Date of Report: April 3, 2026

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:
September 18, 2024, 01:32 PM

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

Log Management / SIEM alert indicating suspicious network activity and a proxy connection to a potentially malicious domain (letsdefwnd.io).

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

A phishing email was sent from voucher@letsdefwnd.io (IP: 45.33.23.183) to the internal user Mateo (mateo@letsdefend.io). Log analysis confirms that the user Mateo clicked on the provided link (https://letsdefwnd.io). Proxy and Endpoint Security logs show a successful outbound connection (Device Action: Allowed) from Mateo's machine (IP: 172.16.17.162) to the external malicious IP (45.33.23.183) over port 443 via the chrome.exe process.

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:

User Mateo's workstation (172.16.17.162) successfully connected to the malicious domain. The host is considered compromised pending further forensic investigation.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:

Was the IT/security team alerted?

☒ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)

Containment Measures

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

Contained the affected host (172.16.17.162) through the Endpoint Security solution (Network Isolation). Blocked the malicious IP (45.33.23.183) and domain (letsdefwnd.io) on the perimeter firewall and proxy.

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

☒ Yes ☐ No

If yes, provide details:

Mateo's network access was suspended, and firewall rules were updated to block indicators of compromise (IOCs). User credentials should be reset as a precaution.

Impacted Services Measures

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

Mateo's Workstation (IP: 172.16.17.162).

Estimated number of affected users, if applicable:

1 user (Mateo).

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):

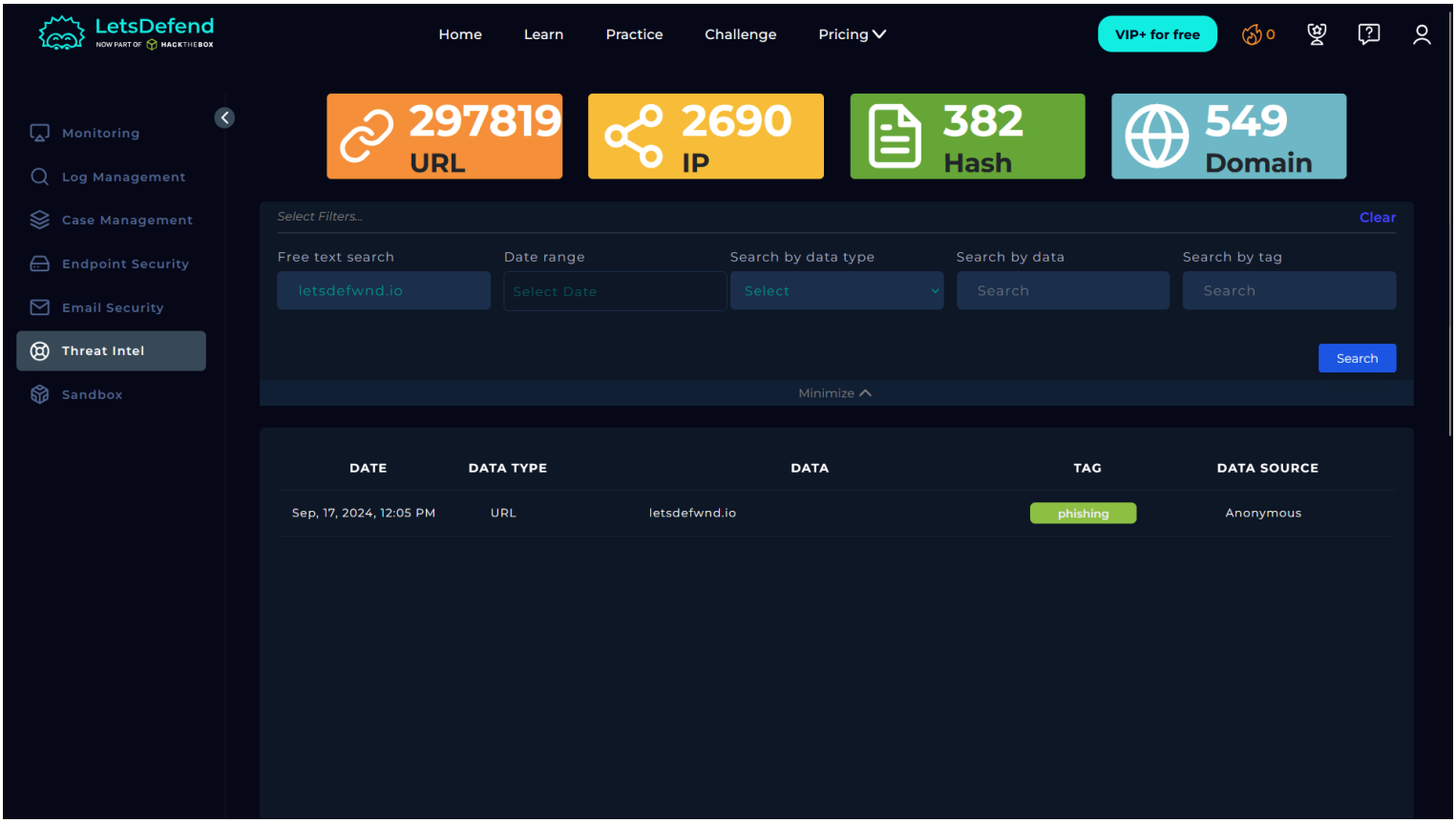
Suspected cause or entry point (e.g., phishing email, unpatched software): Phishing email containing a malicious URL intended to deceive the user (Typosquatting: letsdefwnd instead of letsdefend).

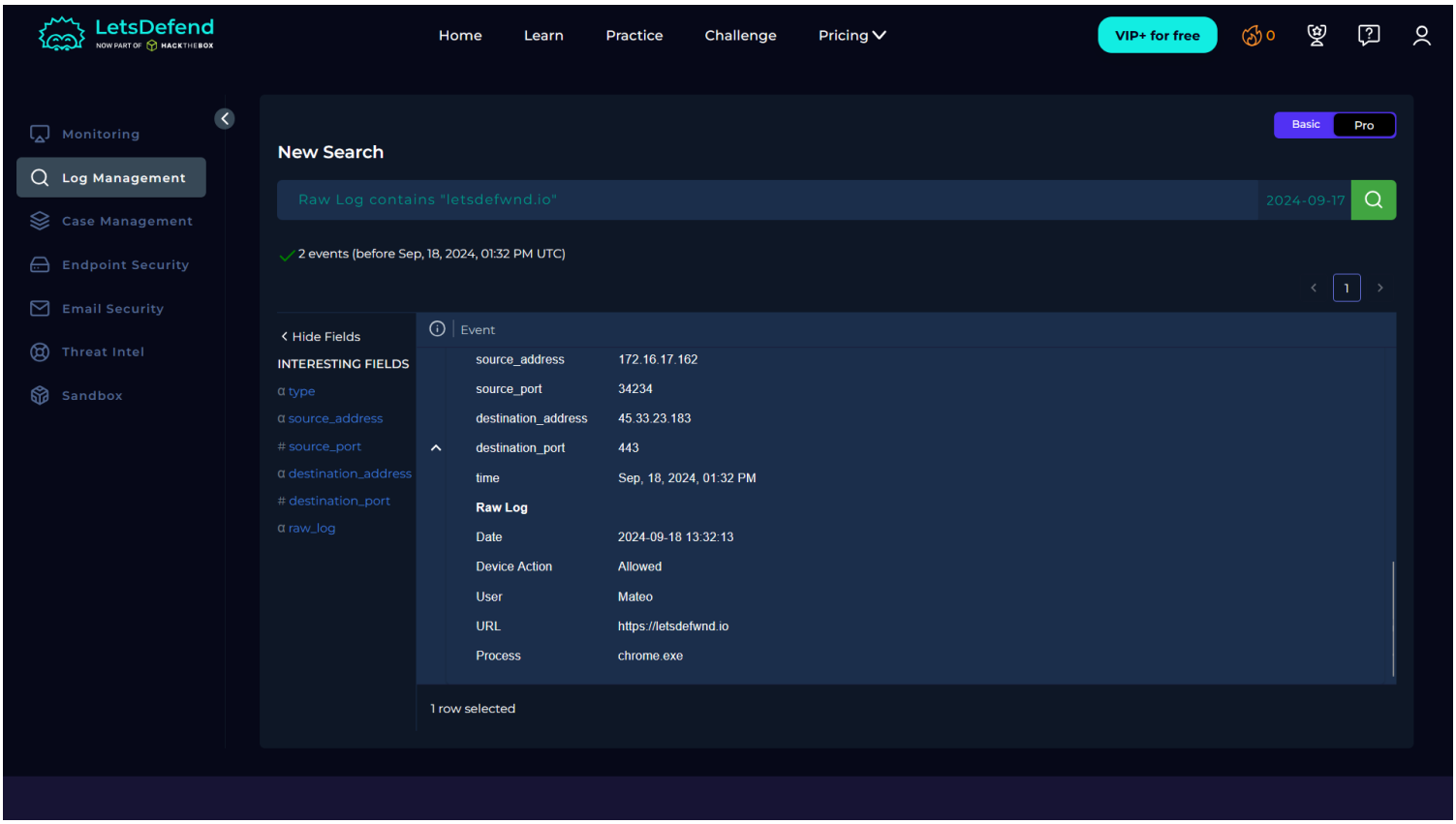
Was the threat internal, external, or unknown?

