:** Felix@letsdefend.io.

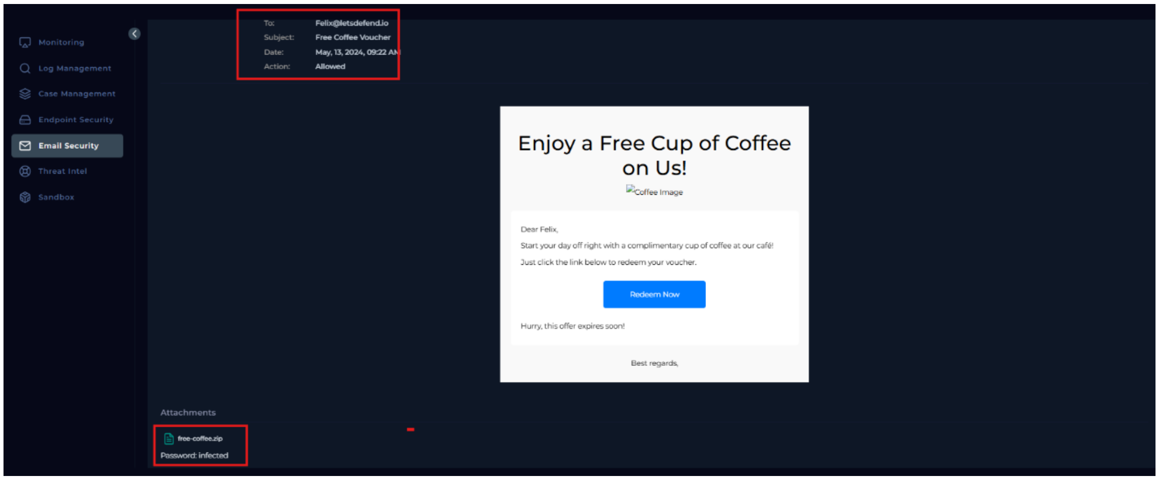
To answer the remaining questions, the next step is to examine the Email Security section to analyze the specific details of the message.



Date	Sender	Recipients	Subject	Final Action
May, 13, 2024, 09:22 AM	free@coffeeshooop.com	Felix@letsdefend.io	Free Coffee Voucher	Allowed

Figure 6: The Email sent.

I searched the Email Security section for the recipient's address to review the specific email messages associated with it.



To: Felix@letsdefend.io
Subject: Free Coffee Voucher
Date: May, 13, 2024, 09:22 AM
Action: Allowed

Enjoy a Free Cup of Coffee on Us!

Dear Felix,

Start your day off right with a complimentary cup of coffee at our café!

Just click the link below to redeem your voucher.

Hurry, this offer expires soon!

Best regards,

free-coffee.zip
Password: infected

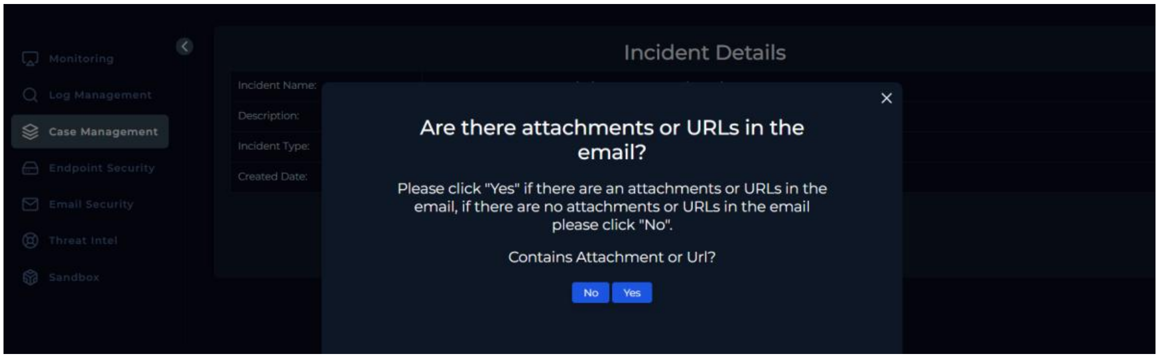
Figure 7: Email content.

After reviewing the **Email Security** section, I found that an email sent to **Felix@letsdefend.io** contained both a "Redeem Now" link and a malicious attachment named **free-coffee.zip** (password: **infected**).

5. Is the mail content suspicious?

- Yes, the mail content is suspicious

6. Are there any attachment?
    - Yes, there is an attachment named **free-coffee.zip**



Are there attachments or URLs in the email?

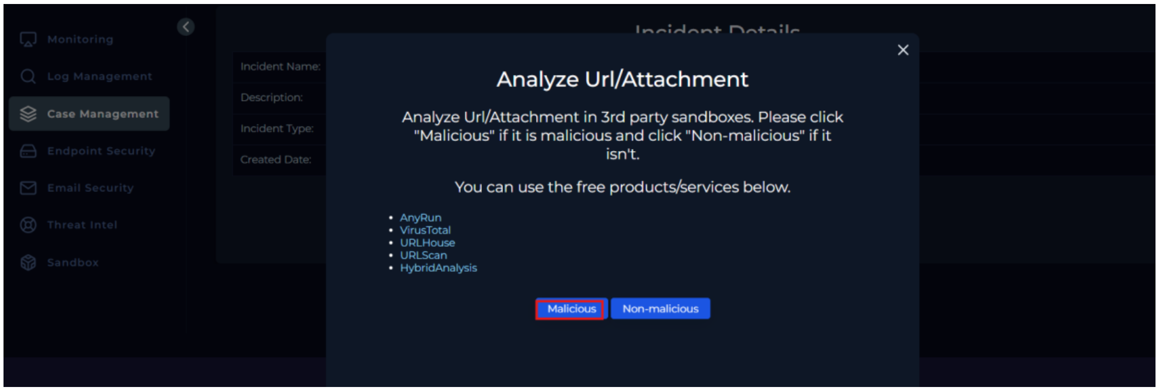
Please click "Yes" if there are an attachments or URLs in the email, if there are no attachments or URLs in the email please click "No".

