Contact Person

Full name
Ahmed Emad Nasr

Job title / role
Incident Response Analyst

Department / team
Security Operations Center (SOC)

Email address
Ahmed.em.nasr@gmail.com

Phone number
+201018166445

The Incident

Date and time discovered:
May, 13, 2024, 09:22 AM.

How was the incident detected? (E.g., user report, monitoring system alert)

A Medium severity alert was triggered in the Monitoring system under the rule "SOC282 - Phishing Alert - Deceptive Mail Detected".

Detailed description of the incident (include what occurred, where, and how):

- A phishing email was received by the internal user Felix@letsdefend.io from the external address free@coffeeshooop.com with the subject "Free Coffee Voucher".
- The sender's domain (coffeeshooop.com) uses typosquatting to appear legitimate.
- The action taken by the email security gateway was "Allowed".
- The email contained an attachment named free-coffee.zip along with the password infected written in the email body to bypass automated scanning.
- The source IP address of the email (103.80.134.63) is flagged in the Threat Intelligence feed for phishing activities.
- Endpoint browser history for the user Felix (IP: 172.16.20.151) shows that on May 13, 2024, at 12:59 PM, the user accessed an AWS S3 URL containing the file free-coffee.zip.
- Shortly after, starting at 13:01:00, terminal history on Felix's machine logs the execution of cmd.exe followed by multiple system enumeration commands, including systeminfo, wmic logicaldisk get caption,description,providername, tasklist /svc, ipconfig /all, and route print.

Was the incident ongoing at the time of report?

☐ Yes ☒ No

Have any files, accounts, or systems been compromised?

☒ Yes ☐ No

If yes, please describe:

The workstation assigned to Felix (172.16.20.151) is confirmed compromised. The sequence of enumeration commands executed in the terminal immediately following the download of the suspicious zip file indicates successful execution of a malicious payload.

Notification

Was your supervisor or manager notified?

☐ Yes ☒ No

Date/time of notification:
April 6, 2026

Was the IT/security team alerted?

☒ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)
Escalated to the Incident Response team via Case Management for immediate host containment.

Containment Measures

What immediate actions were taken to contain the threat? (E.g., system shutdown, network isolation)

- Isolate Felix's workstation (172.16.20.151) from the network to prevent further internal reconnaissance or lateral movement.
- Delete the malicious email from Felix's inbox and search the enterprise exchange environment for other recipients of emails from coffeeshooop.com.

Were any user accounts disabled, firewalls updated, or services suspended?

☒ Yes ☐ No

If yes, provide details:

- Block the sender's domain (coffeeshooop.com) and the source IP (103.80.134.63) on the email gateway and perimeter firewalls.
- Suspend Felix's Active Directory account and initiate a mandatory password reset.

Impacted Services Measures

List any systems, devices, or applications affected by the incident:

- Workstation Hostname: Felix (IP: 172.16.20.151).
- Email Account: Felix@letsdefend.io.

Estimated number of affected users, if applicable:

1 user (Felix).

Was there any known data loss or exposure?

☐ Yes ☒ No

If yes, describe the type of data (e.g., personal info, credentials, financial):

Preliminary Analysis *(Optional)*

Suspected cause or entry point (e.g., phishing email, unpatched software):