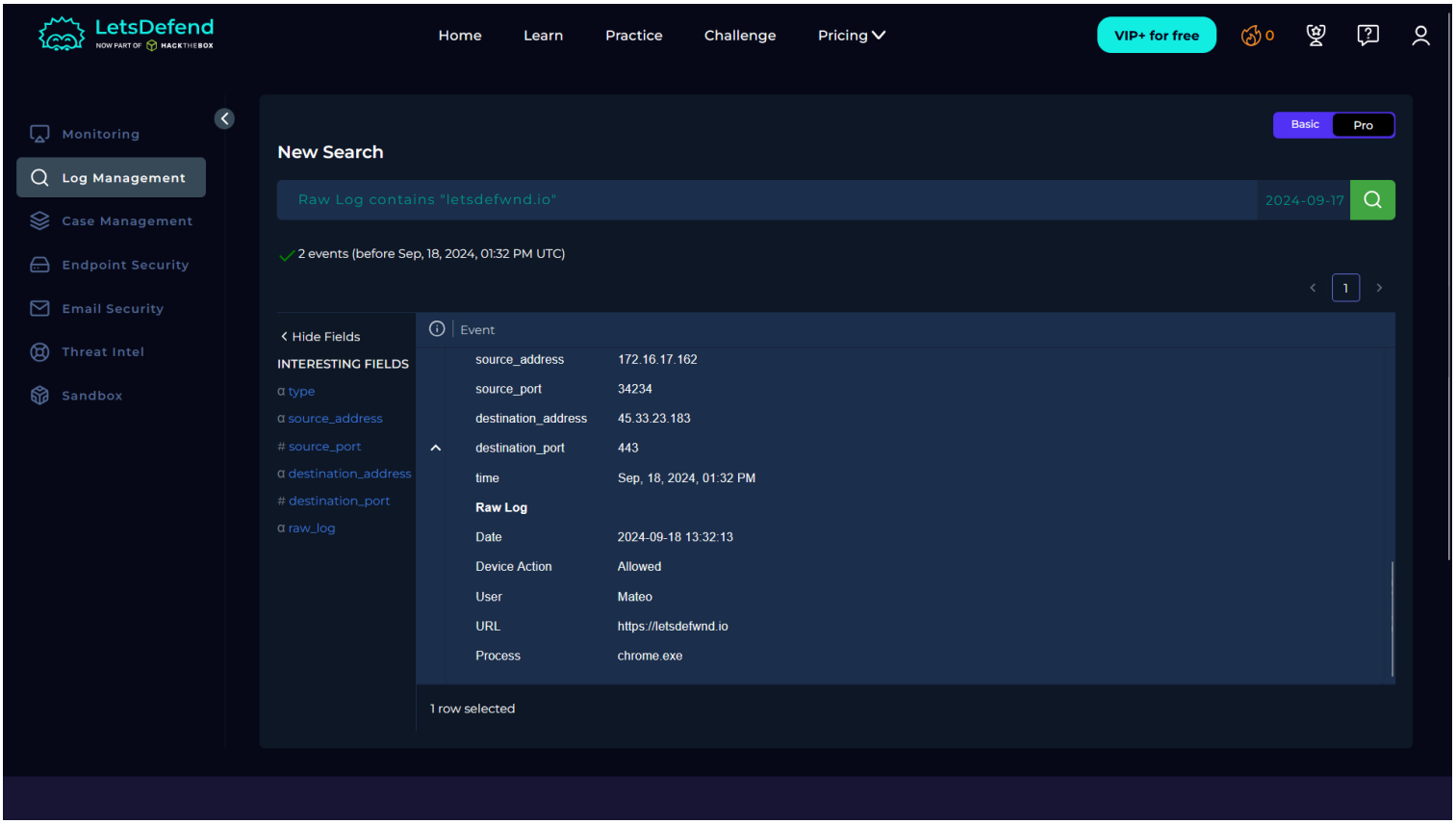
☐ Internal ☒ External ☐ Unknown

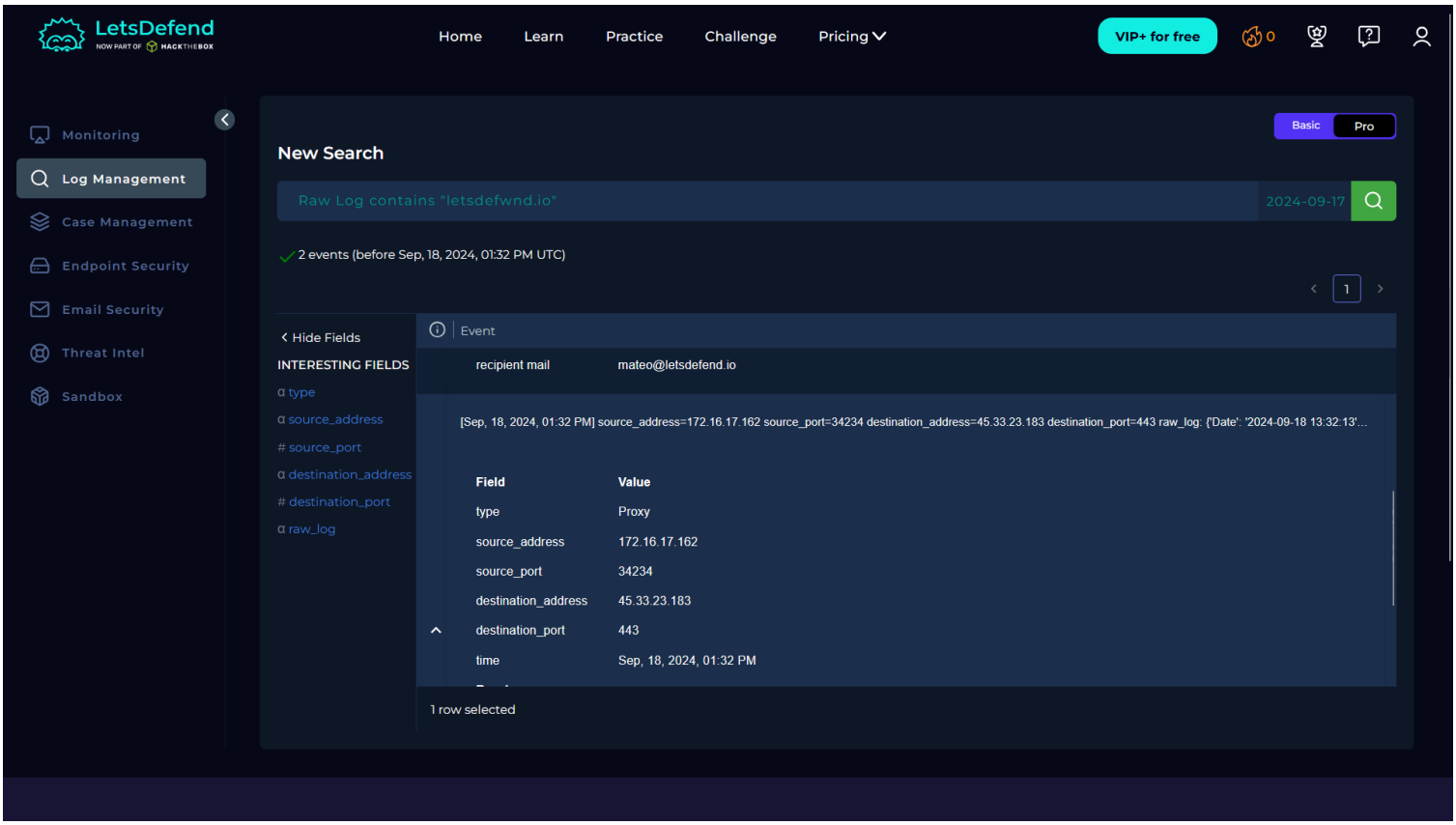
Submitted by:

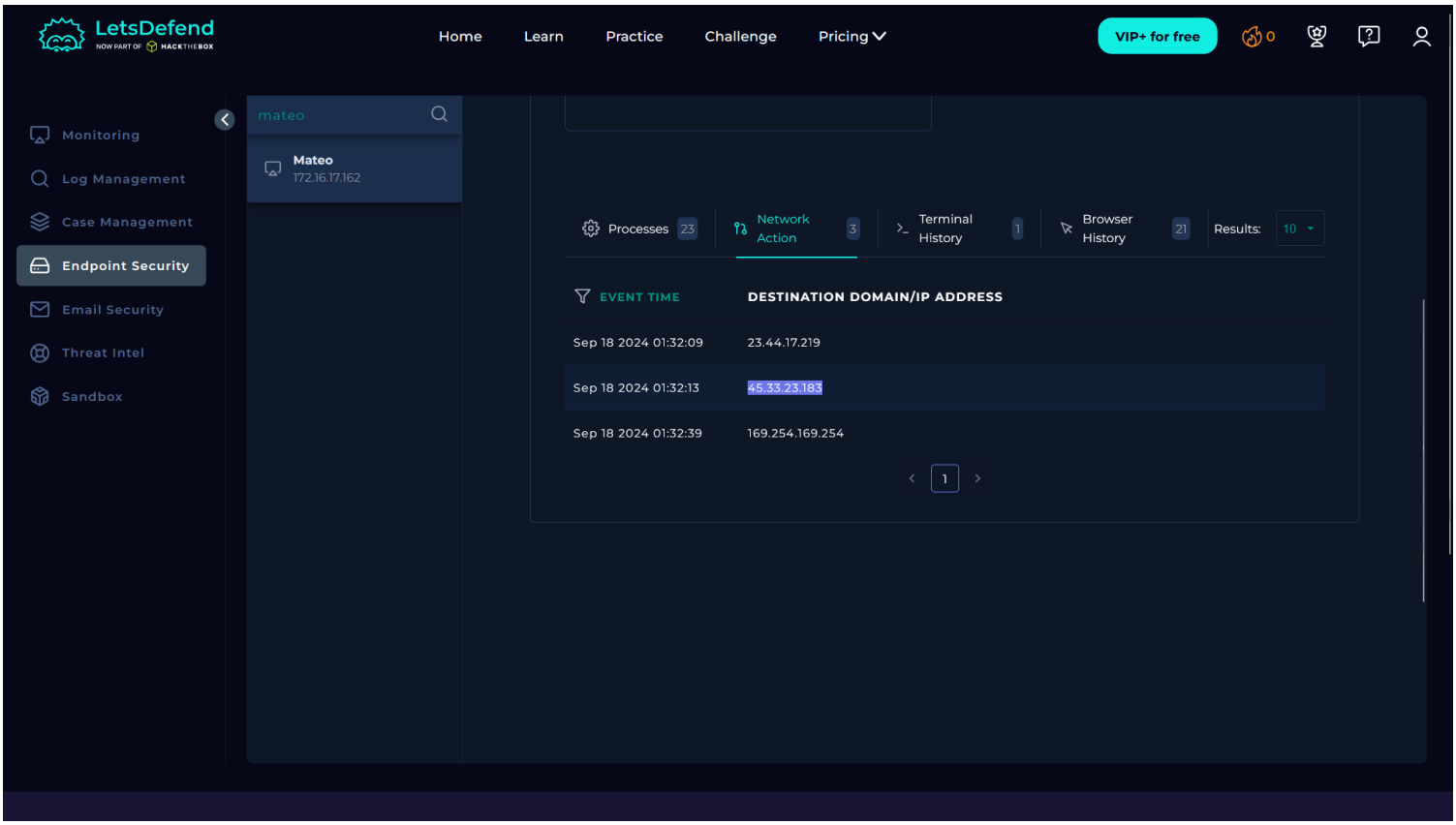
Ahmed Emad Nasr	Ahmed Emad Nasr	April 3, 2026
Name	**Signature**	**Date submitted**