Contains Attachment or Url?

Figure 8: Next Playbook Question.

Answer: Yes

- **Attachment Found:** The email contains an attached file titled **free-coffee.zip** located at the bottom of the message.
- **URL Found:** The email body includes a "Redeem Now" button that links to an external download URL.
- **Suspicious Indicator:** The attachment is password-protected with the word **"infected"**, which is a high-risk indicator often used to conceal malicious content from automated scanners.



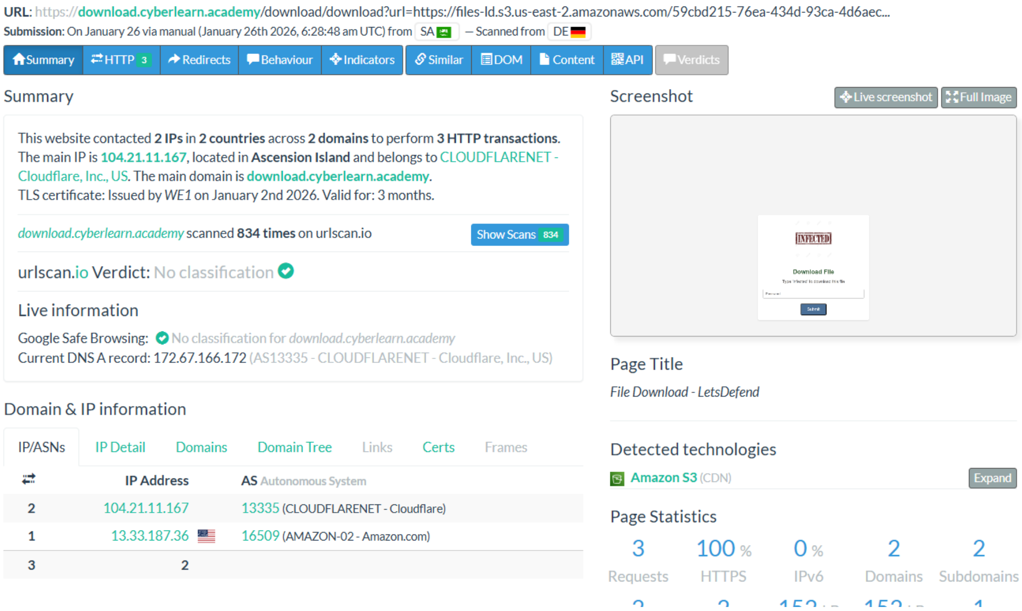
Analyze Url/Attachment

Analyze Url/Attachment in 3rd party sandboxes. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

Figure 9: Next Playbook Question.

Yes, This URL is Malicious.



URL: https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec...
Submission: On January 26 via manual (January 26th 2026, 6:28:48 am UTC) from SA — Scanned from DE

Summary

This website contacted **2 IPs** in **2 countries** across **2 domains** to perform **3 HTTP transactions**. The main IP is 104.21.11.167, located in **Ascension Island** and belongs to CLOUDFLARENET - Cloudflare, Inc., US. The main domain is **download.cyberlearn.academy**.
TLS certificate: Issued by *WE1* on January 2nd 2026. Valid for: 3 months.

download.cyberlearn.academy scanned **834 times** on urlscan.io

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *download.cyberlearn.academy*
Current DNS A record: 172.67.166.172 (AS13335 - CLOUDFLARENET - Cloudflare, Inc., US)

Domain & IP information

⇄	IP Address	AS Autonomous System
2	104.21.11.167	13335 (CLOUDFLARENET - Cloudflare)
1	13.33.187.36	16509 (AMAZON-02 - Amazon.com)
3	2	

Screenshot

Page Title

File Download - LetsDefend

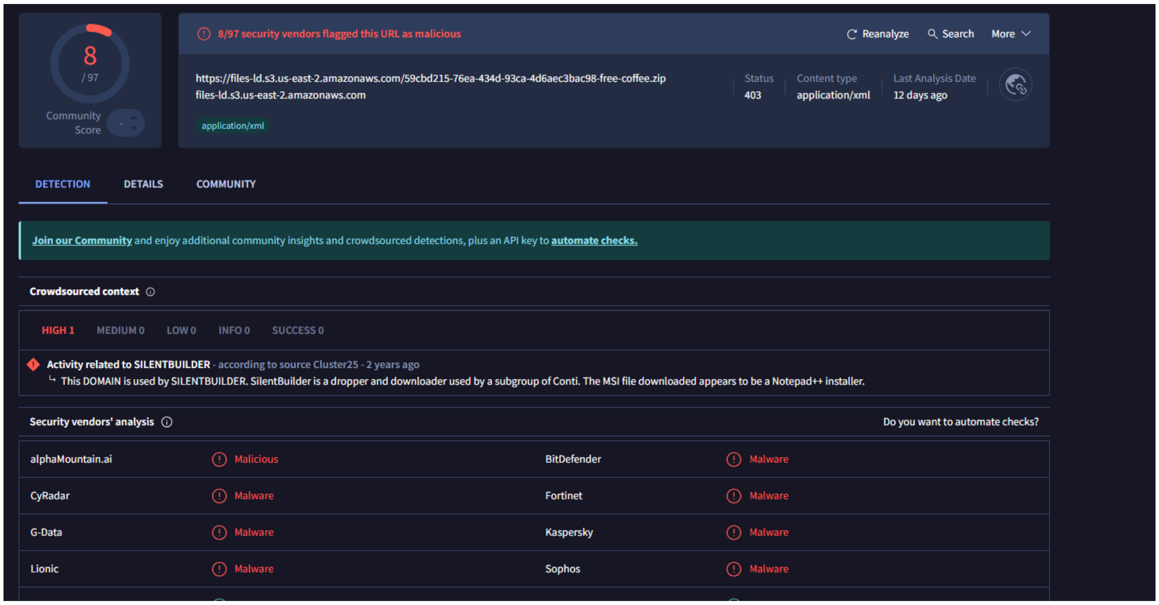
Detected technologies

Amazon S3 (CDN)

