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:
Feb, 13, 2024, 02:04 AM.

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

A Low-level security alert was triggered in the Monitoring system under the rule "SOC257 - VPN Connection Detected from Unauthorized Country".

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

- An external IP address (113.161.158.12) successfully established a VPN connection to the destination address 33.33.33.33 (URL: https://vpn-letsdefend.io) using the credentials of the user monica@letsdefend.io (Hostname: Monica).
- Prior to the successful connection alert, between 01:50 AM and 01:58 AM on Feb 13, 2024, the firewall logged 21 events from this same source IP (113.161.158.12) connecting to various destination ports on 33.33.33.33 (e.g., ports 443, 11121, 31054).
- The Threat Intelligence feed indicates that this specific source IP (113.161.158.12) was previously flagged by AbuseCH for "Brute Force" activity on Dec 07, 2023.

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 VPN account for the user monica@letsdefend.io has been compromised and accessed from an unauthorized external location.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 4, 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 containment.

Containment Measures

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

- Terminated the active VPN session for user monica@letsdefend.io.
- Blocked the malicious source IP (113.161.158.12) on the external firewall.

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

☒ Yes ☐ No

If yes, provide details:

- Disabled the Active Directory/VPN account for user monica pending a mandatory password reset and Multi-Factor Authentication (MFA) review.
- Firewall rules updated to drop all inbound traffic from 113.161.158.12.

Impacted Services Measures

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

- VPN Gateway (https://vpn-letsdefend.io / IP: 33.33.33.33).
- User account: monica@letsdefend.io (Hostname: Monica).

Estimated number of affected users, if applicable:

1 user (Monica).

Was there any known data loss or exposure?

☐ Yes ☒ No

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

N/A

Preliminary Analysis *(Optional)*

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

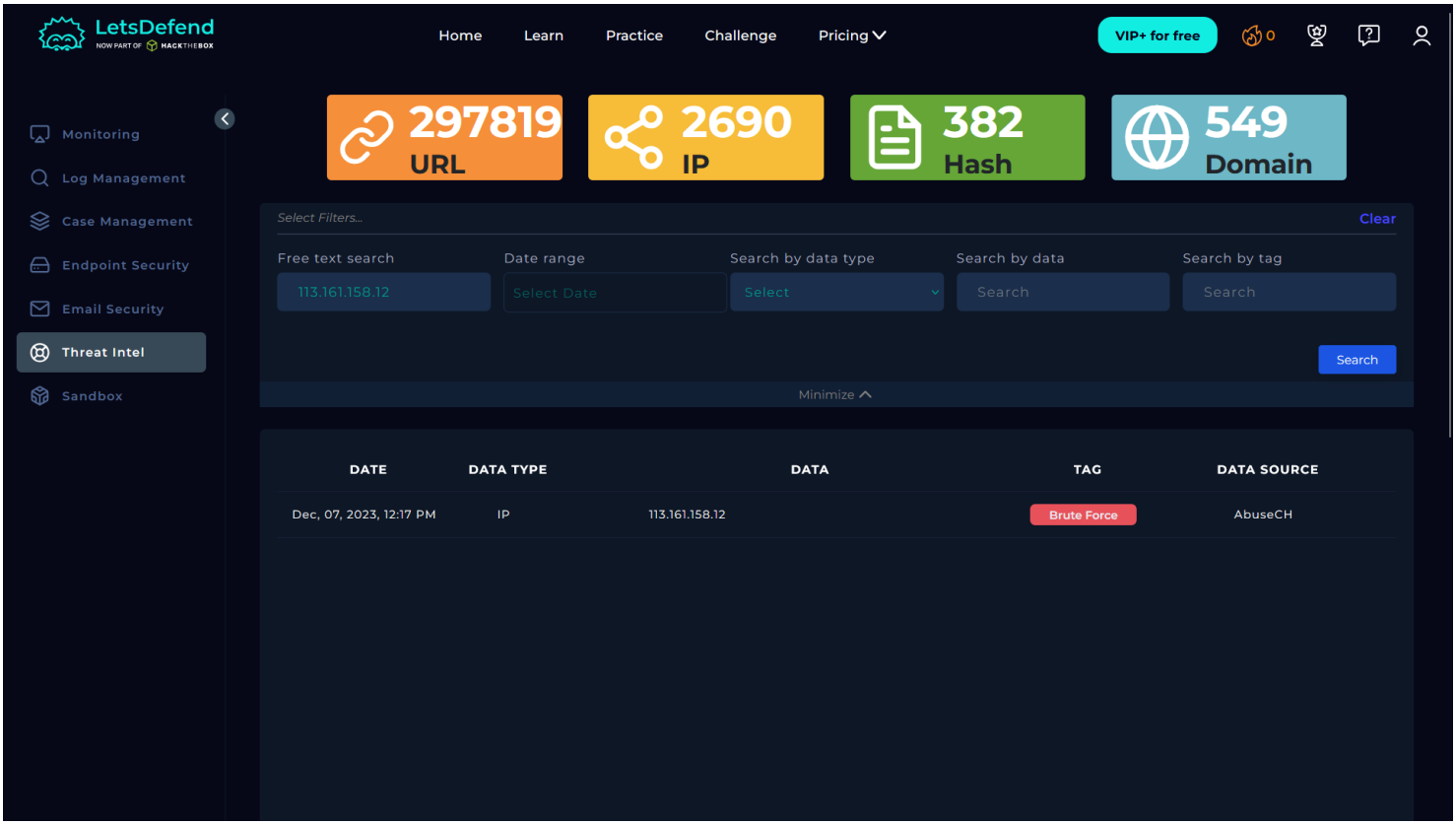
Compromised user credentials, highly likely obtained via a Brute Force attack, given the multiple firewall port connection attempts prior to login and the source IP's known history of Brute Force activities.

