SOC282 - Phishing Alert - Deceptive Mail Detected

Hey, Today I will write about investigation of “**SOC282 - Phishing Alert - Deceptive Mail Detected**”

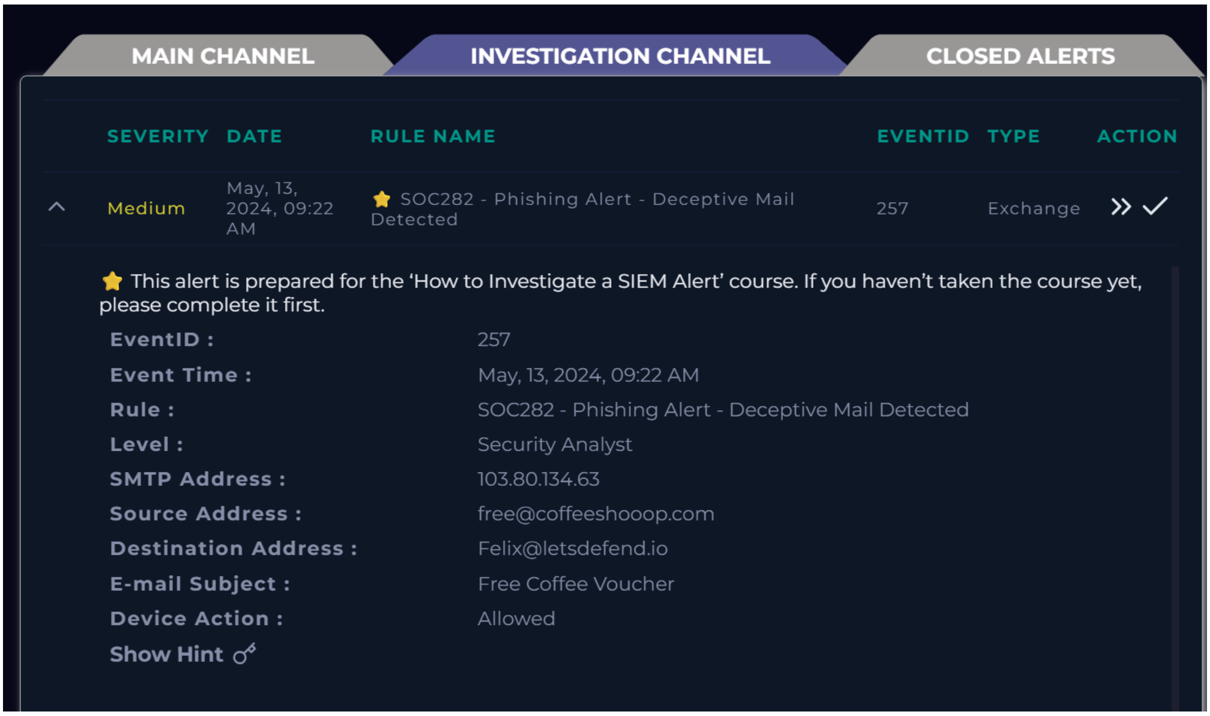
Before we begin lets understand some keywords.
Phishing: It is a type of cyberattack where someone tricks you into giving away sensitive information like passwords, OTPs, bank details, or personal data by pretending to be a trusted person or organization.

Playbook: They are crucial for a Security Operations Center for several reasons. A couple of those reasons are Consistency and Standardization. Playbooks ensure that incident responses are handled consistently across the team. By standardizing procedures, SOC analysts can respond to threats in a uniform manner, reducing the chances of errors or missed steps.

VirusTotal: It is a free tool used by analyst for scanning URLs, IP addresses, and domains for malicious content

Now let’s start investigating

This is the alert that appears in our investigation channel.



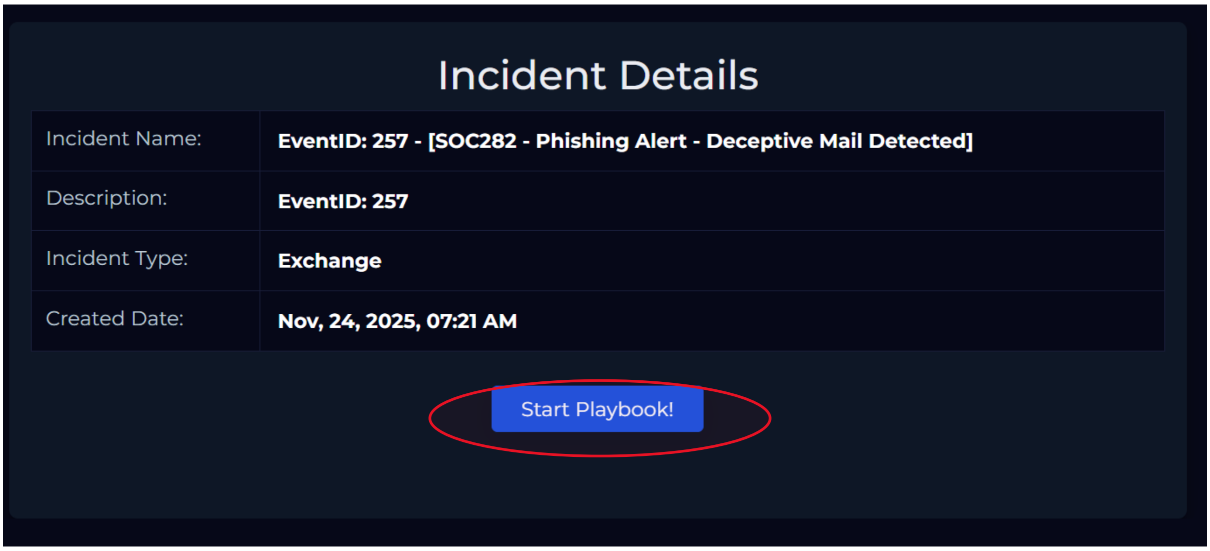
SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	May, 13, 2024, 09:22 AM	⭐ SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	» ✓