Page Statistics

3	100 %	0 %	2	2
Requests	HTTPS	IPv6	Domains	Subdomains

Figure 10: urlscan result.



8 / 97 Community Score

8/97 security vendors flagged this URL as malicious

https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip
files-ld.s3.us-east-2.amazonaws.com
application/xml

Status	Content type	Last Analysis Date
403	application/xml	12 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

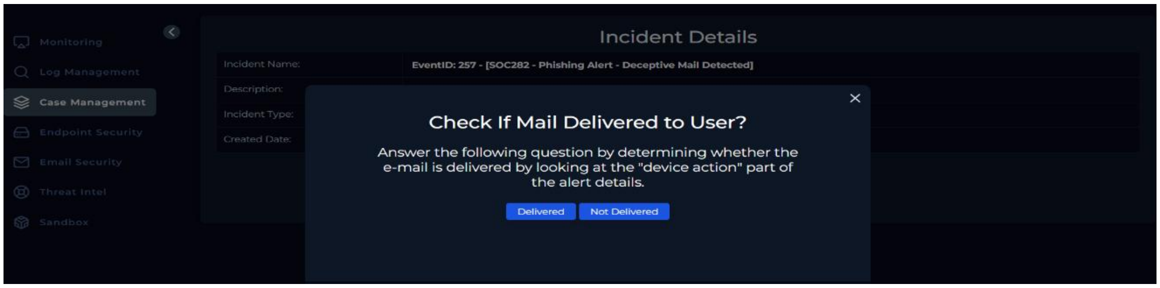
Activity related to SILENTBUILDER - according to source Cluster25 - 2 years ago
↳ This DOMAIN is used by SILENTBUILDER. SilentBuilder is a dropper and downloader used by a subgroup of Conti. The MSI file downloaded appears to be a Notepad++ installer.

Security vendors' analysis — Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malware	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malware	Sophos	Malware

Figure 11: Virstotal result.

Third-party analysis via VirusTotal and urlscan.io confirms the URL is malicious. The link directs to an Amazon S3 bucket to download a password-protected ZIP file. Furthermore, VirusTotal flagged the domain associated with 'SILENTBUILDER,' a known downloader used by cybercrime groups.



Incident Details

Incident Name: EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]

Description:

Incident Type:

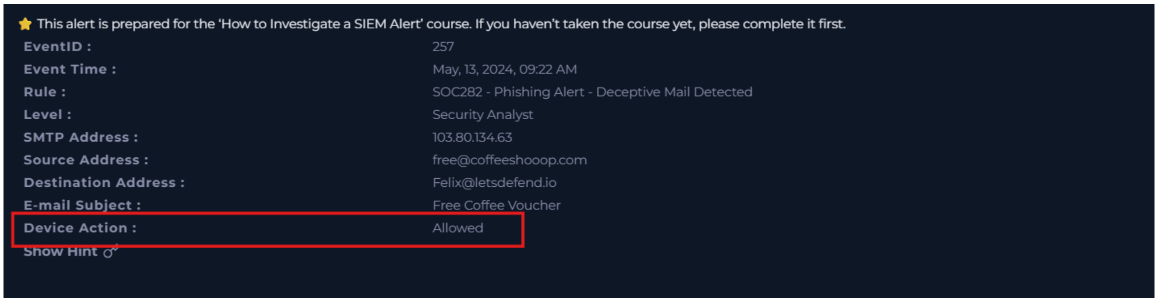
Created Date:

Check If Mail Delivered to User?

Answer the following question by determining whether the e-mail is delivered by looking at the "device action" part of the alert details.

Figure 12: Next Playbook Question.

Email is considered 'Delivered' if the Device Action is marked as 'Allowed,' indicating it bypassed security filters and reached the user's inbox; however, if the action is 'Deleted,' 'Blocked,' or 'Quarantined,' it means the security system successfully intercepted the threat, and the status should be marked as 'Not Delivered'.

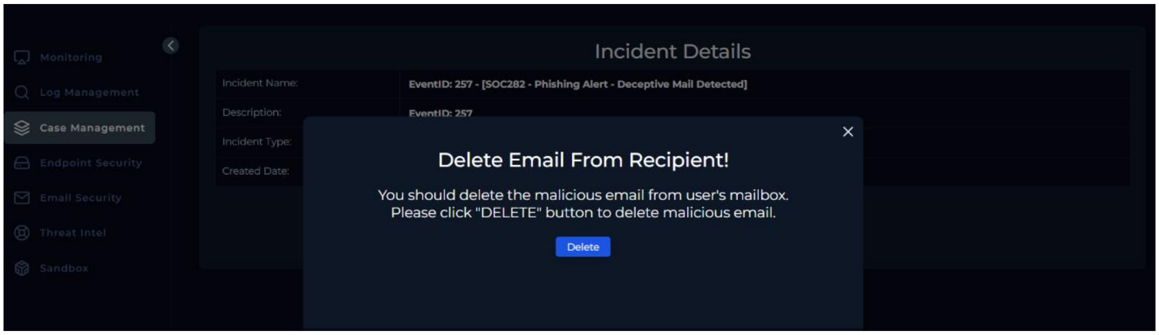


⭐ This alert is prepared for the 'How to Investigate a SIEM Alert' course. If you haven't taken the course yet, please complete it first.