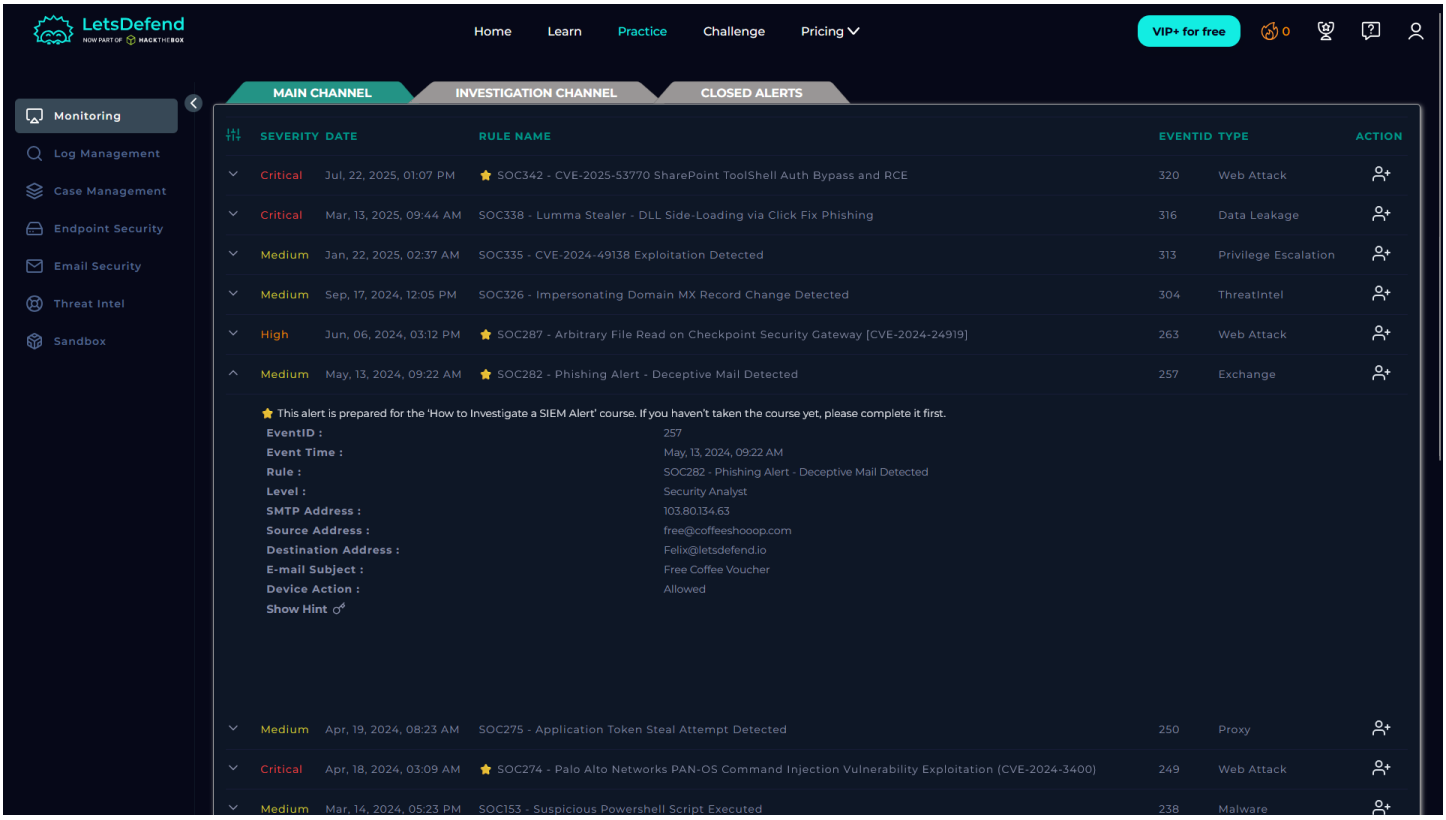
- **Suspected cause or entry point (e.g., phishing email, unpatched software):**
  - A successful phishing attack utilizing a typosquatted domain and a password-protected zip file attachment (free-coffee.zip) containing a malicious payload that was executed by the user, leading to automated system enumeration.
-