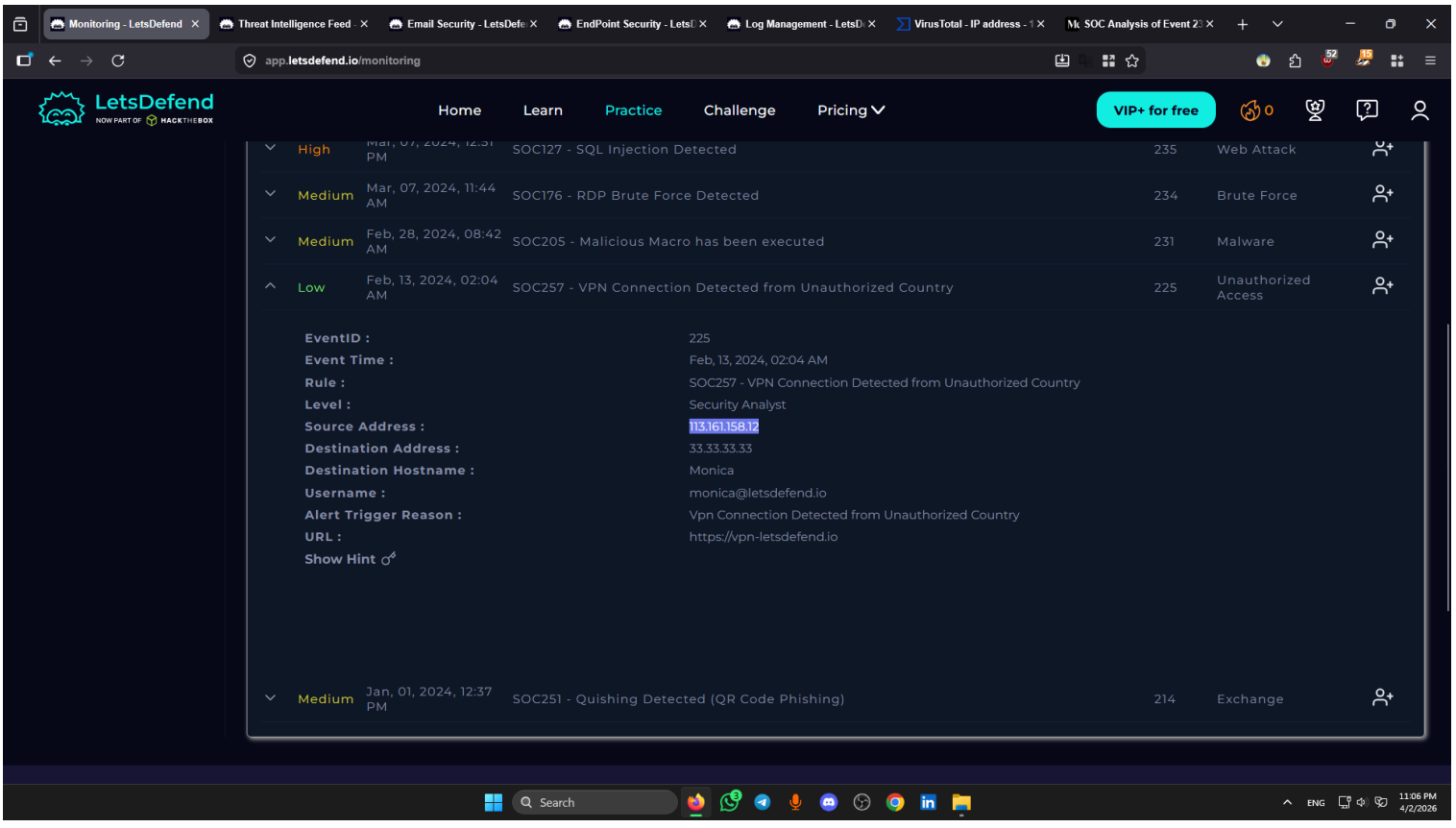
Was the threat internal, external, or unknown?