⭐ 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

Let’s start with the playbook

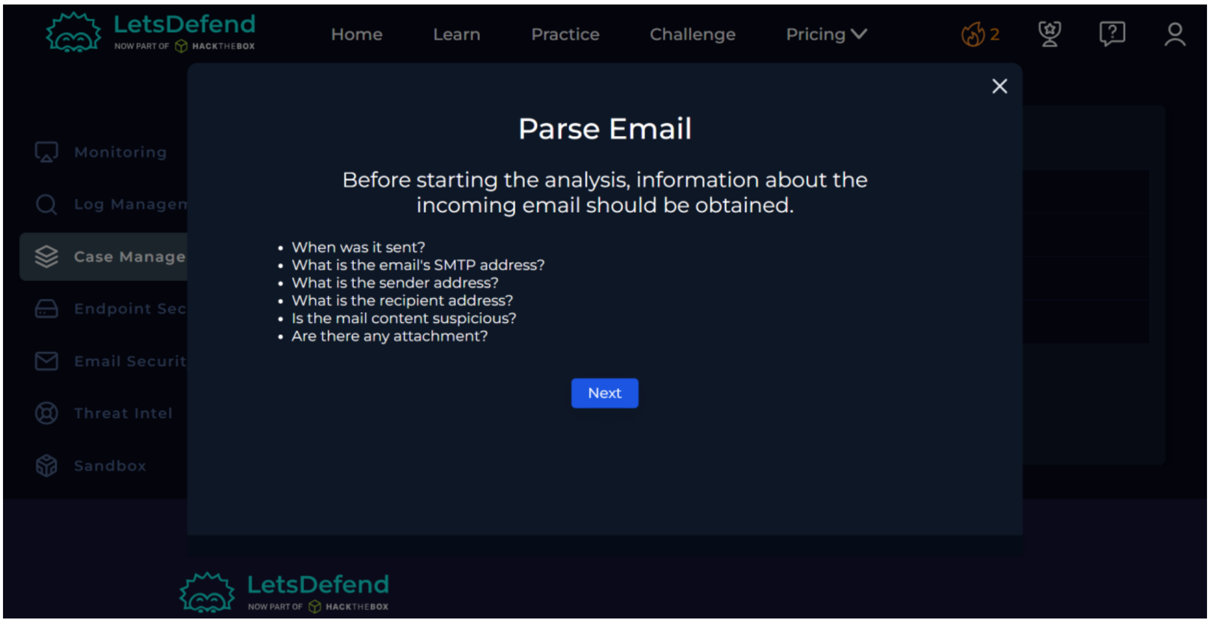


Incident Details

Incident Name:	EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]
Description:	EventID: 257
Incident Type:	Exchange
Created Date:	Nov, 24, 2025, 07:21 AM

Click on >> Start Playbook button

The first step of the playbook is asking us to obtain the information about the alert

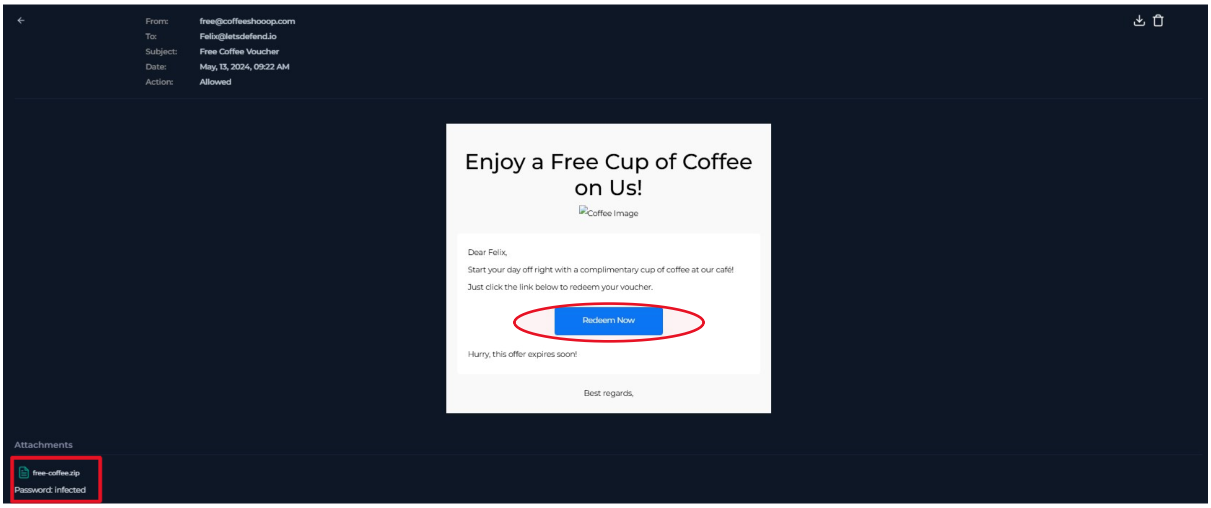


Parse Email

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?

- When was it sent?
  May, 13, 2024, 09:22 AM
- What is the email's SMTP address?
  103.80.134.63
- What is the sender address?
  free@coffeeshooop.com
- What is the recipient address?
  Felix@letsdefend.io
- Is the mail content suspicious?
  Yes, the mail contains suspicious content. The attacker is trying to trick the user by sending free vouchers!



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.

Redeem Now

Hurry, this offer expires soon!

Best regards,

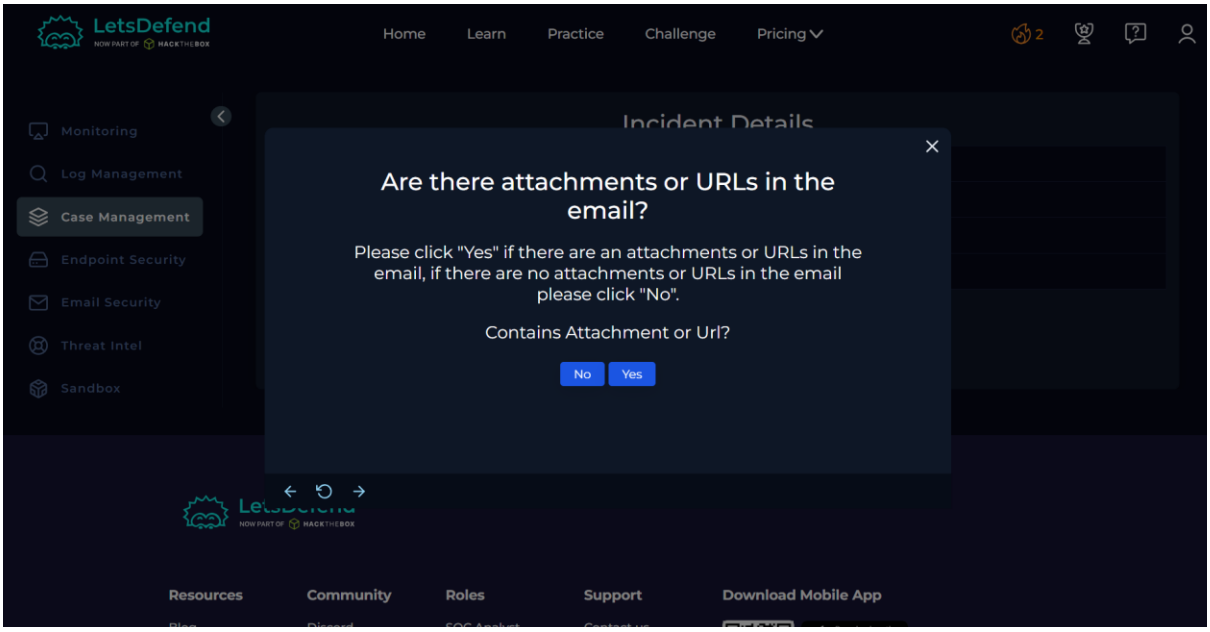
Attachments

free-coffee.zip
Password: infected

- Are there any attachment?