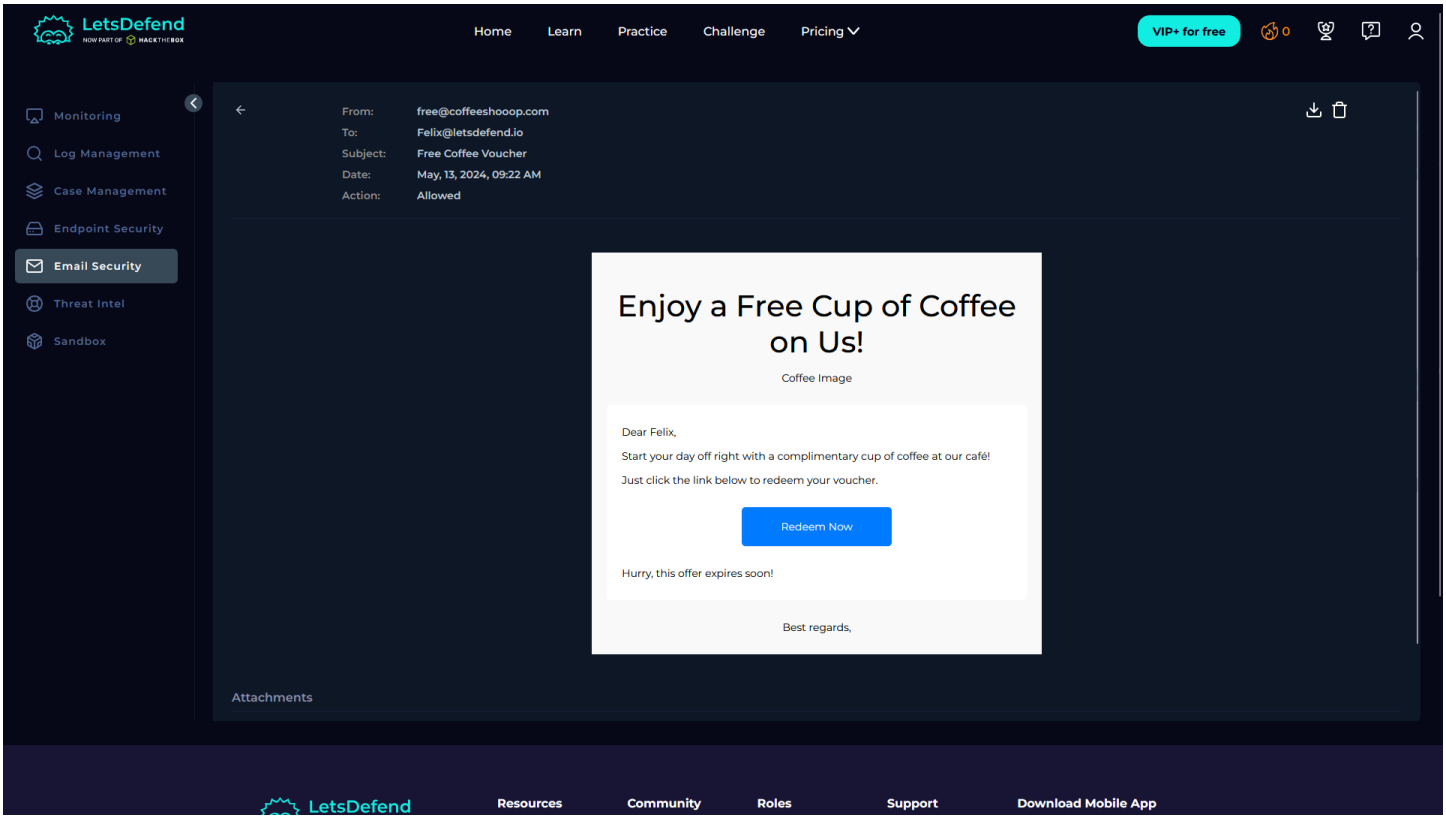
Was the threat internal, external, or unknown?