EventID :	257
Event Time :	May, 13, 2024, 09:22 AM
Rule :	SOC282 - Phishing Alert - Deceptive Mail Detected
Level :	Security Analyst
SMTP Address :	103.80.134.63
Source Address :	free@coffeeshooop.com
Destination Address :	Felix@letsdefend.io
E-mail Subject :	Free Coffee Voucher
Device Action :	Allowed

Figure 13: The Alert Content.

Based on the investigation, the email was successfully Delivered. This is confirmed by the 'Device Action' in the alert details, which is set to 'Allowed,' indicating the security system did not block the message.



Incident Details

Incident Name: EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]

Description: EventID: 257

Incident Type:

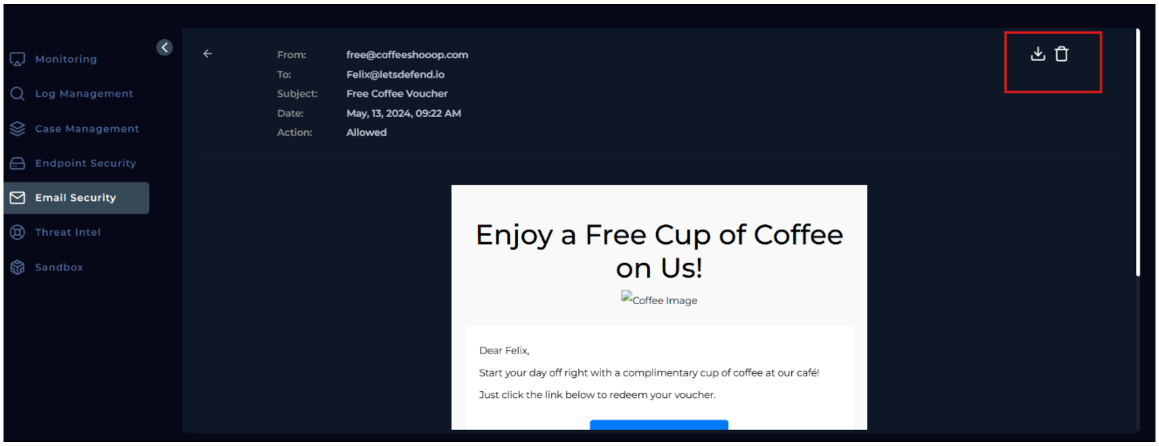
Created Date:

Delete Email From Recipient!

You should delete the malicious email from user's mailbox. Please click "DELETE" button to delete malicious email.

Figure 14: Next Playbook Question.

Since the email was confirmed as Malicious and was successfully Delivered to the inbox, we must now proceed to the 'Email Security' section to delete the message and prevent the user from interacting with it.



From: free@coffeeshooop.com
To: Felix@letsdefend.io
Subject: Free Coffee Voucher
Date: May, 13, 2024, 09:22 AM
Action: Allowed

Enjoy a Free Cup of Coffee on Us!

Coffee Image

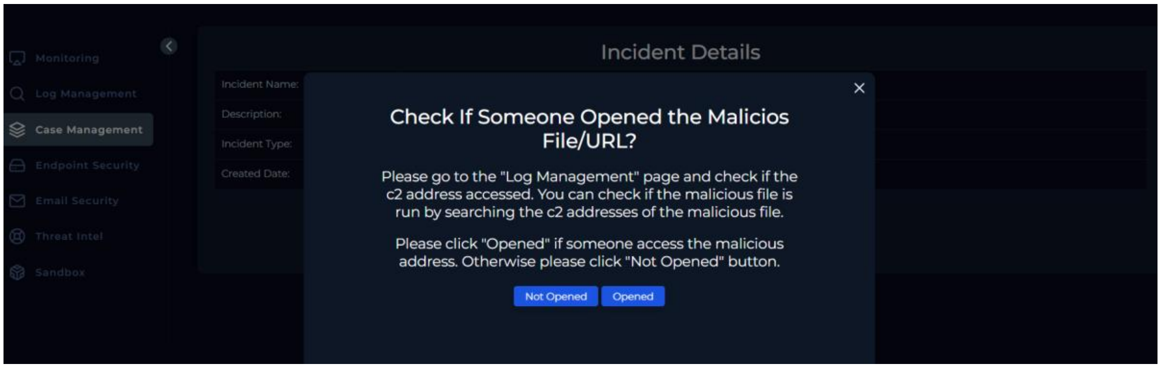
Dear Felix,

Start your day off right with a complimentary cup of coffee at our café!

Just click the link below to redeem your voucher.

Figure 15: Delete Email.

We successfully deleted the email.