  Yes, there is an attachment with file name **free-coffee.zip**

The playbook's next phase is to look for attachments



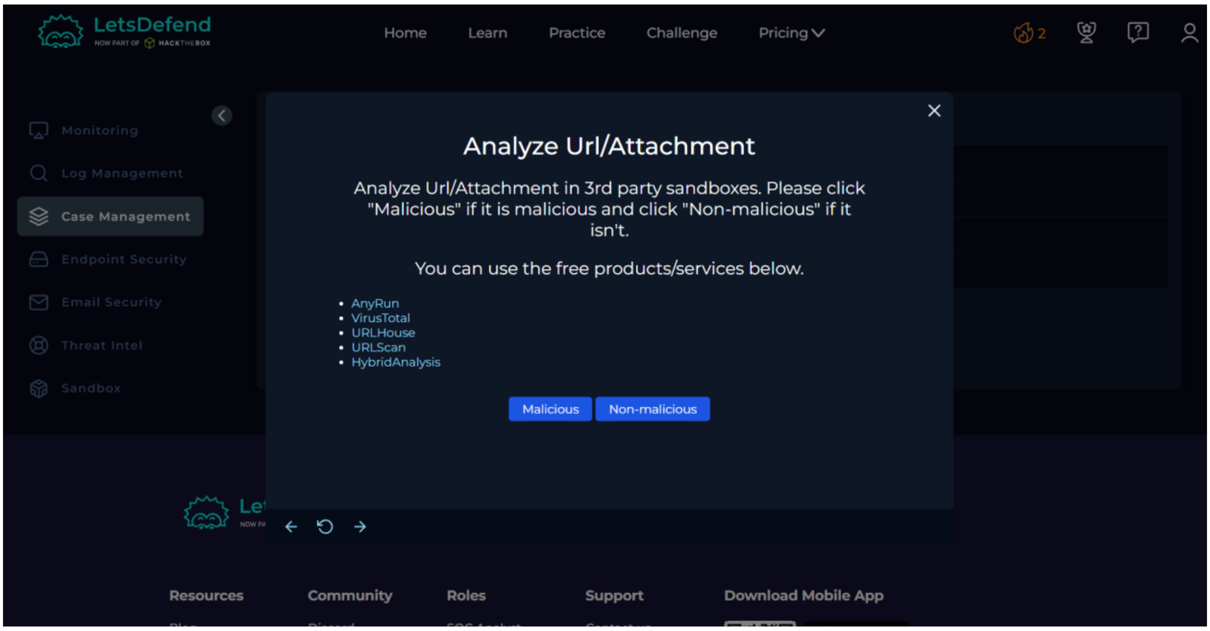
Are there attachments or URLs in the email?

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?

No Yes

Click on >> Yes, because we found both attachment and URL in the email



Analyze Url/Attachment

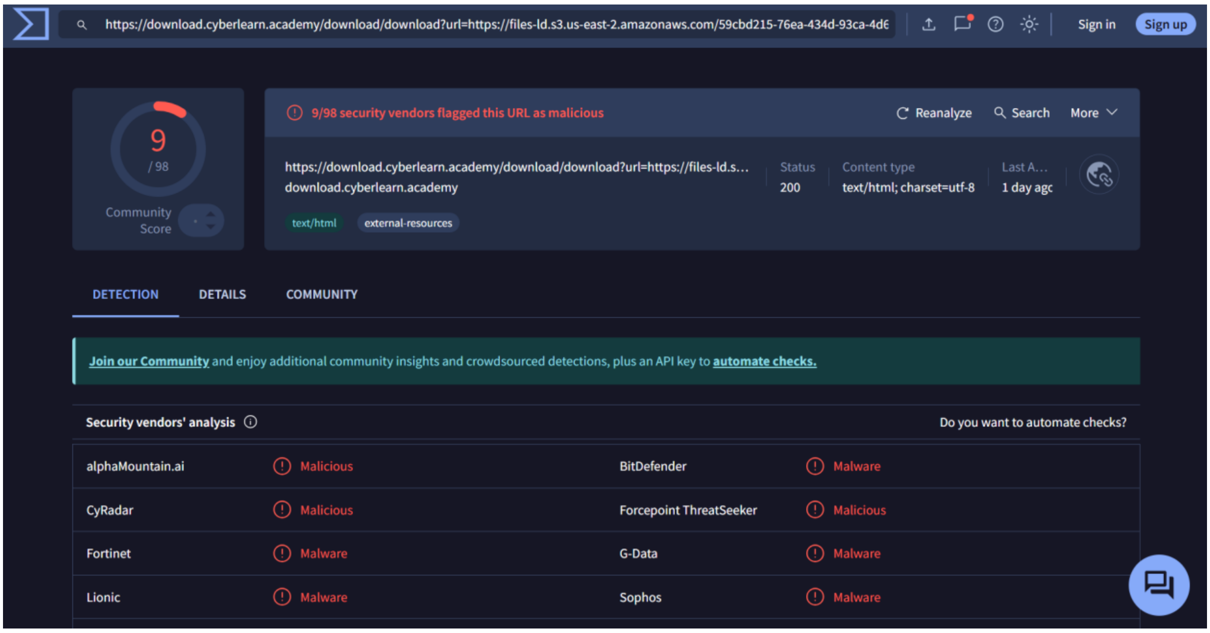
Analyze Url/Attachment in 3rd party sandboxes. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

Malicious Non-malicious

Let us analyze the attached URL on VirusTotal


https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6
Sign in
Sign up
9
/ 98
Community Score
Reanalyze
Search
More
DETECTION
DETAILS
COMMUNITY
text/html
external-resources

9/98 security vendors flagged this URL as malicious

https://download.cyberlearn.academy/download/download?url=https://files-ld.s...
download.cyberlearn.academy

Status 200

Content type text/html; charset=utf-8

Last A... 1 day agc

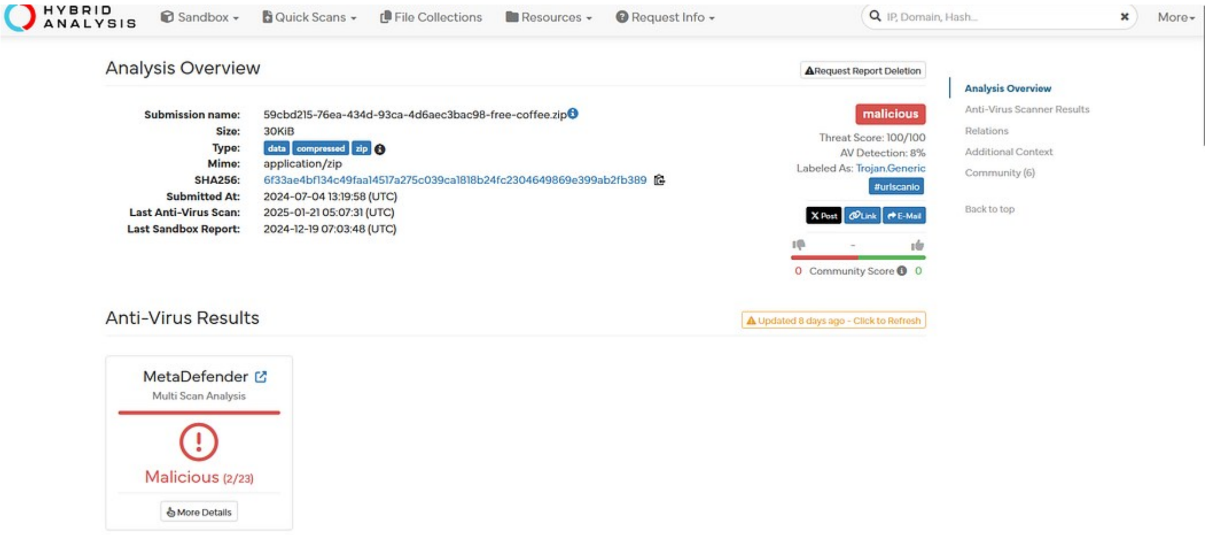
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

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

The URL is flagged as malicious!