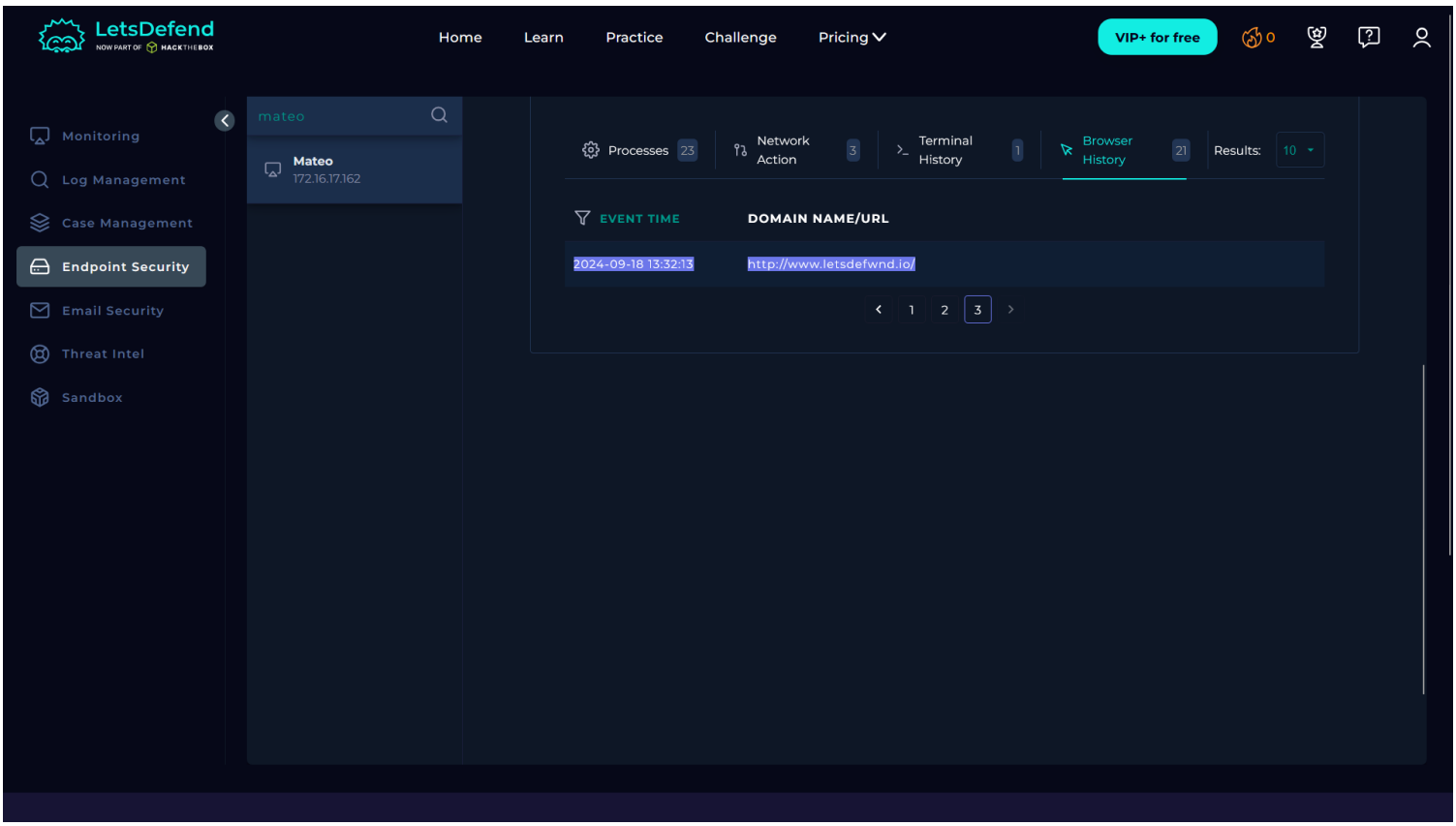

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
297819
URL
2690
IP
382
Hash
549
Domain
Select Filters...
Clear
Free text search
letsdefwnd.io
Date range
Select Date
Search by data type
Select
Search by data
Search
Search by tag
Search
Search
Minimize
DATE
DATA TYPE
DATA
TAG
DATA SOURCE
Sep, 17, 2024, 12:05 PM
URL
letsdefwnd.io
phishing
Anonymous

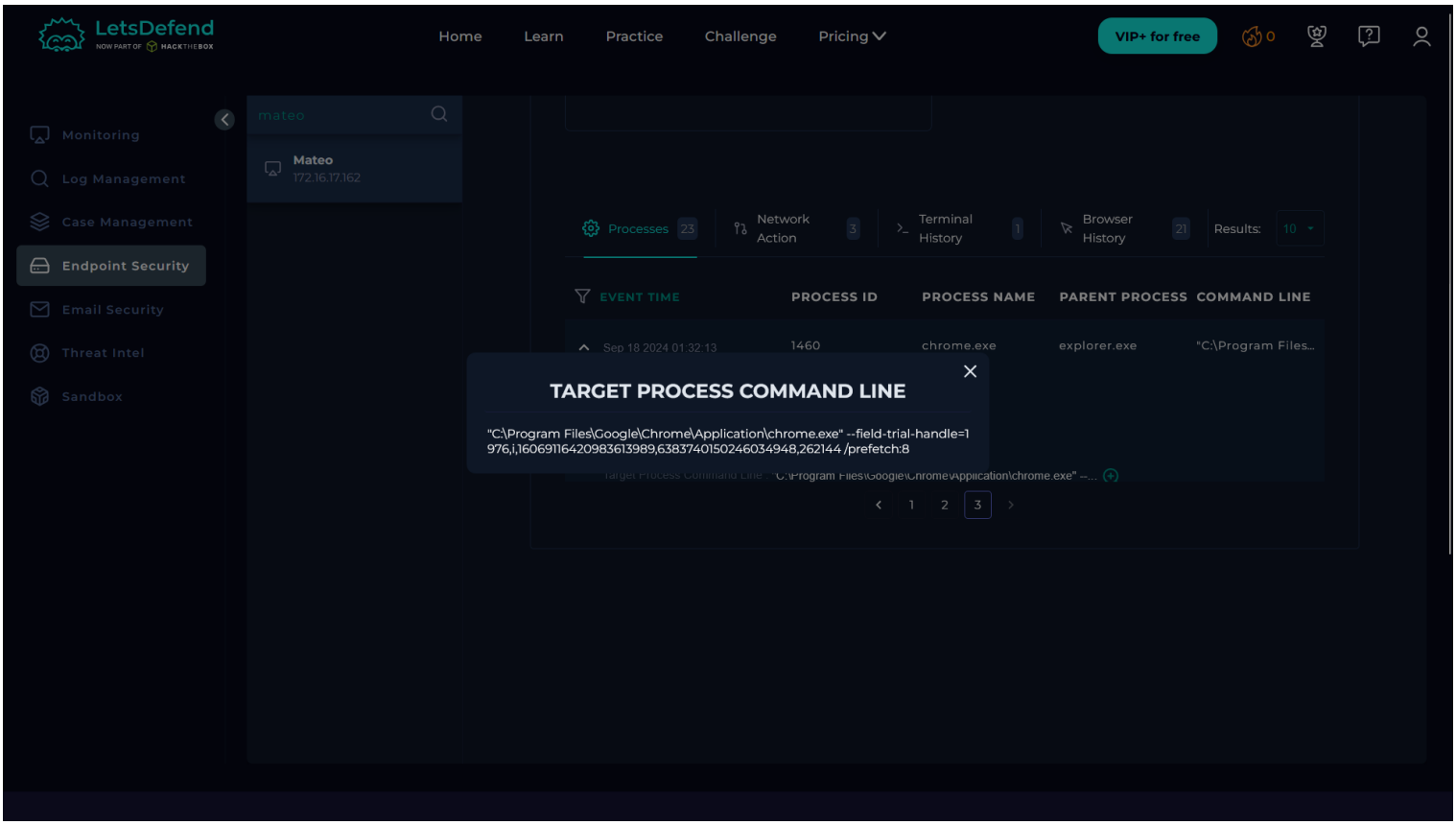

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
Basic
Pro
New Search
Raw Log contains "letsdefwnd.io"
2024-09-17
2 events (before Sep, 18, 2024, 01:32 PM UTC)
1
Hide Fields
INTERESTING FIELDS
α type
α source_address
source_port
α destination_address
destination_port
α raw_log
Event
source_address 172.16.17.162
source_port 34234
destination_address 45.33.23.183
destination_port 443
time Sep, 18, 2024, 01:32 PM
Raw Log
Date 2024-09-18 13:32:13
Device Action Allowed
User Mateo
URL https://letsdefwnd.io
Process chrome.exe
1 row selected