Incident Details

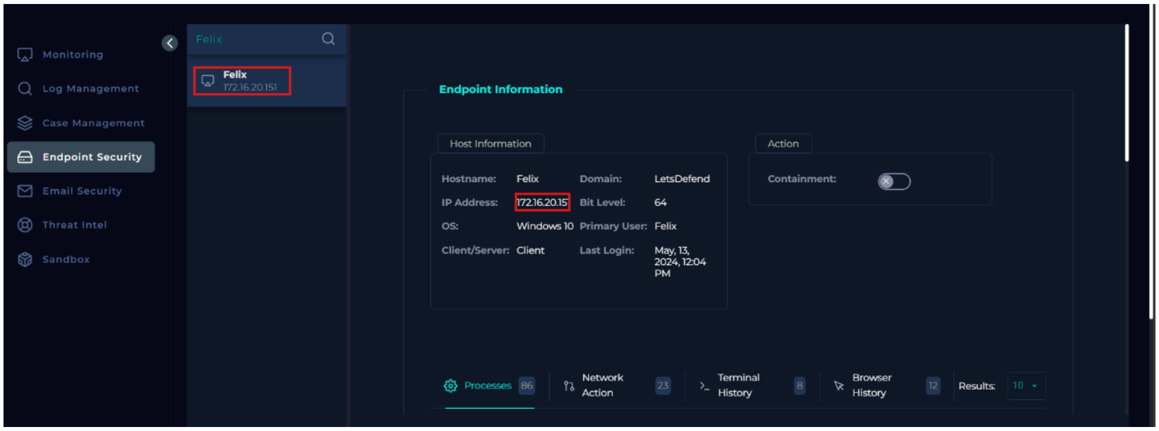
Check If Someone Opened the Malicios File/URL?

Please go to the "Log Management" page and check if the c2 address accessed. You can check if the malicious file is run by searching the c2 addresses of the malicious file.

Please click "Opened" if someone access the malicious address. Otherwise please click "Not Opened" button.

Figure 16: Next Playbook Question.

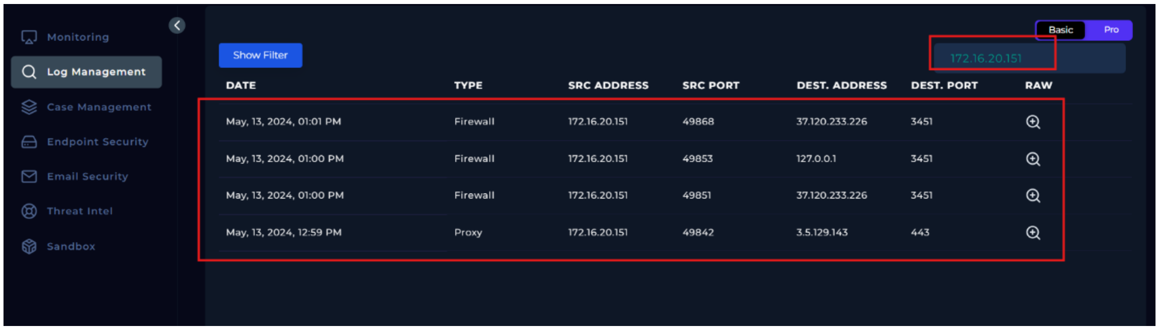
To investigate if the malicious link or file was accessed, I navigated to 'Endpoint Security' and searched for Felix's host details. I successfully identified Felix's IP address, which I will now use to cross-reference with 'Log Management' to check for any connections to the identified C2 addresses.



Hostname: Felix
Domain: LetsDefend
IP Address: 172.16.20.15
Bit Level: 64
OS: Windows 10
Primary User: Felix
Client/Server: Client
Last Login: May, 13, 2024, 12:04 PM

Figure 17: Endpoint Security Content.

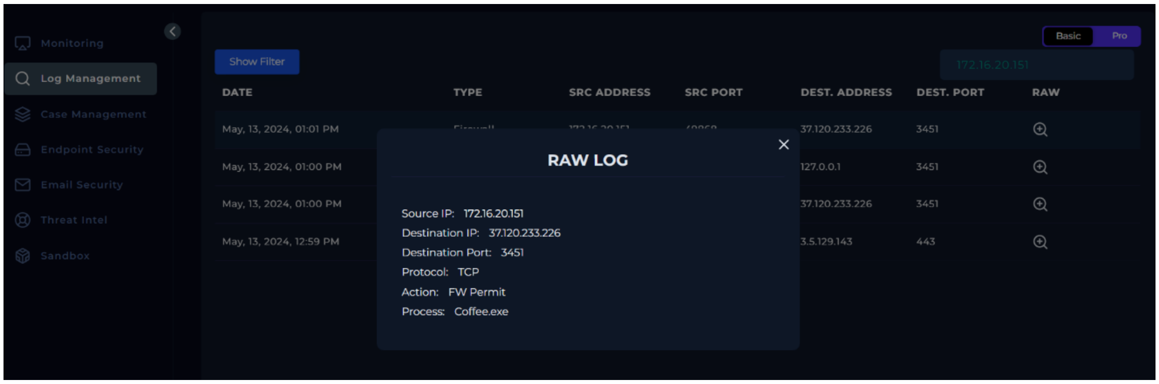
Felix's IP (172.16.20.151)



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
May, 13, 2024, 01:01 PM	Firewall	172.16.20.151	49868	37.120.233.226	3451	🔍
May, 13, 2024, 01:00 PM	Firewall	172.16.20.151	49853	127.0.0.1	3451	🔍
May, 13, 2024, 01:00 PM	Firewall	172.16.20.151	49851	37.120.233.226	3451	🔍
May, 13, 2024, 12:59 PM	Proxy	172.16.20.151	49842	3.5.129.143	443	🔍

Figure 18: Log Management Content.

After checking the Log Management for Felix's IP (172.16.20.151), I discovered network logs from the same date as the initial incident. While these logs show active outbound connections.