Analysis Overview

Submission name:	59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip
Size:	30KiB
Type:	data compressed zip
Mime:	application/zip
SHA256:	6f33ae4bf134c49faa14517a275c039ca1818b24fc2304649869e399ab2fb389
Submitted At:	2024-07-04 13:19:58 (UTC)
Last Anti-Virus Scan:	2025-01-21 05:07:31 (UTC)
Last Sandbox Report:	2024-12-19 07:03:48 (UTC)

malicious

Threat Score: 100/100
AV Detection: 8%
Labeled As: Trojan.Generic
#urlscanio

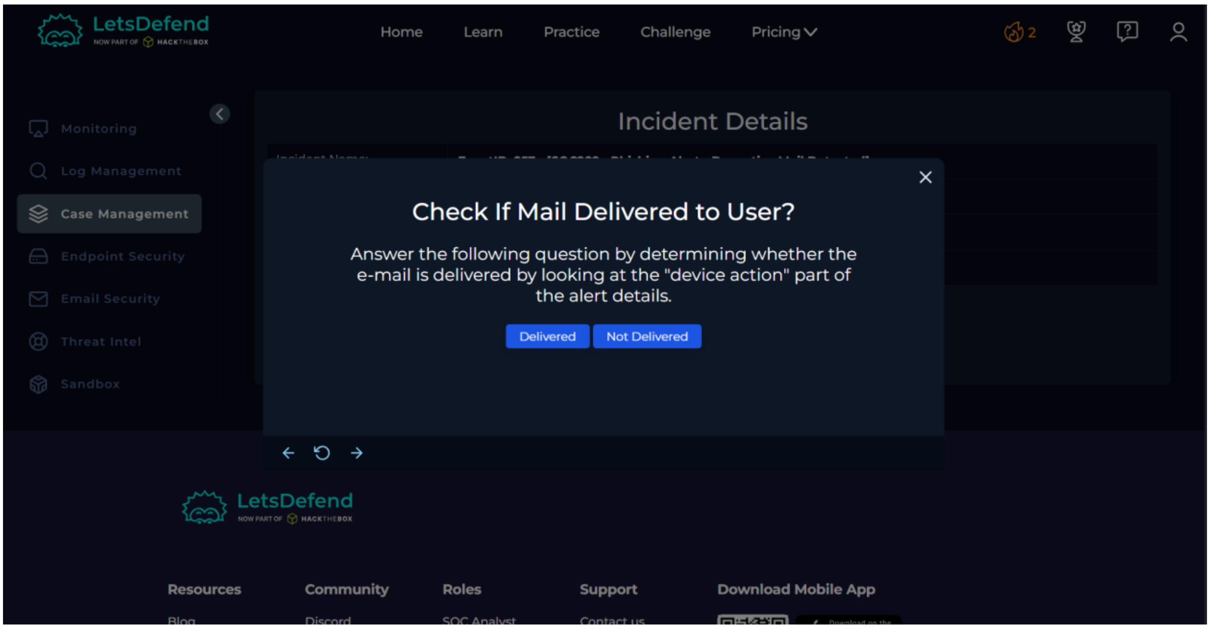
0 Community Score 0

Anti-Virus Results

Updated 8 days ago - Click to Refresh

MetaDefender
Multi Scan Analysis
Malicious (2/23)

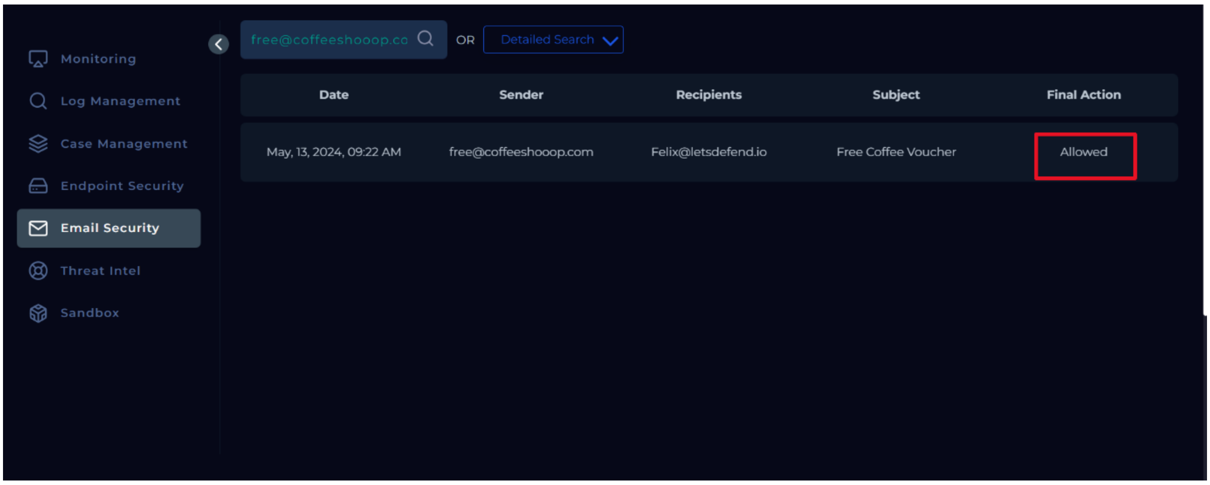
Click on >> Malicious



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.

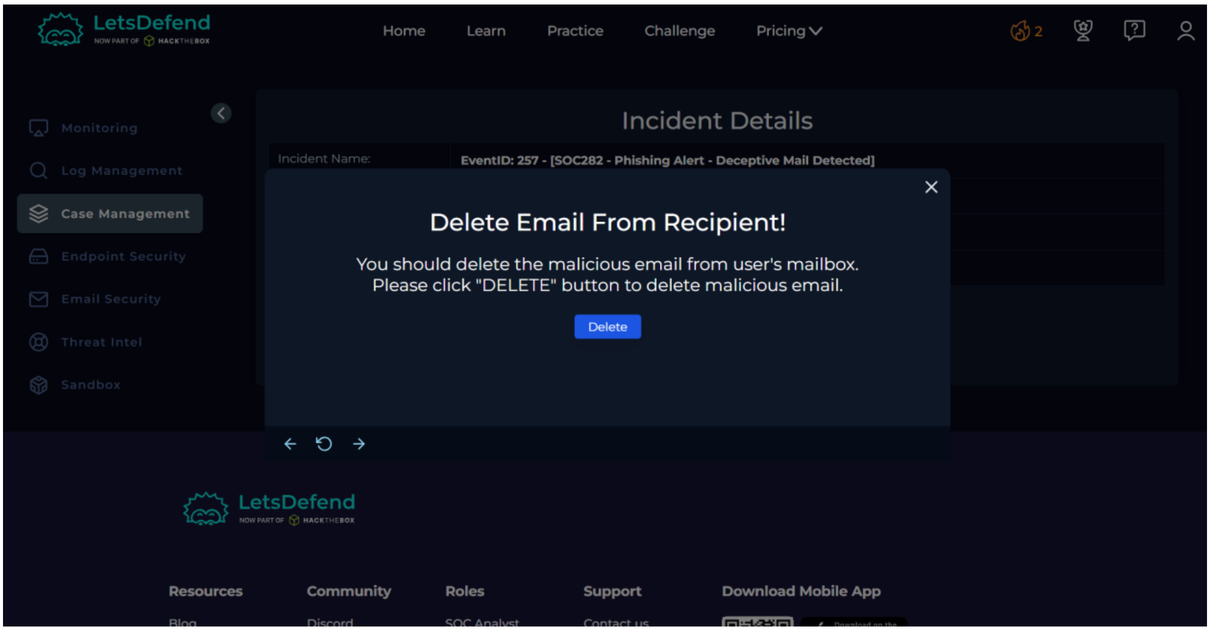
Let us go to Email Security page and find this out



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

As we can see the final action is displayed as **Allowed** that means the message was delivered to the user.