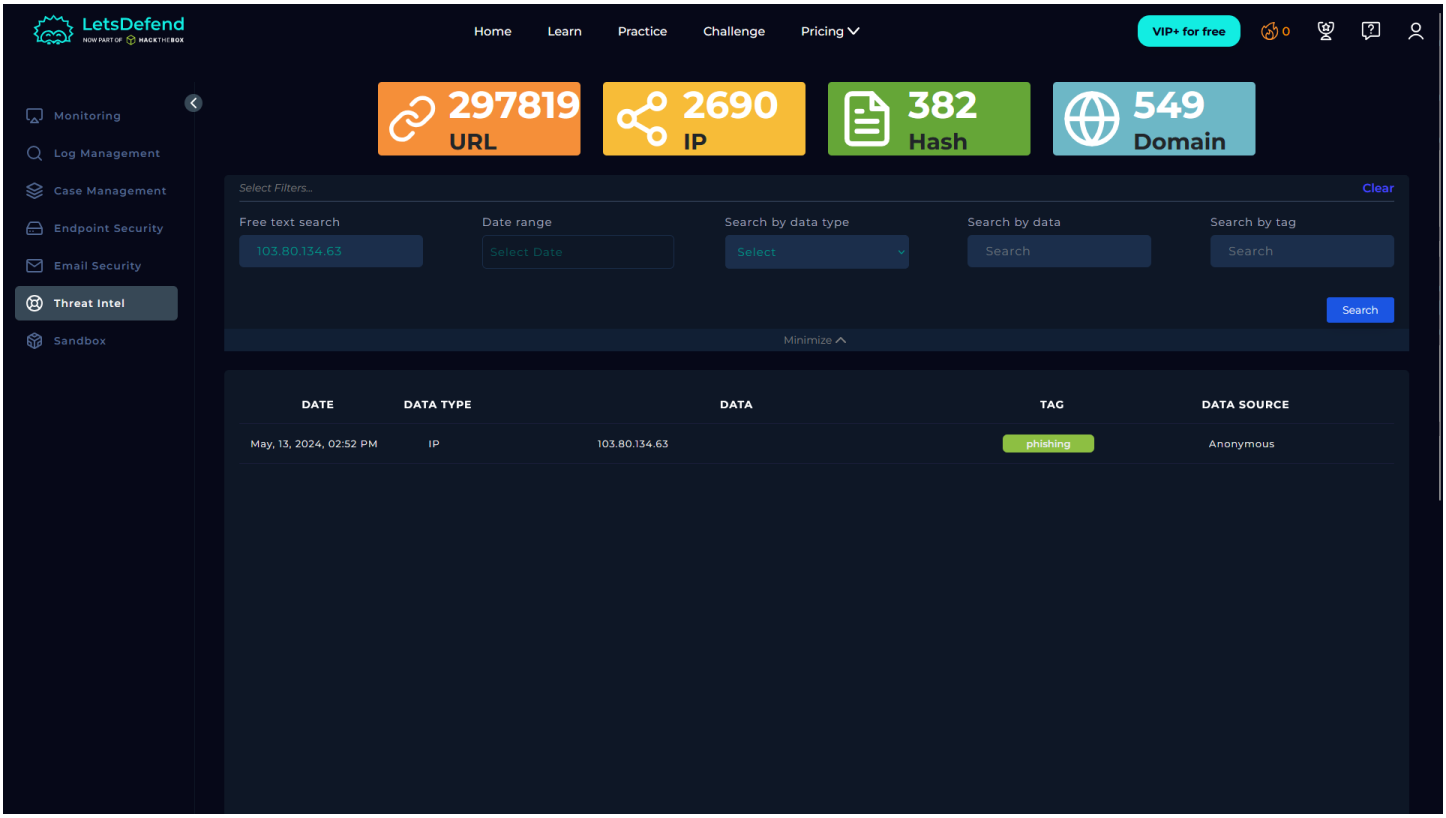
☐ Internal ☒ External ☐ Unknown