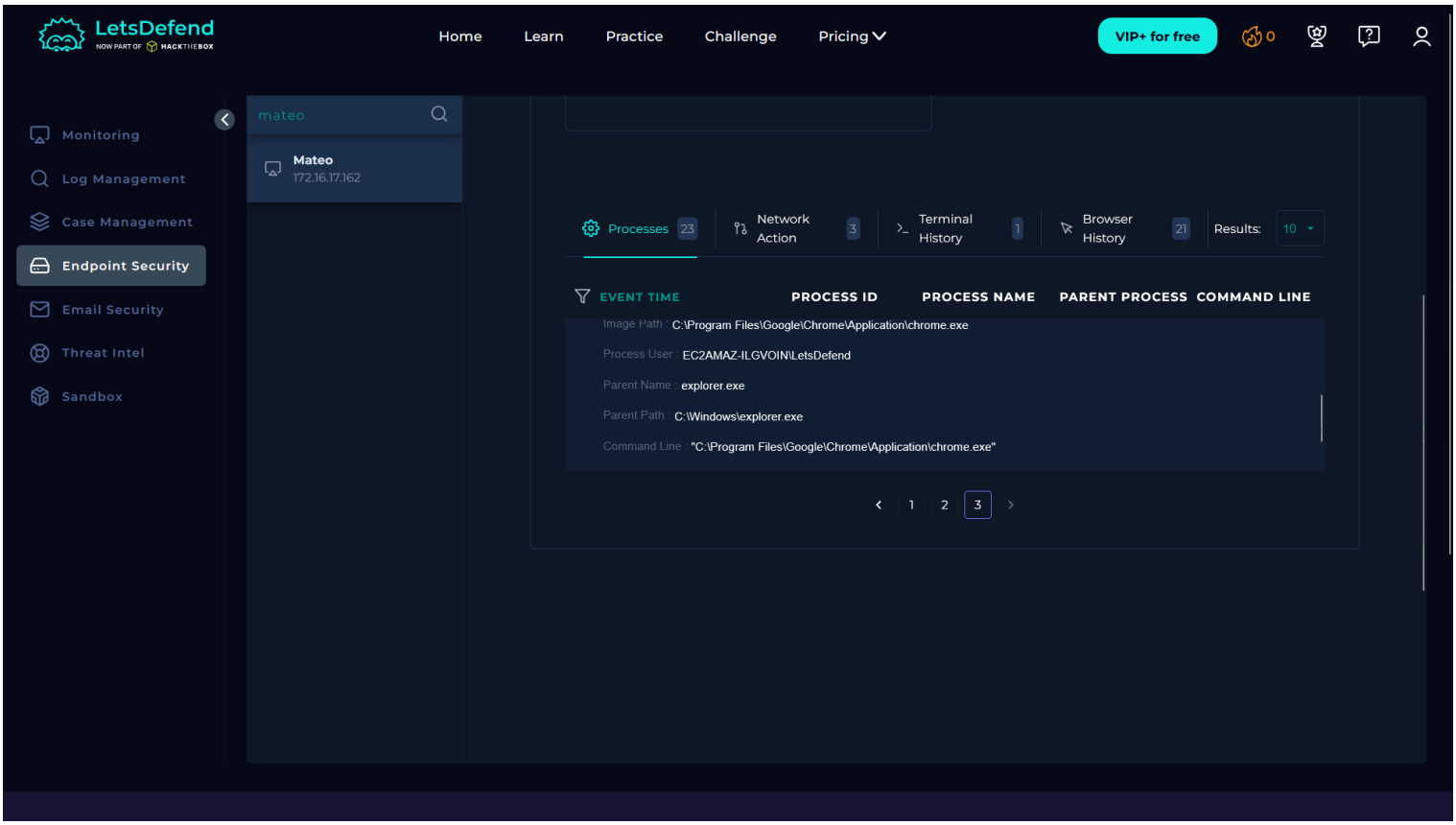

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Raw Log contains "letsdefwnd.io"
2024-09-17
2 events (before Sep, 18, 2024, 01:32 PM UTC)
1
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
source_address 172.16.17.162
source_port 34234
destination_address 45.33.23.183
destination_port 443
time Sep, 18, 2024, 01:32 PM
Raw Log
Date 2024-09-18 13:32:13
Device Action Allowed
User Mateo
URL https://letsdefwnd.io
Process chrome.exe
1 row selected

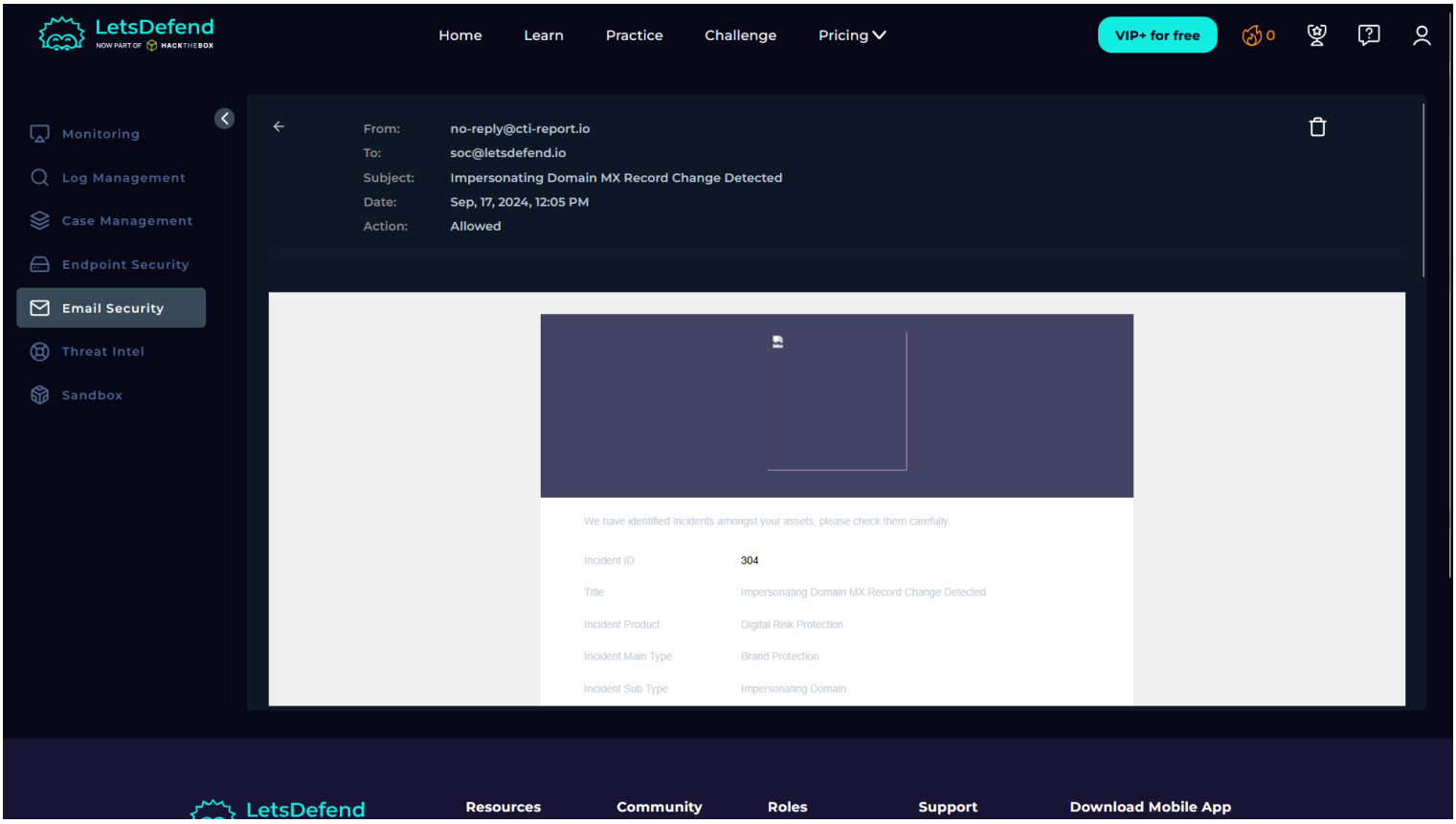

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Raw Log contains "letsdefwnd.io"
2024-09-17
2 events (before Sep, 18, 2024, 01:32 PM UTC)
1
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
recipient mail mateo@letsdefend.io
[Sep, 18, 2024, 01:32 PM] source_address=172.16.17.162 source_port=34234 destination_address=45.33.23.183 destination_port=443 raw_log: {'Date': '2024-09-18 13:32:13'...
Field
Value
type Proxy
source_address 172.16.17.162
source_port 34234
destination_address 45.33.23.183
destination_port 443
time Sep, 18, 2024, 01:32 PM
1 row selected