Click on >> Delivered



Incident Details

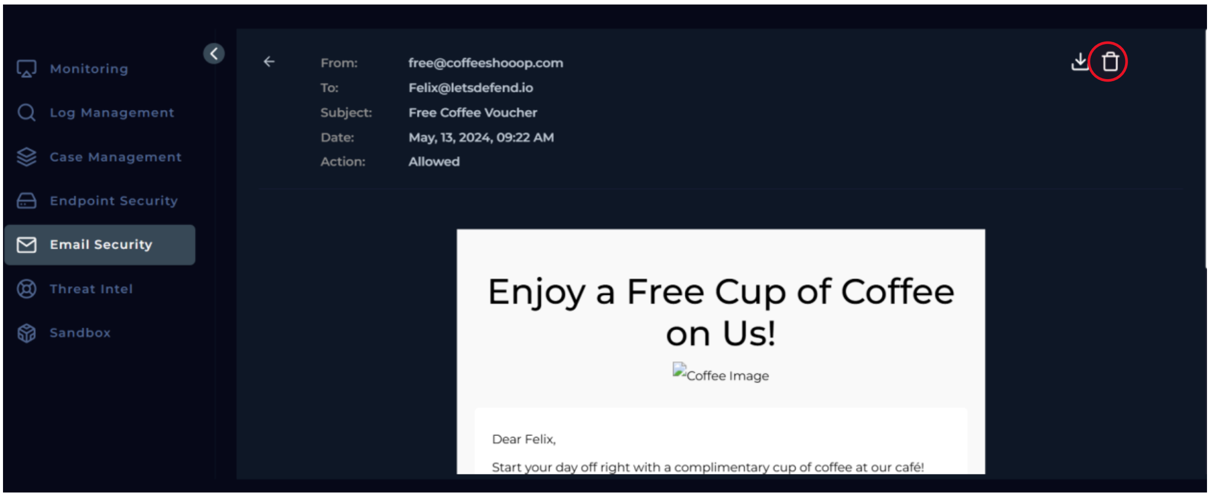
Incident Name: EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]

Delete Email From Recipient!

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

Delete

For this go to Email Security Page and delete the mail



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

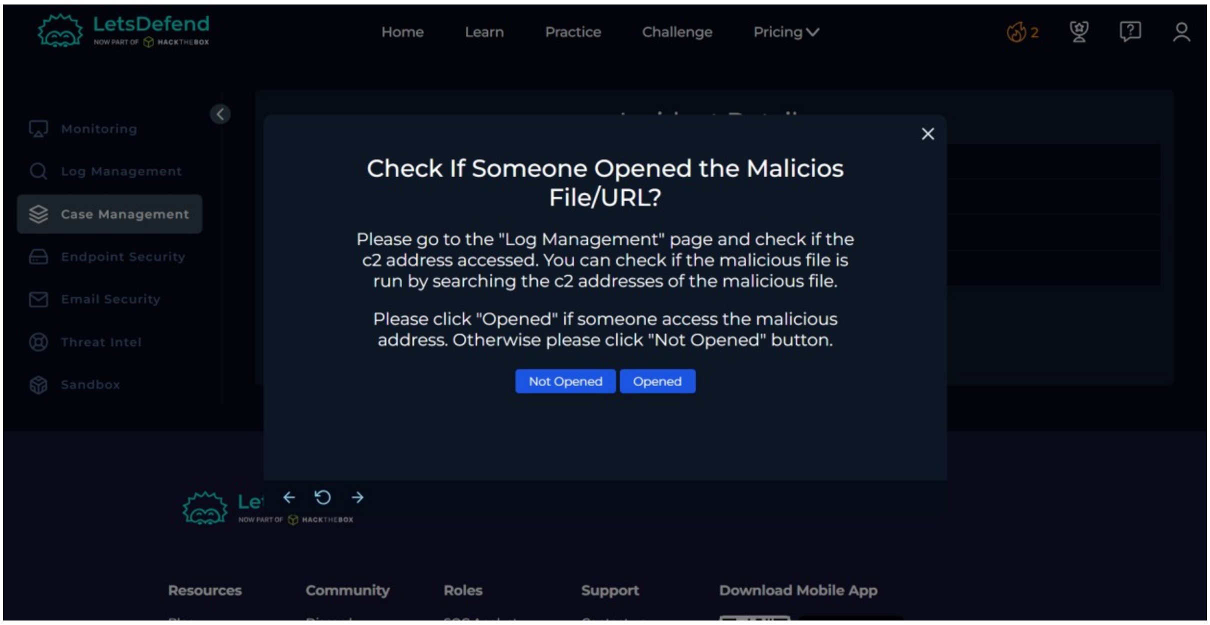
Enjoy a Free Cup of Coffee on Us!

Coffee Image

Dear Felix,

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

Click on >> Delete



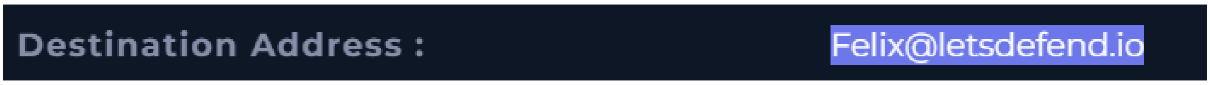
Check If Someone Opened the Malicios File/URL?

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.

Not Opened | Opened

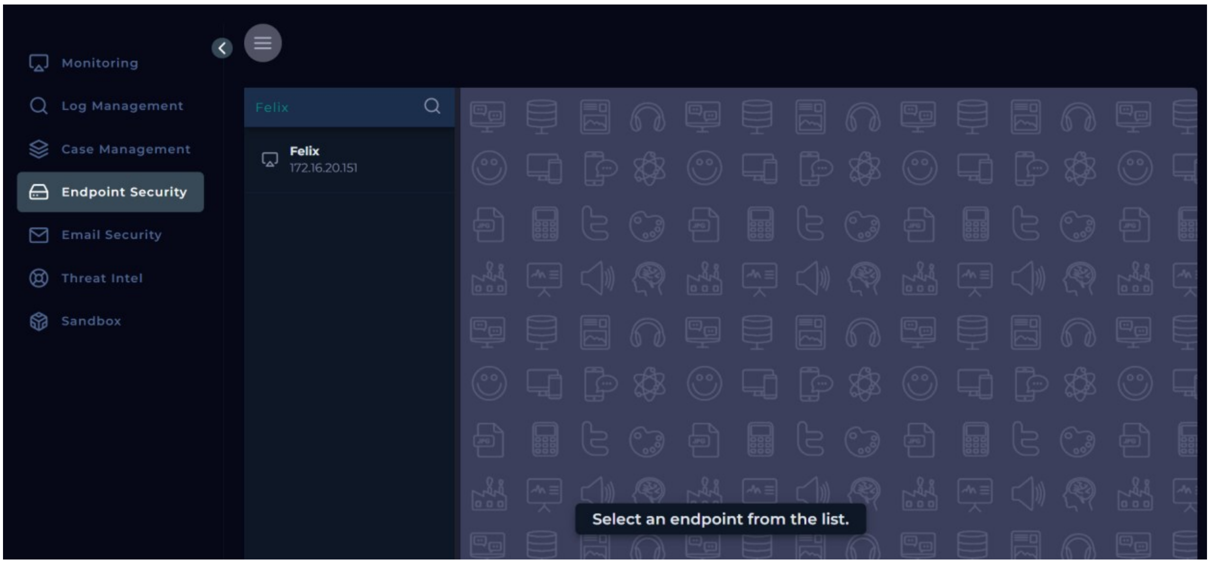
To find this we need to go to Endpoint Security Page, as we know the users email address we can find out his name