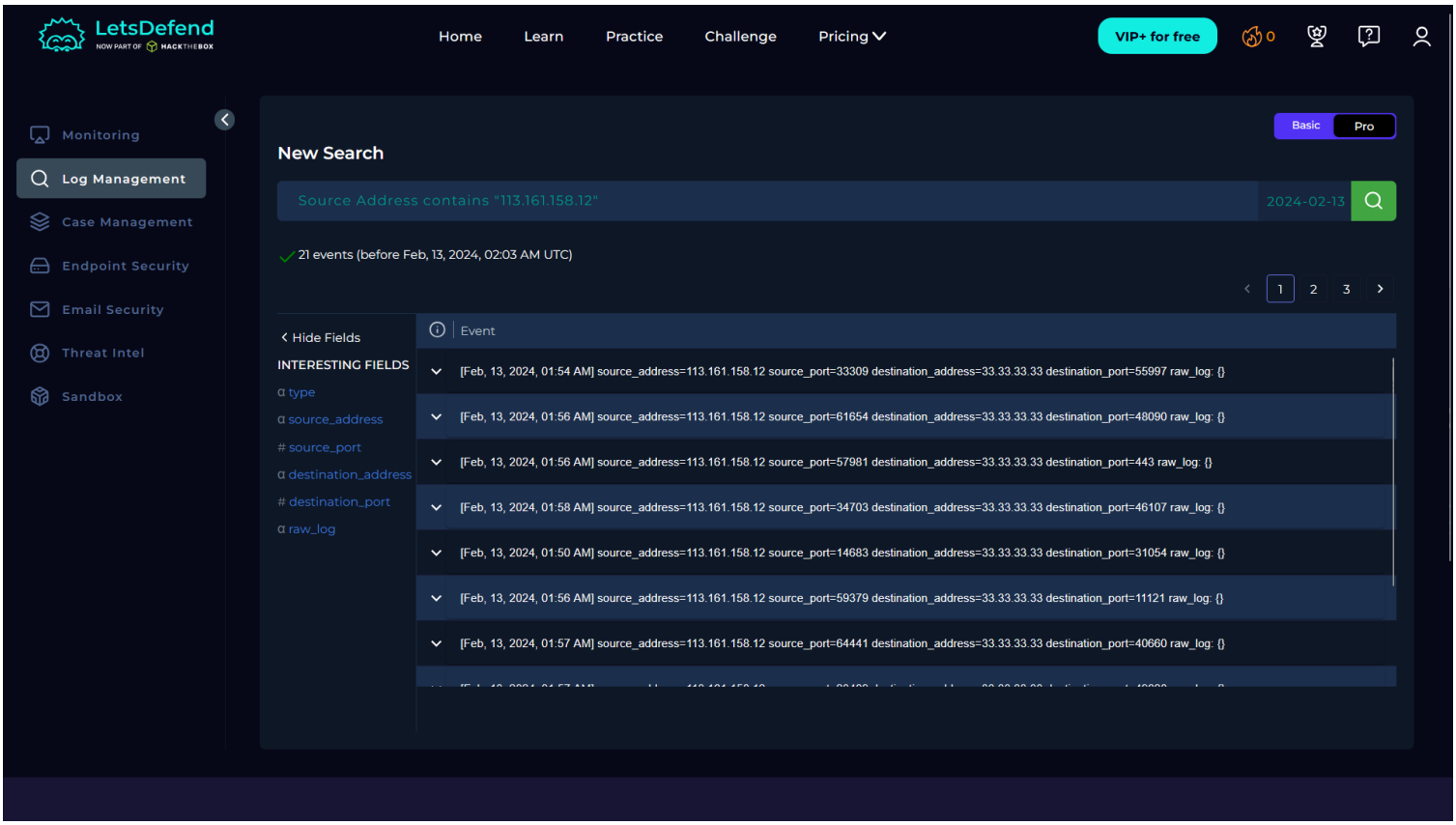
☐ Internal ☒ External ☐ Unknown