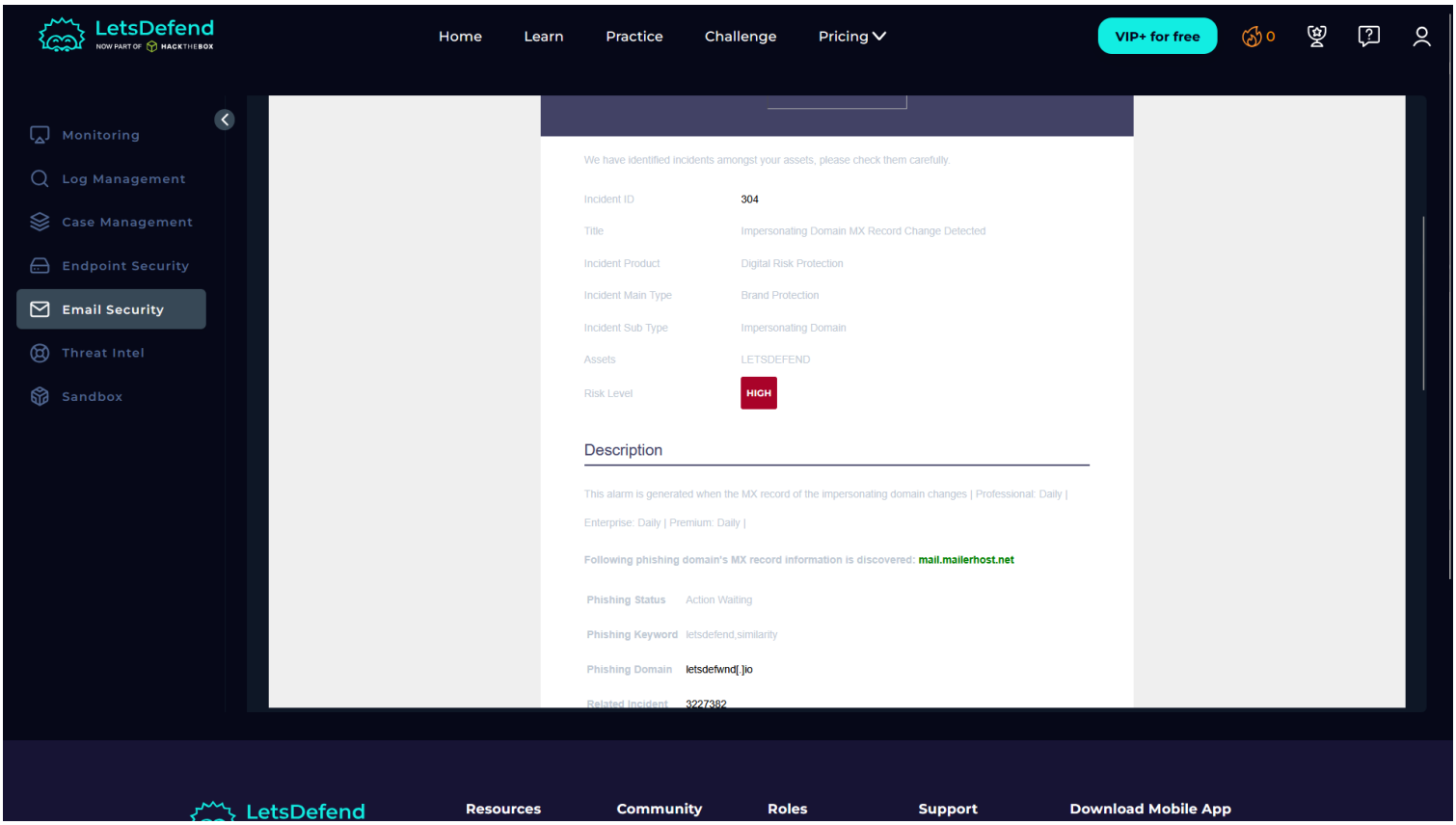

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
mateo
Mateo
172.16.17.162
Processes 23
Network Action 3
Terminal History 1
Browser History 21
Results: 10
EVENT TIME
DESTINATION DOMAIN/IP ADDRESS
Sep 18 2024 01:32:09
23.44.17.219
Sep 18 2024 01:32:13
45.33.23.183
Sep 18 2024 01:32:39
169.254.169.254
1