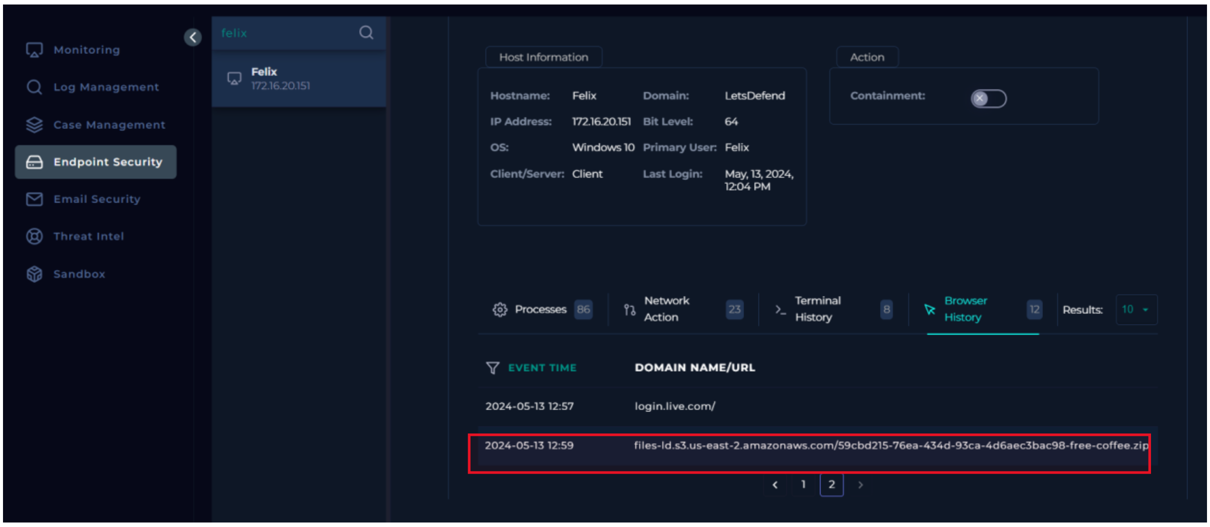
Destination Address : Felix@letsdefend.io

So the name of the user is **Felix.**

Search the same of the EDR page



Click on >> Felix



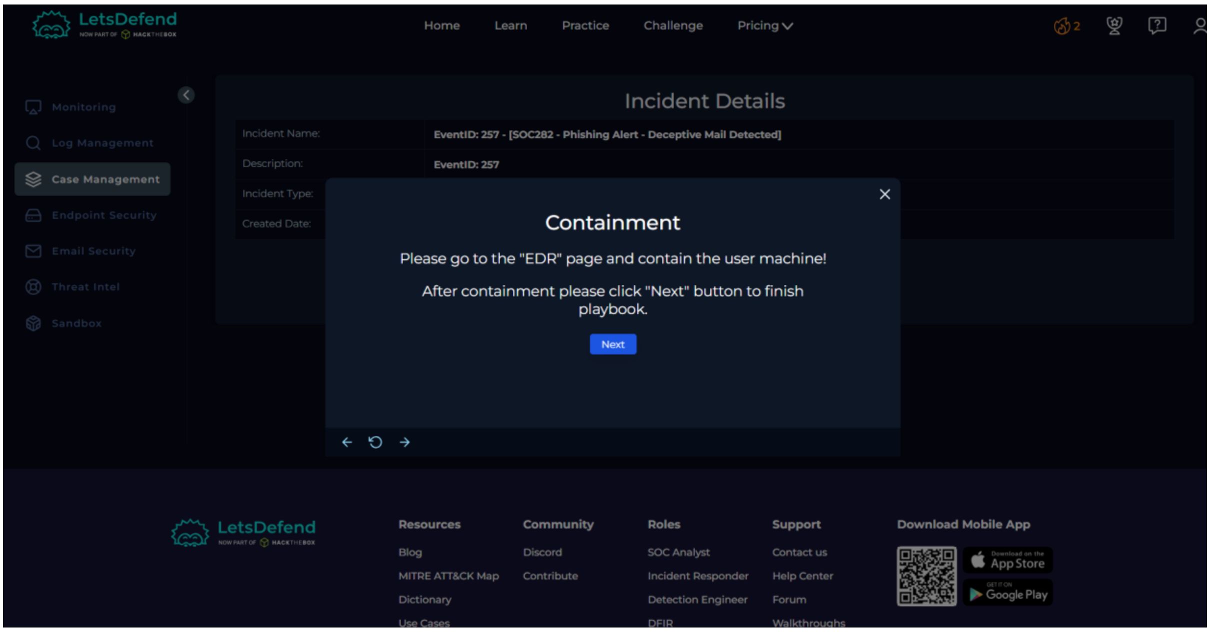
Hostname: Felix | Domain: LetsDefend
IP Address: 172.16.20.151 | Bit Level: 64
OS: Windows 10 | Primary User: Felix
Client/Server: Client | Last Login: May, 13, 2024, 12:04 PM

Containment:

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

As we can see that the user has opened the malicious URL

Click on >> Opened



Incident Details

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

Description: EventID: 257

Incident Type:

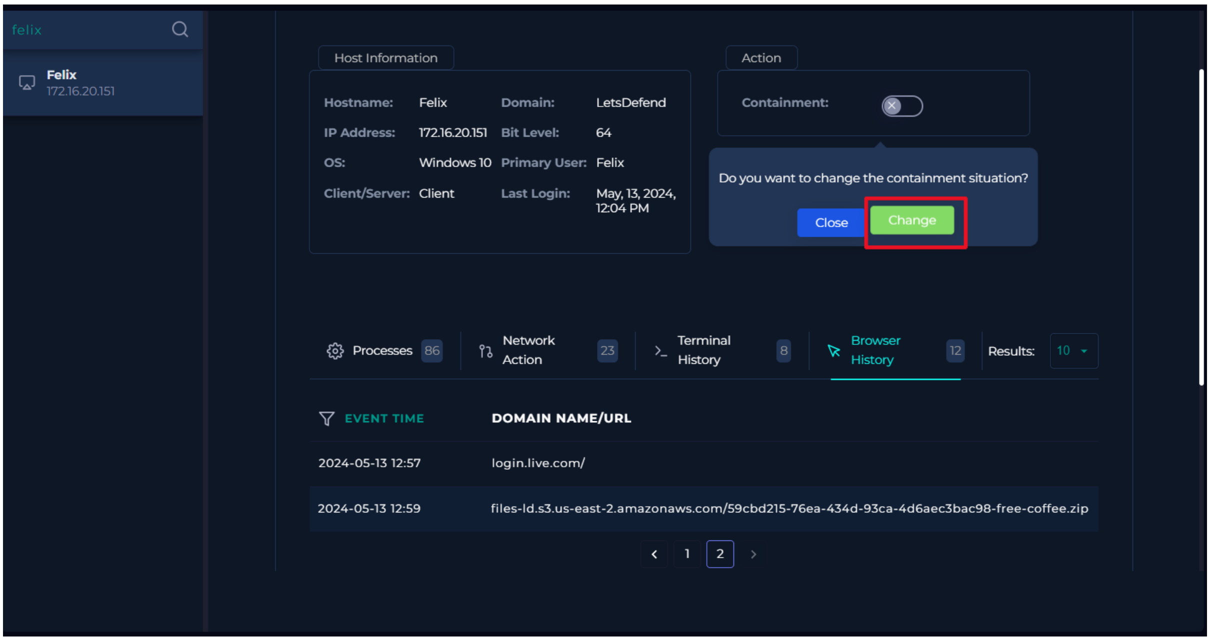
Created Date:

Containment

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

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

We need to make sure that this infected machine does not infect other systems connected to the same network. So, Isolate the infected machine



Hostname: Felix Domain: LetsDefend

IP Address: 172.16.20.151 Bit Level: 64

OS: Windows 10 Primary User: Felix

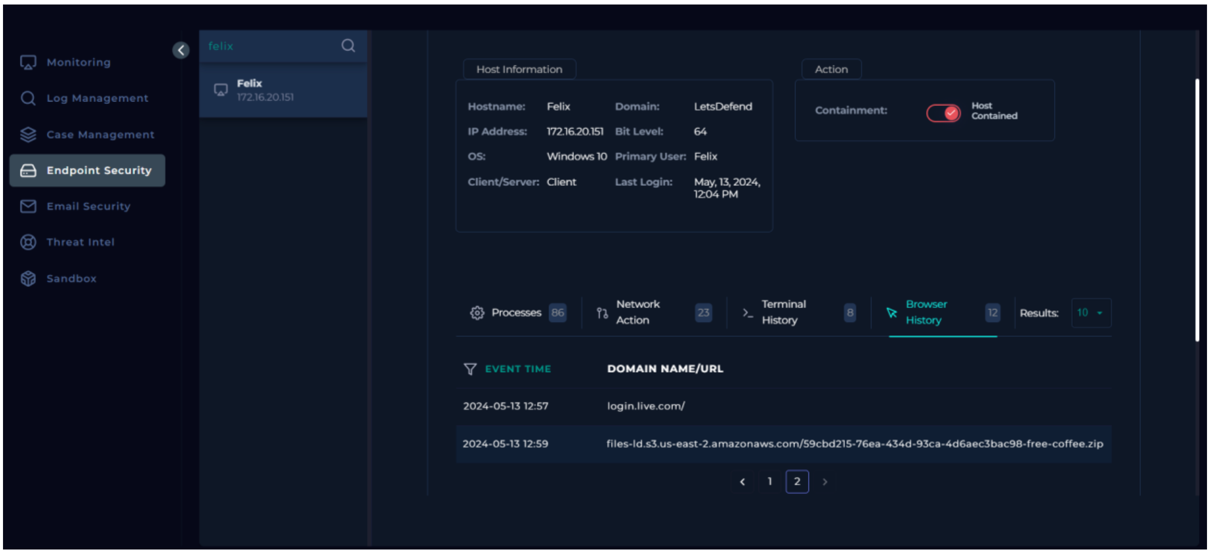
Client/Server: Client Last Login: May, 13, 2024, 12:04 PM

Containment:

Do you want to change the containment situation?

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

Click on >> Change



Hostname: Felix Domain: LetsDefend

IP Address: 172.16.20.151 Bit Level: 64

OS: Windows 10 Primary User: Felix

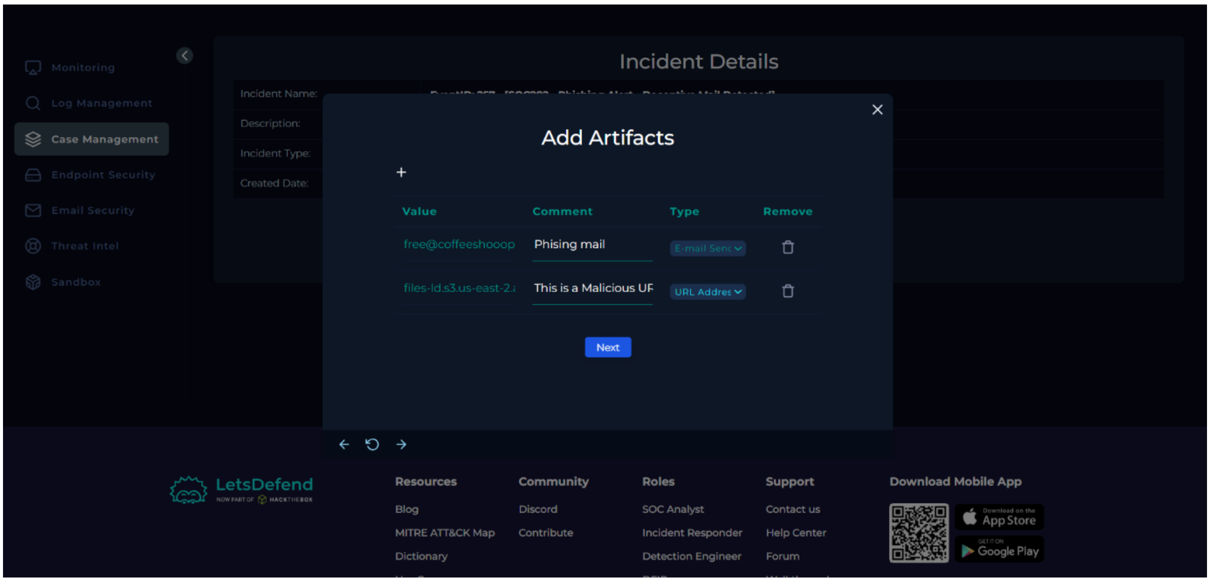
Client/Server: Client Last Login: May, 13, 2024, 12:04 PM

Containment: Host Contained

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

The Host is now contained

Click on >> Next



Add Artifacts

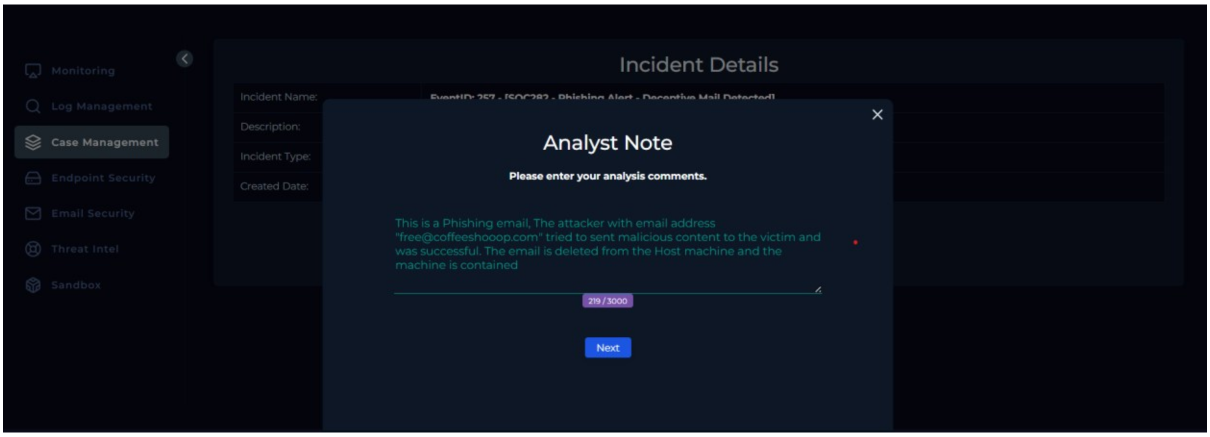
+

Value	Comment	Type	Remove
free@coffeeshooop	Phising mail	E-mail Senc	🗑
files-ld.s3.us-east-2.a	This is a Malicious UF	URL Addres	🗑