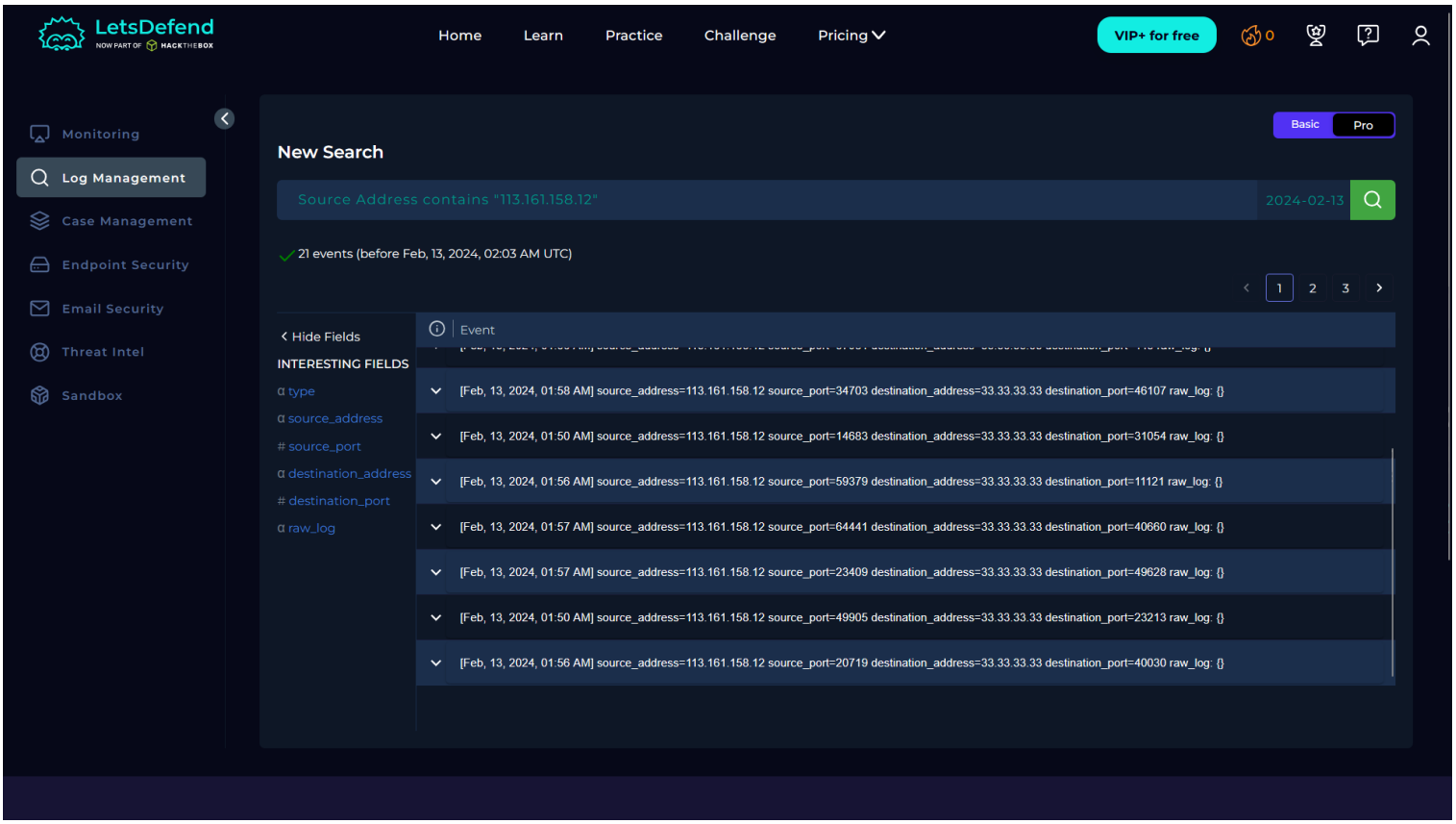
Submitted by:

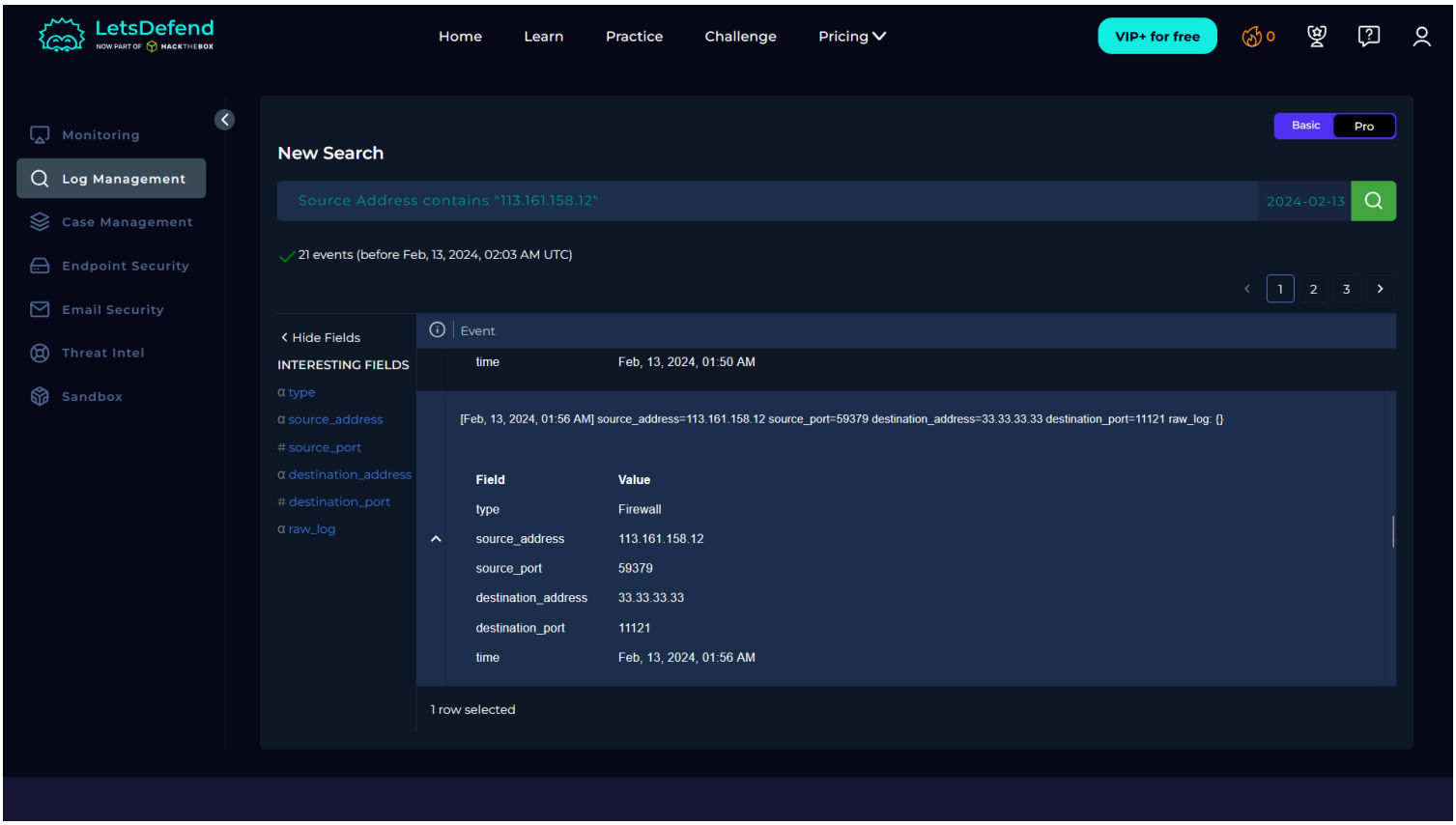
Ahmed Emad Nasr	Ahmed Emad Nasr	
Name	**Signature**	**Date submitted**