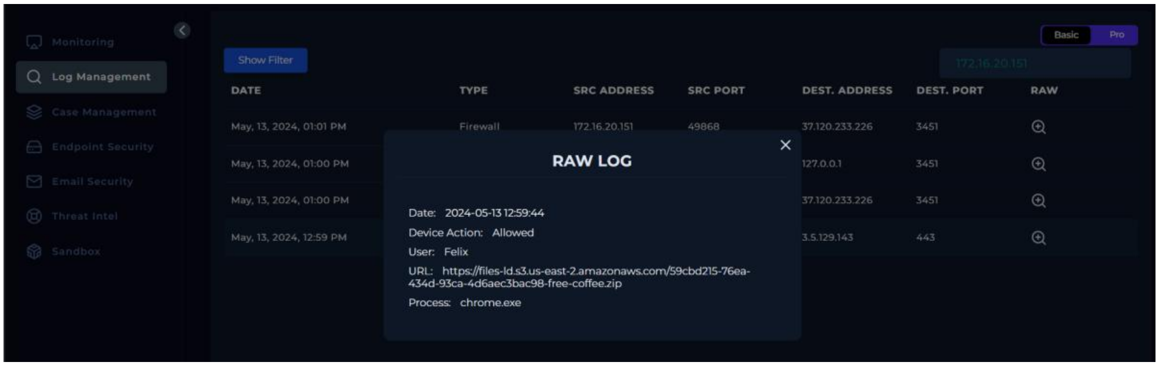


RAW LOG

Source IP: 172.16.20.151
Destination IP: 37.120.233.226
Destination Port: 3451
Protocol: TCP
Action: FW Permit
Process: Coffee.exe

Figure 19: First Alert Check.

Investigation of **Felix's IP (172.16.20.151)** in the logs confirmed the malicious file was **Opened**. The **RAW LOG** shows a process named **'Coffee.exe'** successfully connected to an external IP, proving execution on the host.



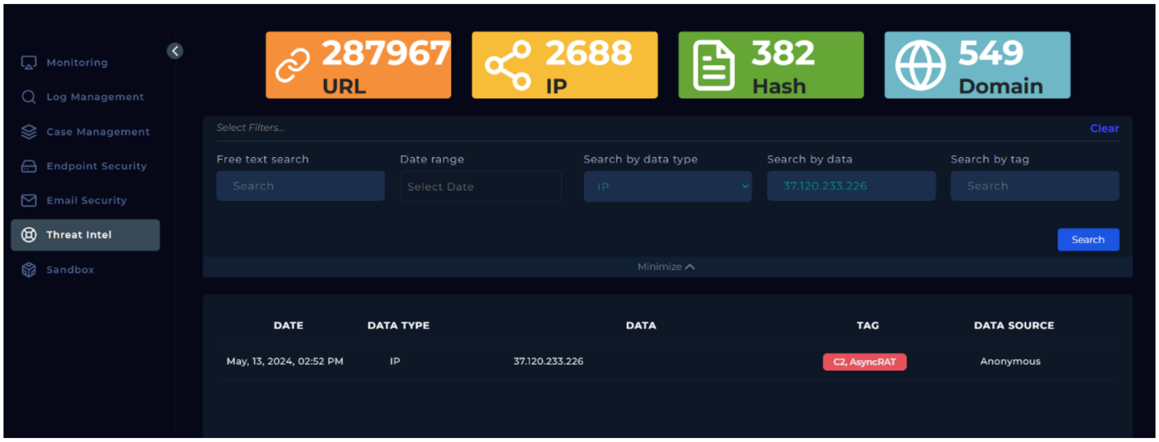
RAW LOG

Date: 2024-05-13 12:59:44
Device Action: Allowed
User: Felix
URL: https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip
Process: chrome.exe

Figure 20: Second Alert Check.

The Proxy logs confirm that the user (Felix) accessed the malicious link using 'chrome.exe', which resulted in the successful download of the 'free-coffee.zip' file.

So, to investigate the destination IP (37.120.233.226) found in the logs, I searched for it in the 'Threat Intel' section to identify any known malicious associations or C2 activity.

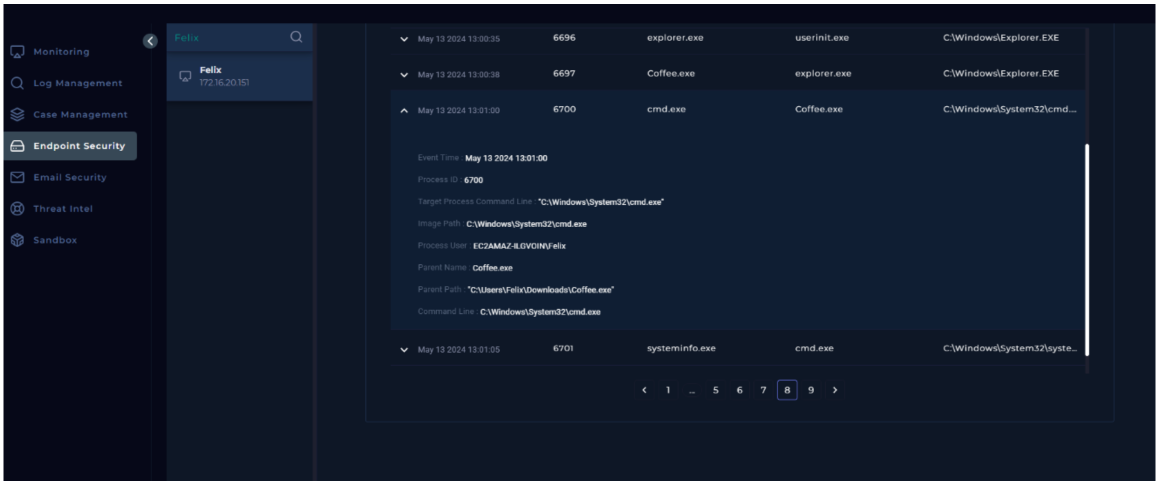


Free text search: Search
Date range: Select Date
Search by data type: IP
Search by data: 37.120.233.226
Search by tag: Search

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
May, 13, 2024, 02:52 PM	IP	37.120.233.226	C2, AsyncRAT	Anonymous

Figure 21: Threat intel result.