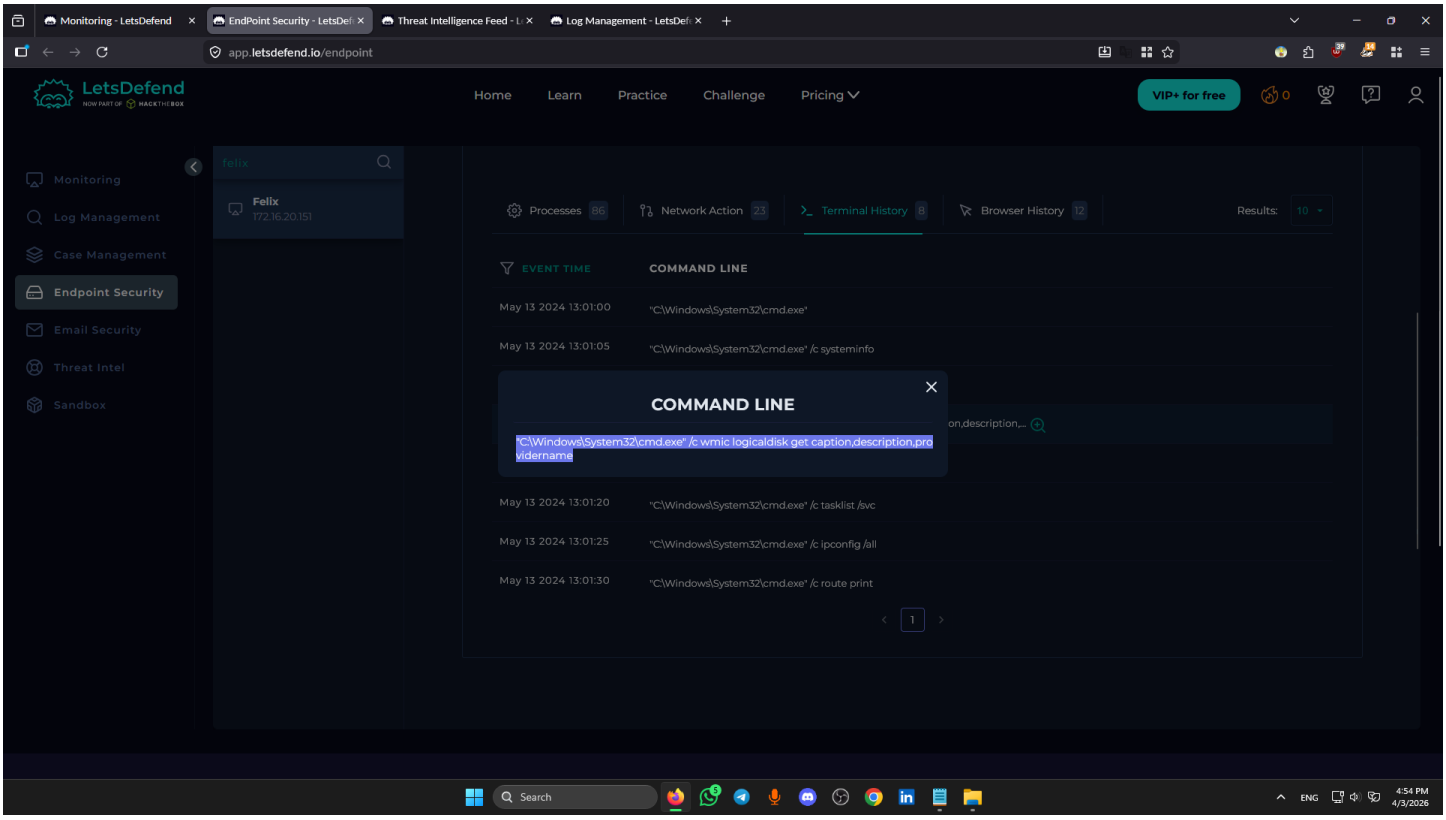
Submitted by:

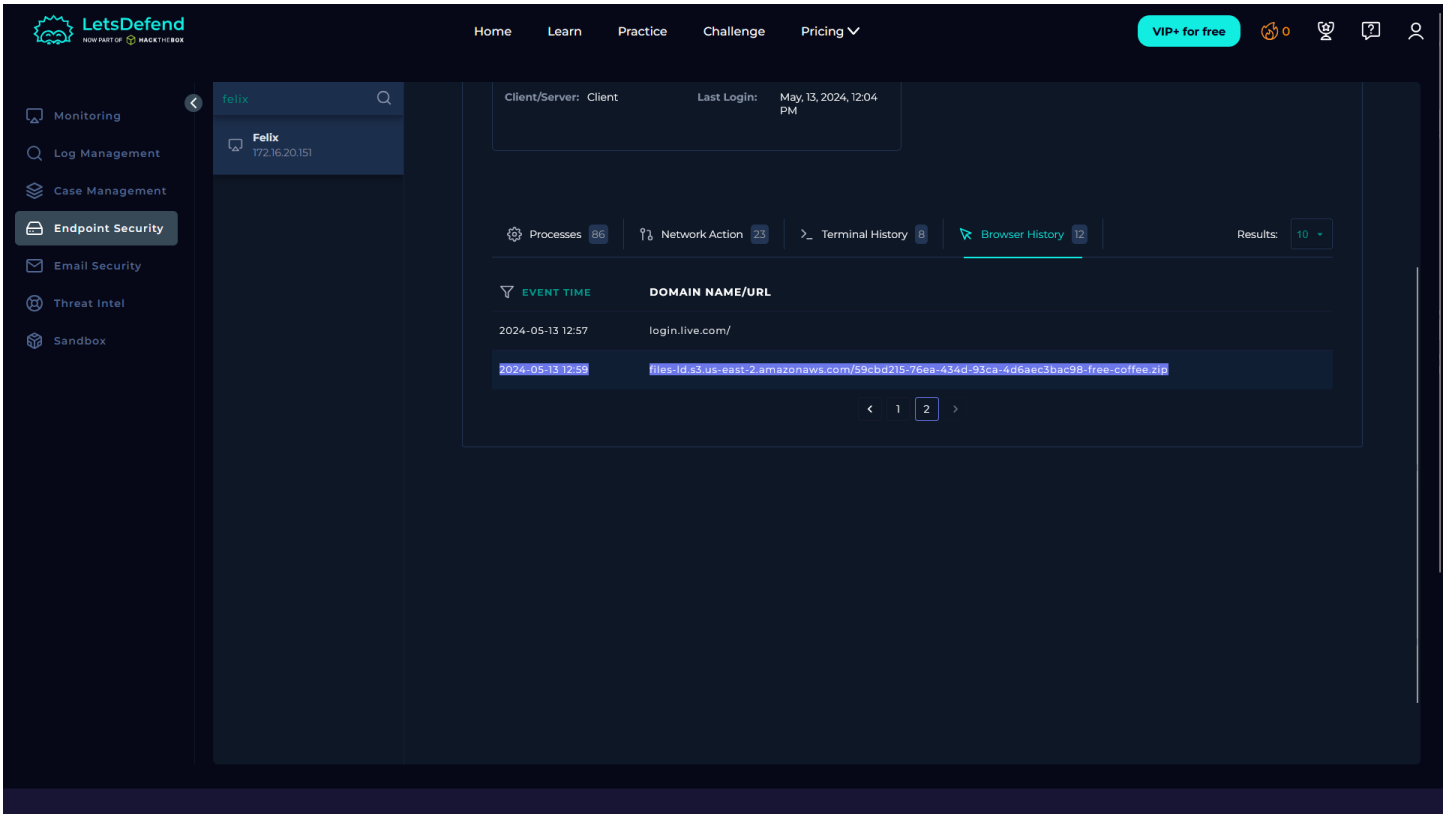
Ahmed Emad Nasr	Ahmed Emad Nasr	
Name	**Signature**	**Date submitted**