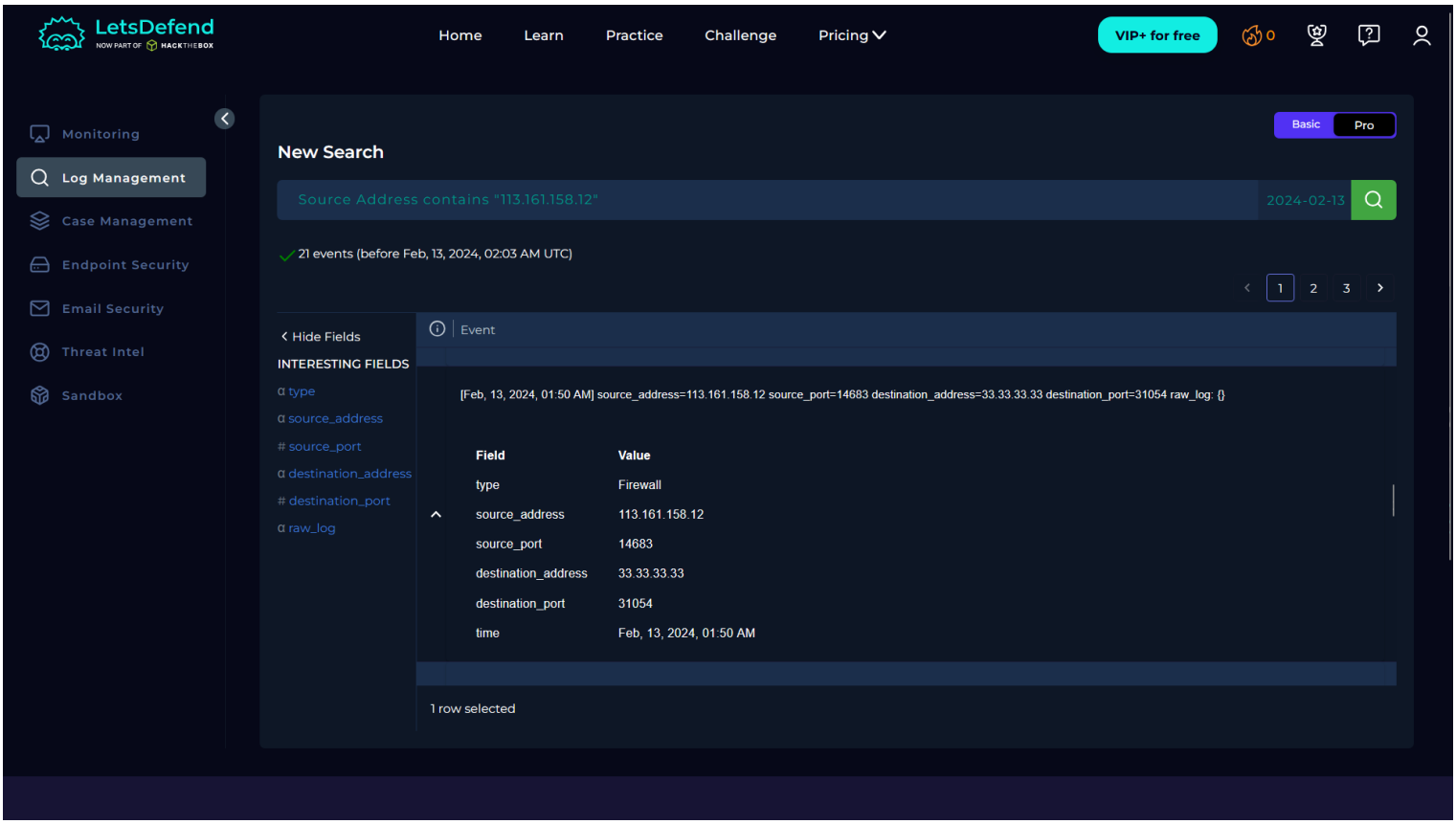

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
297819
URL
2690
IP
382
Hash
549
Domain
Select Filters...
Clear
Free text search
113.161.158.12
Date range
Select Date
Search by data type
Select
Search by data
Search
Search by tag
Search
Search
Minimize
DATE
DATA TYPE
DATA
TAG
DATA SOURCE
Dec, 07, 2023, 12:17 PM
IP
113.161.158.12
Brute Force
AbuseCH


Monitoring - LetsDefend
Threat Intelligence Feed -
Email Security - LetsDefe
EndPoint Security - Lets
Log Management - LetsD
VirusTotal - IP address -
SOC Analysis of Event 2
app.letsdefend.io/monitoring
LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
High
PM
SOC127 - SQL Injection Detected
235
Web Attack
Medium
Mar, 07, 2024, 11:44 AM
SOC176 - RDP Brute Force Detected
234
Brute Force
Medium
Feb, 28, 2024, 08:42 AM
SOC205 - Malicious Macro has been executed
231
Malware
Low
Feb, 13, 2024, 02:04 AM
SOC257 - VPN Connection Detected from Unauthorized Country
225
Unauthorized Access
EventID : 225
Event Time : Feb, 13, 2024, 02:04 AM
Rule : SOC257 - VPN Connection Detected from Unauthorized Country
Level : Security Analyst
Source Address : 113.161.158.12
Destination Address : 33.33.33.33
Destination Hostname : Monica
Username : monica@letsdefend.io
Alert Trigger Reason : Vpn Connection Detected from Unauthorized Country
URL : https://vpn-letsdefend.io
Show Hint
Medium