Next

Add Artifacts

Click on >> Next



Analyst Note

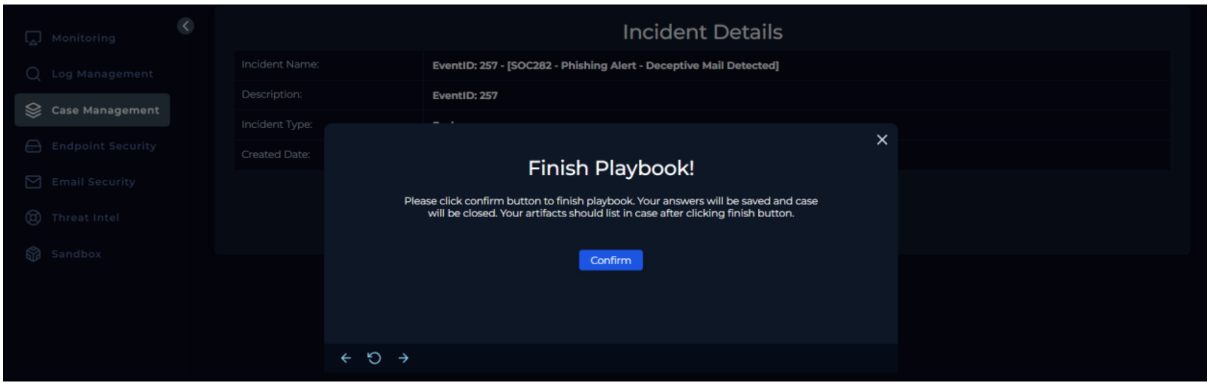
Please enter your analysis comments.

This is a Phishing email, The attacker with email address "free@coffeeshooop.com" tried to sent malicious content to the victim and was successful. The email is deleted from the Host machine and the machine is contained

219 / 3000

Next

Click On >> Next



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

Description: EventID: 257

Incident Type:

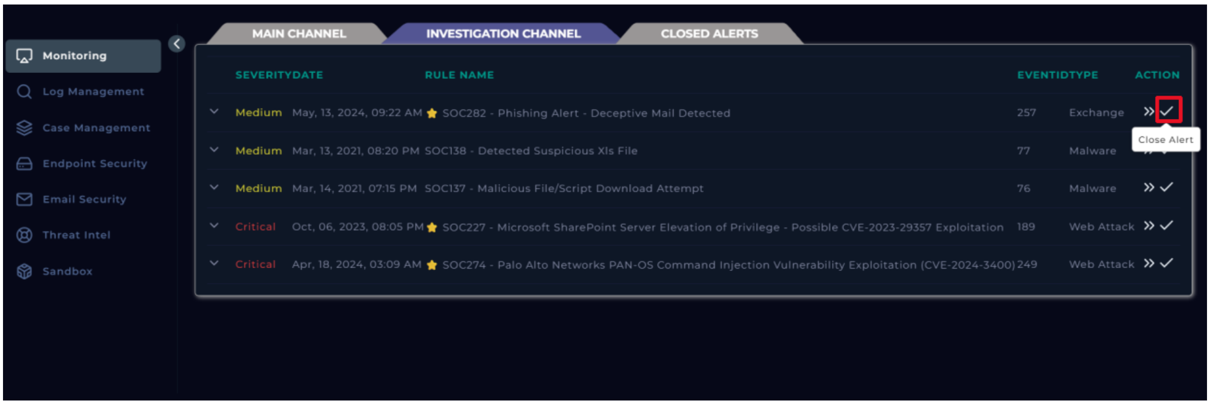
Created Date:

Finish Playbook!

Please click confirm button to finish playbook. Your answers will be saved and case will be closed. Your artifacts should list in case after clicking finish button.

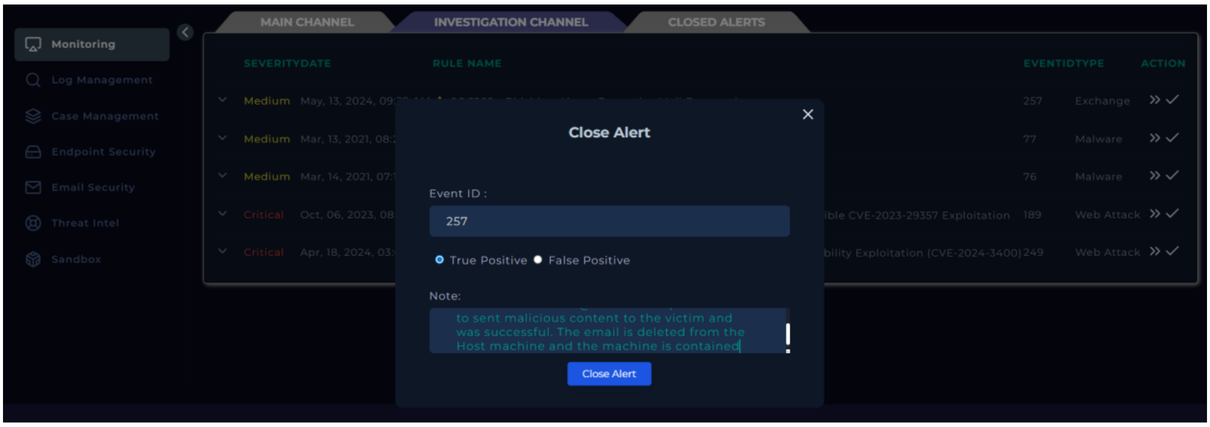
Confirm

Click on >> Confirm



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	May, 13, 2024, 09:22 AM	SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	» ✓
Medium	Mar, 13, 2021, 08:20 PM	SOC138 - Detected Suspicious Xls File	77	Malware	» ✓
Medium	Mar, 14, 2021, 07:15 PM	SOC137 - Malicious File/Script Download Attempt	76	Malware	» ✓
Critical	Oct, 06, 2023, 08:05 PM	SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation	189	Web Attack	» ✓
Critical	Apr, 18, 2024, 03:09 AM	SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)	249	Web Attack	» ✓

Click on >> Close Alert



Close Alert

Event ID : 257

● True Positive ○ False Positive

Note:
to sent malicious content to the victim and
was successful. The email is deleted from the
Host machine and the machine is contained

Click on >> Closed Alert

Lessons Learned

- Email security filters aren't foolproof: This email bypassed initial security measures, highlighting the need for multiple layers of defense.
- User awareness is critical: Even with technical controls, users remain the last line of defense. Security awareness training could have prevented Felix from opening the malicious URL.
- Quick response matters: Rapid identification and containment prevented the potential compromise from spreading across the network.
- Documentation is essential: Proper artifact collection enables future analysis and helps identify patterns in attacker behavior.

Conclusion

This investigation demonstrates a typical phishing attack lifecycle: from initial delivery to user interaction and finally containment. The quick response prevented a potentially serious security incident from escalating. As SOC analysts, our role is not just to respond to threats but to continuously learn from each incident to strengthen our organization's security posture.