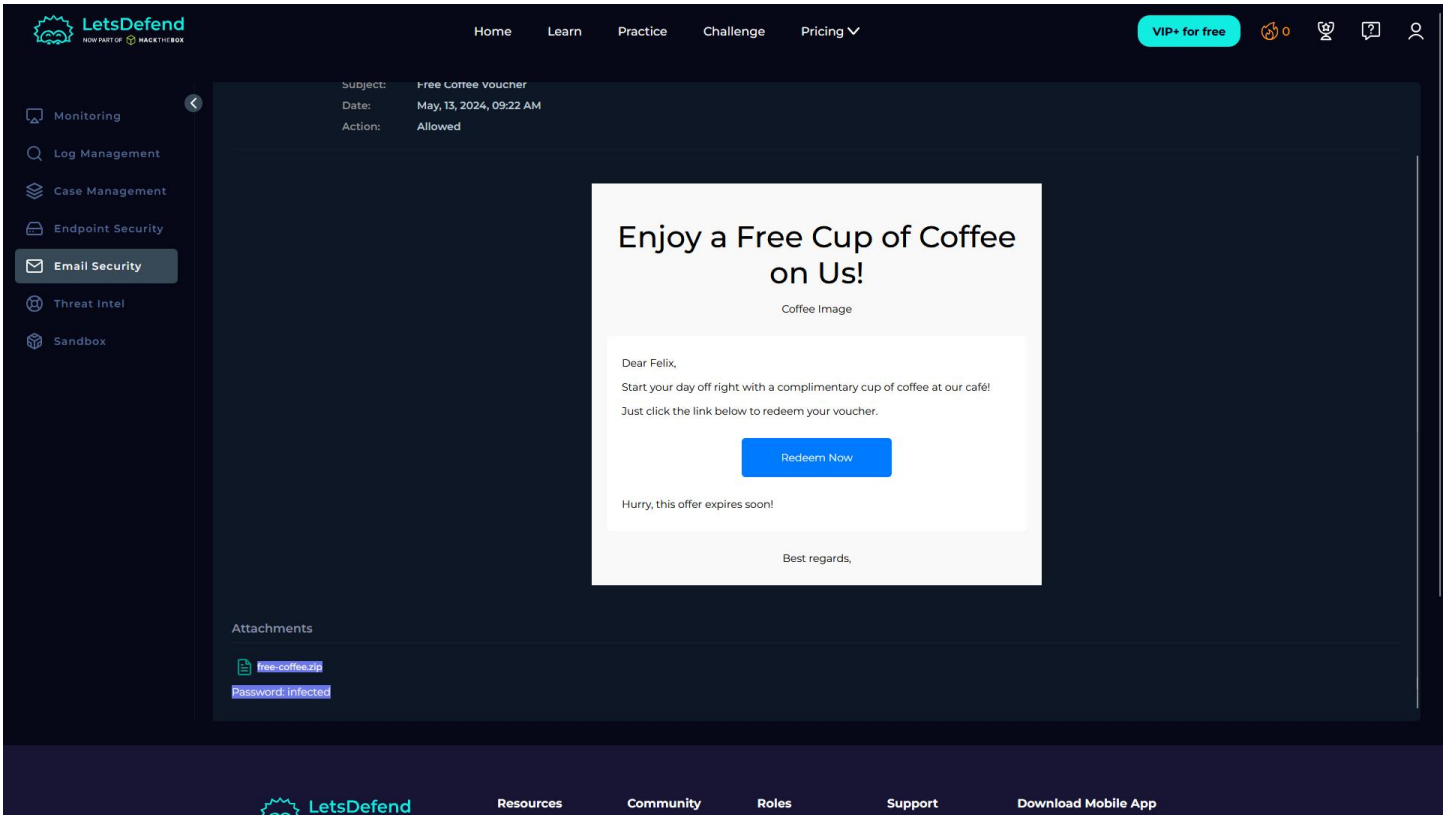

LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
MAIN CHANNEL
INVESTIGATION CHANNEL
CLOSED ALERTS
SEVERITY DATE RULE NAME EVENTID TYPE ACTION
Critical Jul, 22, 2025, 01:07 PM SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE 320 Web Attack
Critical Mar, 13, 2025, 09:44 AM SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing 316 Data Leakage
Medium Jan, 22, 2025, 02:37 AM SOC335 - CVE-2024-49138 Exploitation Detected 313 Privilege Escalation
Medium Sep, 17, 2024, 12:05 PM SOC326 - Impersonating Domain MX Record Change Detected 304 ThreatIntel
High Jun, 06, 2024, 03:12 PM SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919] 263 Web Attack
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
Medium Apr, 19, 2024, 08:23 AM SOC275 - Application Token Steal Attempt Detected 250 Proxy
Critical Apr, 18, 2024, 03:09 AM SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400) 249 Web Attack
Medium Mar, 14, 2024, 05:23 PM SOC153 - Suspicious Powershell Script Executed 238 Malware


LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
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
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
297819
URL
2690
IP
382
Hash
549
Domain
Select Filters...
Clear
Free text search
103.80.134.63
Date range
Select Date
Search by data type
Select
Search by data
Search
Search by tag
Search
Search
Minimize
DATE
DATA TYPE
DATA
TAG
DATA SOURCE
May, 13, 2024, 02:52 PM
IP
103.80.134.63
phishing
Anonymous


Monitoring - LetsDefend
EndPoint Security - LetsDefe
Threat Intelligence Feed - L
Log Management - LetsDefe
app.letsdefend.io/endpoint
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
felix
Felix
172.16.20.151
Processes 86
Network Action 23
Terminal History 8
Browser History 12
Results: 10
EVENT TIME
COMMAND LINE
May 13 2024 13:01:00
"C:\Windows\System32\cmd.exe"
May 13 2024 13:01:05
"C:\Windows\System32\cmd.exe" /c systeminfo
COMMAND LINE
"C:\Windows\System32\cmd.exe" /c wmic logicaldisk get caption,description,providername
May 13 2024 13:01:20
"C:\Windows\System32\cmd.exe" /c tasklist /svc
May 13 2024 13:01:25
"C:\Windows\System32\cmd.exe" /c ipconfig /all
May 13 2024 13:01:30
"C:\Windows\System32\cmd.exe" /c route print
Search
ENG
4:54 PM
4/3/2026


LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
felix
Felix
172.16.20.151
Client/Server: Client
Last Login: May, 13, 2024, 12:04 PM
Processes 86
Network Action 23
Terminal History 8
Browser History 12
Results: 10
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
1
2


LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
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
LetsDefend
Resources
Community
Roles
Support
Download Mobile App