I searched the suspicious IP address ($37.120.233.226$) in the Threat Intel section. The results confirmed it is a known malicious address, tagged as a C2 server for AsyncRAT.



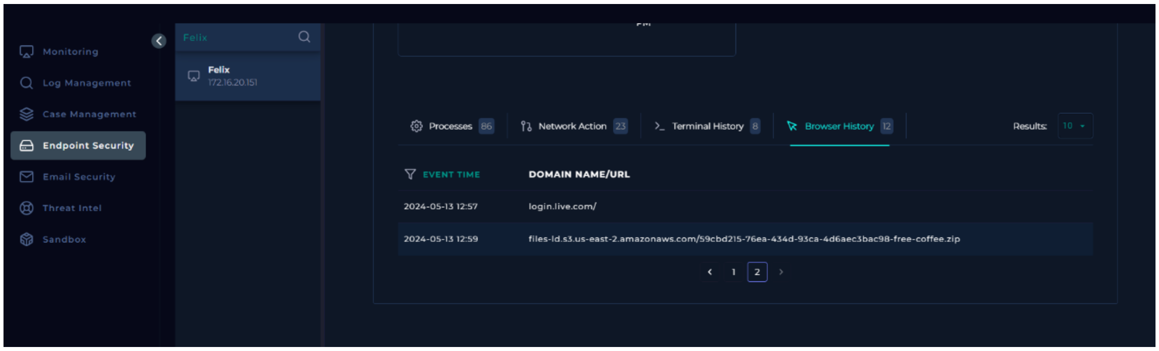
May 13 2024 13:00:35	6696	explorer.exe	userinit.exe	C:\Windows\Explorer.EXE
May 13 2024 13:00:38	6697	Coffee.exe	explorer.exe	C:\Windows\Explorer.EXE
May 13 2024 13:01:00	6700	cmd.exe	Coffee.exe	C:\Windows\System32\cmd....

Event Time : May 13 2024 13:01:00
Process ID : 6700
Target Process Command Line : "C:\Windows\System32\cmd.exe"
Image Path : C:\Windows\System32\cmd.exe
Process User : EC2AMAZ-ILGVOIN\Felix
Parent Name : Coffee.exe
Parent Path : "C:\Users\Felix\Downloads\Coffee.exe"
Command Line : C:\Windows\System32\cmd.exe

May 13 2024 13:01:05	6701	systeminfo.exe	cmd.exe	C:\Windows\System32\syste...

Figure 22: Processes.

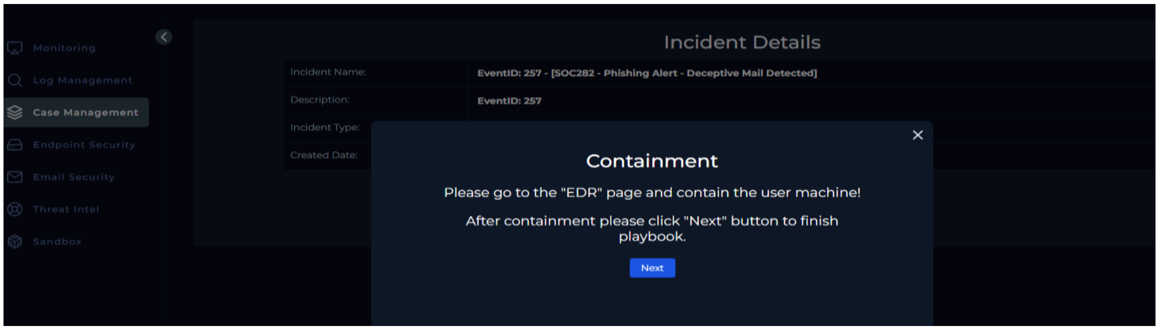
Further investigation in 'Endpoint Security' confirms that the malicious process 'Coffee.exe' (PID: 6697) was executed by Felix. This process subsequently triggered 'cmd.exe' to run system reconnaissance commands like 'systeminfo.exe', proving active post-exploitation activity on the host.



EVENT TIME	DOMAIN NAME/URL
2024-05-13 12:57	login.live.com/
2024-05-13 12:59	files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip

Figure 23: Browser History.

In 'Endpoint Security', I confirmed the malicious process 'Coffee.exe' was executed from Felix's downloads folder. Browser history also shows the user accessed the S3 bucket link at 12:59 to download the file.



Incident Details

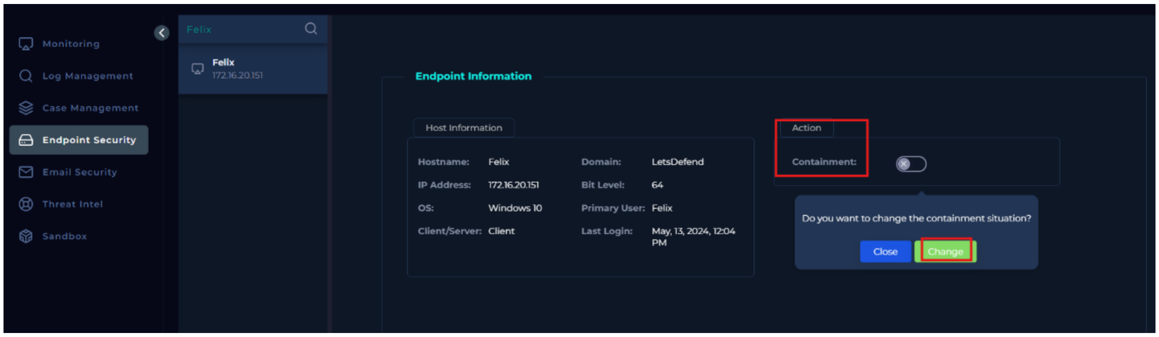
Incident Name: EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]
Description: EventID: 257
Incident Type:
Created Date:

Containment

Please go to the "EDR" page and contain the user machine!