Jan, 01, 2024, 12:37 PM
SOC251 - Quishing Detected (QR Code Phishing)
214
Exchange
Search
ENG
11:06 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
Basic
Pro
New Search
Source Address contains "113.161.158.12"
2024-02-13
21 events (before Feb, 13, 2024, 02:03 AM UTC)
1
2
3
Hide Fields
INTERESTING FIELDS
α type
α source_address
source_port
α destination_address
destination_port
α raw_log
Event
[Feb, 13, 2024, 01:54 AM] source_address=113.161.158.12 source_port=33309 destination_address=33.33.33.33 destination_port=55997 raw_log: {}
[Feb, 13, 2024, 01:56 AM] source_address=113.161.158.12 source_port=61654 destination_address=33.33.33.33 destination_port=48090 raw_log: {}
[Feb, 13, 2024, 01:56 AM] source_address=113.161.158.12 source_port=57981 destination_address=33.33.33.33 destination_port=443 raw_log: {}
[Feb, 13, 2024, 01:58 AM] source_address=113.161.158.12 source_port=34703 destination_address=33.33.33.33 destination_port=46107 raw_log: {}
[Feb, 13, 2024, 01:50 AM] source_address=113.161.158.12 source_port=14683 destination_address=33.33.33.33 destination_port=31054 raw_log: {}
[Feb, 13, 2024, 01:56 AM] source_address=113.161.158.12 source_port=59379 destination_address=33.33.33.33 destination_port=11121 raw_log: {}
[Feb, 13, 2024, 01:57 AM] source_address=113.161.158.12 source_port=64441 destination_address=33.33.33.33 destination_port=40660 raw_log: {}