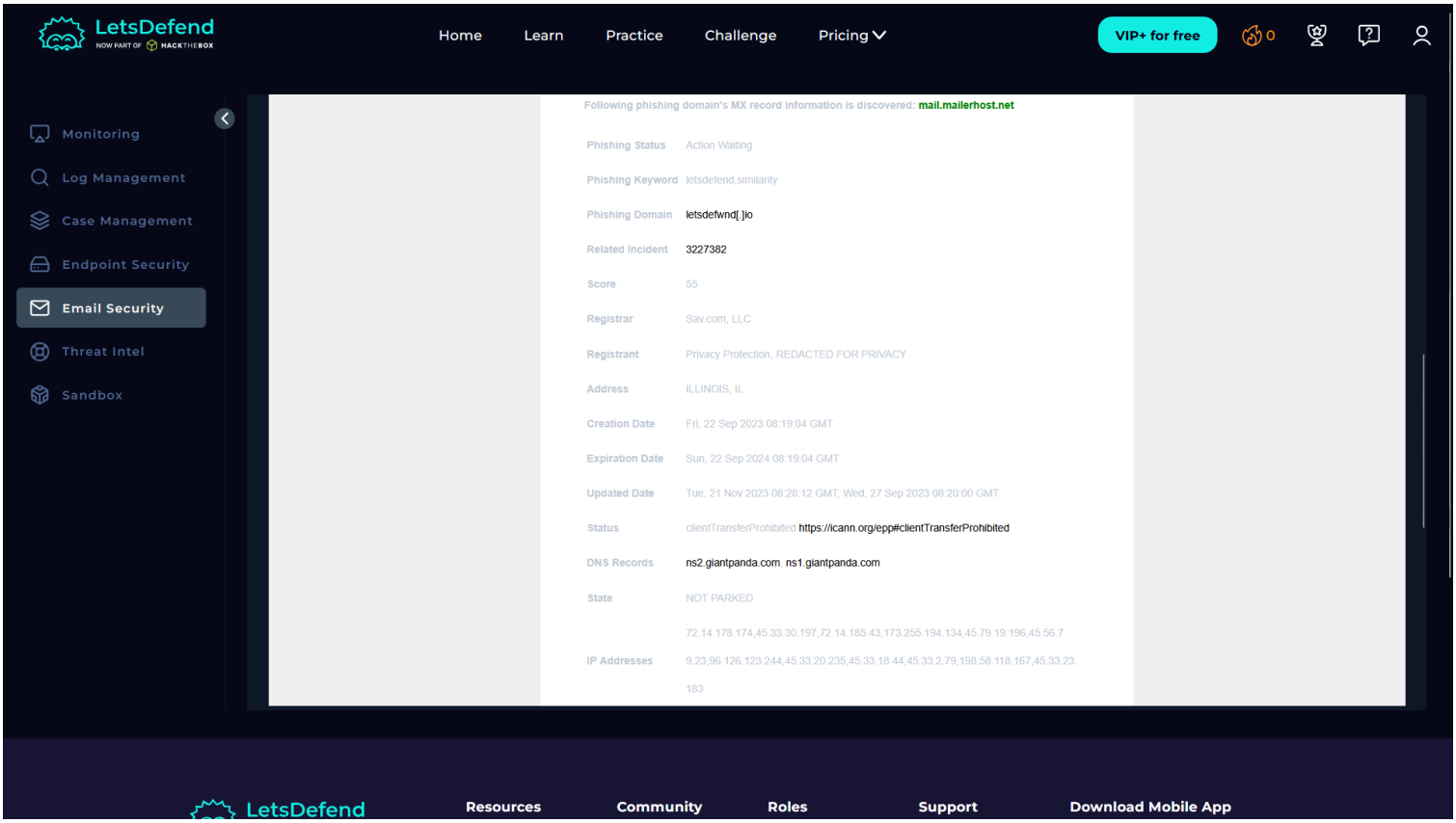

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
mateo
Mateo
172.16.17.162
Processes 23
Network Action 3
Terminal History 1
Browser History 21
Results: 10
EVENT TIME
DOMAIN NAME/URL
2024-09-18 13:32:13
http://www.letsdefwnd.io/
1
2
3

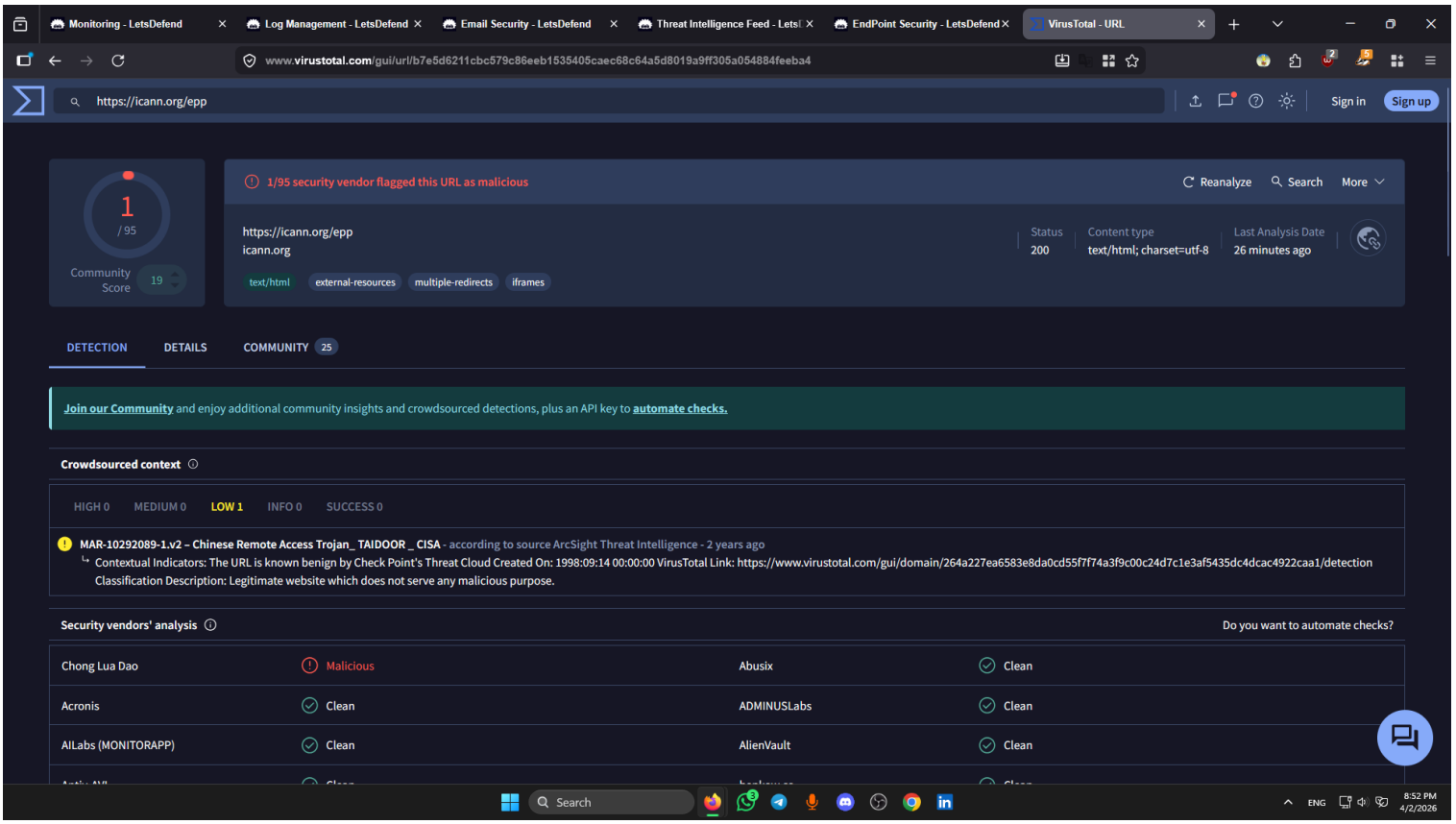

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
mateo
Mateo
172.16.17.162
Processes 23
Network Action 3
Terminal History 1
Browser History 21
Results: 10
EVENT TIME
PROCESS ID
PROCESS NAME
PARENT PROCESS
COMMAND LINE
Sep 18 2024 01:32:13
1460
chrome.exe
explorer.exe
"C:\Program Files...
TARGET PROCESS COMMAND LINE
"C:\Program Files\Google\Chrome\Application\chrome.exe" --field-trial-handle=1976,i,16069116420983613989,6383740150246034948,262144 /prefetch:8
1
2
3