After containment please click "Next" button to finish playbook.

Figure 24: Next Playbook Question.



Felix
172.16.20.151

Endpoint Information

Host Information

Hostname: Felix
IP Address: 172.16.20.151
OS: Windows 10
Client/Server: Client
Domain: LetsDefend
Bit Level: 64
Primary User: Felix
Last Login: May, 13, 2024, 12:04 PM

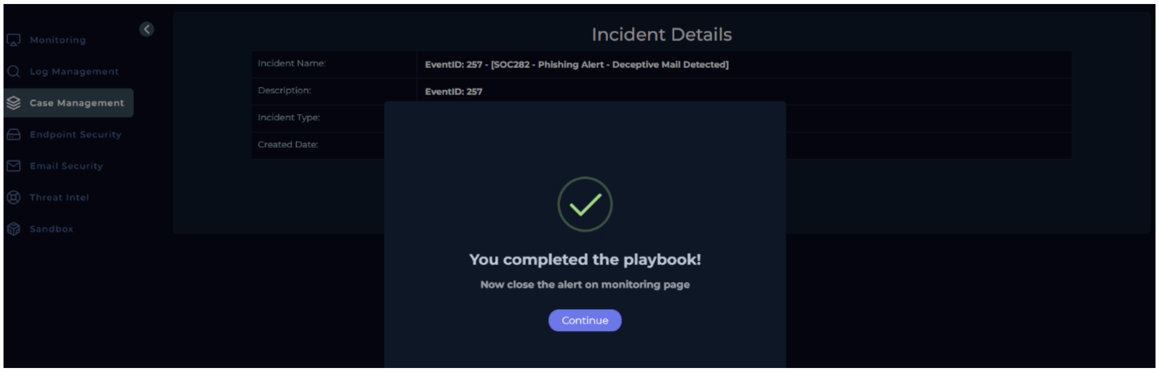
Action

Containment:

Do you want to change the containment situation?

Figure 25: Containment action.

To prevent further damage, I navigated to the 'Endpoint Security' tab and initiated the containment process for Felix's host (172.16.20.151).



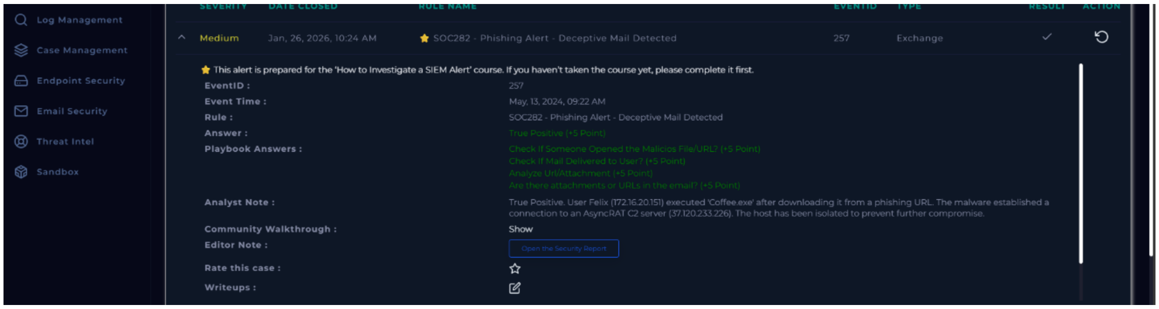
Incident Details

Incident Name: EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]
Description: EventID: 257
Incident Type:
Created Date:

You completed the playbook!

Now close the alert on monitoring page

Figure 26: completed Playbook.



SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
Medium	Jan, 26, 2026, 10:24 AM	SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	✓	

This alert is prepared for the 'How to Investigate a SIEM Alert' course. If you haven't taken the course yet, please complete it first.

EventID : 257
Event Time : May, 13, 2024, 09:22 AM
Rule : SOC282 - Phishing Alert - Deceptive Mail Detected
Answer : True Positive (+5 Point)
Playbook Answers : Check If Someone Opened the Malicios File/URL? (+5 Point)
Check If Mail Delivered to User? (+5 Point)
Analyze Url/Attachment (+5 Point)
Are there attachments or URLs in the email? (+5 Point)
Analyst Note : True Positive. User Felix (172.16.20.151) executed 'Coffee.exe' after downloading it from a phishing URL. The malware established a connection to an AsyncRAT C2 server (37.120.233.226). The host has been isolated to prevent further compromise.
Community Walkthrough : Show
Editor Note :
Rate this case : ☆
Writeups :

Figure 27: Closed Alert.

Here are the artifacts from your investigation:

- **E-mail Sender:** free@coffeeshooop.com — Sender of the malicious phishing email.
- **E-mail Domain:** coffeeshooop.com — Malicious domain used for the phishing campaign.
- **URL Address:** https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip — Malicious download link accessed by the user.
- **IP Address:** 37.120.233.226 — Malicious C2 server associated with AsyncRAT activity.
- **IP Address:** 172.16.20.151 — Compromised internal host belonging to Felix.

Summary

This lab provided a realistic simulation of a SOC Analyst's workflow, demonstrating how to effectively use a Playbook to investigate phishing attacks. It highlighted the importance of correlating email security, network logs, and endpoint activity to verify threats. By following the structured response process, I was able to successfully identify the AsyncRAT infection and take decisive action to contain the compromised host.