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 "113.161.158.12"
2024-02-13
21 events (before Feb, 13, 2024, 02:03 AM UTC)
1
2
3
Hide Fields
INTERESTING FIELDS
α type
α source_address
source_port
α destination_address
destination_port
α raw_log
Event
[Feb, 13, 2024, 01:58 AM] source_address=113.161.158.12 source_port=34703 destination_address=33.33.33.33 destination_port=46107 raw_log: {}
[Feb, 13, 2024, 01:50 AM] source_address=113.161.158.12 source_port=14683 destination_address=33.33.33.33 destination_port=31054 raw_log: {}
[Feb, 13, 2024, 01:56 AM] source_address=113.161.158.12 source_port=59379 destination_address=33.33.33.33 destination_port=11121 raw_log: {}
[Feb, 13, 2024, 01:57 AM] source_address=113.161.158.12 source_port=64441 destination_address=33.33.33.33 destination_port=40660 raw_log: {}
[Feb, 13, 2024, 01:57 AM] source_address=113.161.158.12 source_port=23409 destination_address=33.33.33.33 destination_port=49628 raw_log: {}
[Feb, 13, 2024, 01:50 AM] source_address=113.161.158.12 source_port=49905 destination_address=33.33.33.33 destination_port=23213 raw_log: {}
[Feb, 13, 2024, 01:56 AM] source_address=113.161.158.12 source_port=20719 destination_address=33.33.33.33 destination_port=40030 raw_log: {}


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 "113.161.158.12"
2024-02-13
21 events (before Feb, 13, 2024, 02:03 AM UTC)
1
2
3
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
time
Feb, 13, 2024, 01:50 AM
[Feb, 13, 2024, 01:56 AM] source_address=113.161.158.12 source_port=59379 destination_address=33.33.33.33 destination_port=11121 raw_log: {}
Field
Value
type
Firewall
source_address
113.161.158.12
source_port
59379
destination_address
33.33.33.33
destination_port
11121
time
Feb, 13, 2024, 01:56 AM
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
Basic
Pro
New Search
Source Address contains "113.161.158.12"
2024-02-13
21 events (before Feb, 13, 2024, 02:03 AM UTC)
1
2
3
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
[Feb, 13, 2024, 01:50 AM] source_address=113.161.158.12 source_port=14683 destination_address=33.33.33.33 destination_port=31054 raw_log: {}
Field
Value
type
Firewall
source_address
113.161.158.12
source_port
14683
destination_address
33.33.33.33
destination_port
31054
time
Feb, 13, 2024, 01:50 AM
1 row selected