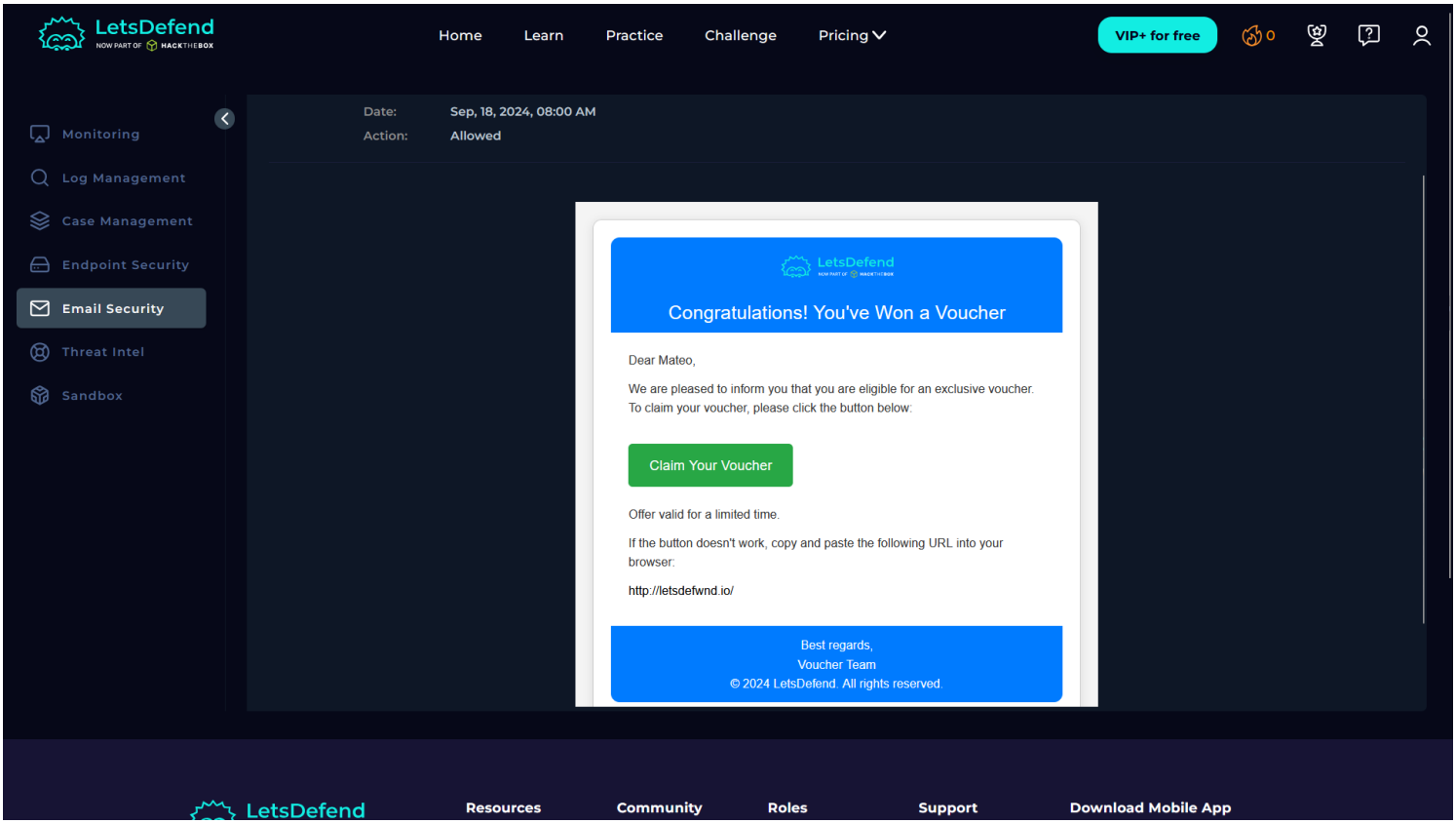

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
mateo
Mateo
172.16.17.162
Processes 23
Network Action 3
Terminal History 1
Browser History 21
Results: 10
EVENT TIME
PROCESS ID
PROCESS NAME
PARENT PROCESS
COMMAND LINE
Image Path : C:\Program Files\Google\Chrome\Application\chrome.exe
Process User : EC2AMAZ-ILGVOIN\LetsDefend
Parent Name : explorer.exe
Parent Path : C:\Windows\explorer.exe
Command Line : "C:\Program Files\Google\Chrome\Application\chrome.exe"
1
2
3


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
From: no-reply@cti-report.io
To: soc@letsdefend.io
Subject: Impersonating Domain MX Record Change Detected
Date: Sep, 17, 2024, 12:05 PM
Action: Allowed
We have identified incidents amongst your assets, please check them carefully.
Incident ID 304
Title Impersonating Domain MX Record Change Detected
Incident Product Digital Risk Protection
Incident Main Type Brand Protection
Incident Sub Type Impersonating Domain
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


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
We have identified incidents amongst your assets, please check them carefully.
Incident ID 304
Title Impersonating Domain MX Record Change Detected
Incident Product Digital Risk Protection
Incident Main Type Brand Protection
Incident Sub Type Impersonating Domain
Assets LETSDEFEND
Risk Level HIGH
Description
This alarm is generated when the MX record of the impersonating domain changes | Professional: Daily | Enterprise: Daily | Premium: Daily |
Following phishing domain's MX record information is discovered: mail.mailerhost.net
Phishing Status Action Waiting
Phishing Keyword letsdefend,similarity
Phishing Domain letsdefwnd[.]io
Related Incident 3227382
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


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
Following phishing domain's MX record information is discovered: mail.mailerhost.net
Phishing Status Action Waiting
Phishing Keyword letsdefend,similarity
Phishing Domain letsdefwnd[.]io
Related Incident 3227382
Score 55
Registrar Sav.com, LLC
Registrant Privacy Protection, REDACTED FOR PRIVACY
Address ILLINOIS, IL
Creation Date Fri, 22 Sep 2023 08:19:04 GMT
Expiration Date Sun, 22 Sep 2024 08:19:04 GMT
Updated Date Tue, 21 Nov 2023 08:28:12 GMT, Wed, 27 Sep 2023 08:20:00 GMT
Status clientTransferProhibited https://icann.org/epp#clientTransferProhibited
DNS Records ns2.giantpanda.com ns1.giantpanda.com
State NOT PARKED
IP Addresses 72.14.178.174,45.33.30.197,72.14.185.43,173.255.194.134,45.79.19.196,45.56.7
9.23,96.126.123.244,45.33.20.235,45.33.18.44,45.33.2.79,198.58.118.167,45.33.23.
183
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


Monitoring - LetsDefend
Log Management - LetsDefend
Email Security - LetsDefend
Threat Intelligence Feed - Letsl
EndPoint Security - LetsDefend
VirusTotal - URL
www.virustotal.com/gui/url/b7e5d6211cbc579c86eeb1535405caec68c64a5d8019a9ff305a054884feeba4
https://icann.org/epp
Sign in
Sign up
1
/ 95
Community Score 19
1/95 security vendor flagged this URL as malicious
Reanalyze
Search
More
https://icann.org/epp
icann.org
text/html
external-resources
multiple-redirects
iframes
Status 200
Content type text/html; charset=utf-8
Last Analysis Date 26 minutes ago
DETECTION
DETAILS
COMMUNITY 25
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Crowdsourced context
HIGH 0
MEDIUM 0
LOW 1
INFO 0
SUCCESS 0
MAR-10292089-1.v2 – Chinese Remote Access Trojan_ TAIDOOR _ CISA - according to source ArcSight Threat Intelligence - 2 years ago
Contextual Indicators: The URL is known benign by Check Point's Threat Cloud Created On: 1998:09:14 00:00:00 VirusTotal Link: https://www.virustotal.com/gui/domain/264a227ea6583e8da0cd55f7f74a3f9c00c24d7c1e3af5435dc4dcac4922caa1/detection
Classification Description: Legitimate website which does not serve any malicious purpose.
Security vendors' analysis
Do you want to automate checks?
Chong Lua Dao Malicious
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
Search
ENG
8:52 PM
4/2/2026


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
Date: Sep, 18, 2024, 08:00 AM
Action: Allowed
LetsDefend
Congratulations! You've Won a Voucher
Dear Mateo,
We are pleased to inform you that you are eligible for an exclusive voucher.
To claim your voucher, please click the button below:
Claim Your Voucher
Offer valid for a limited time.
If the button doesn't work, copy and paste the following URL into your browser:
http://letsdefwnd.io/
Best regards,
Voucher Team
© 2024 LetsDefend. All rights reserved.