LetsDefend

Official Incident Report

Event ID: 234

Rule Name: SOC176 - RDP Brute Force Detected

Table of Contents

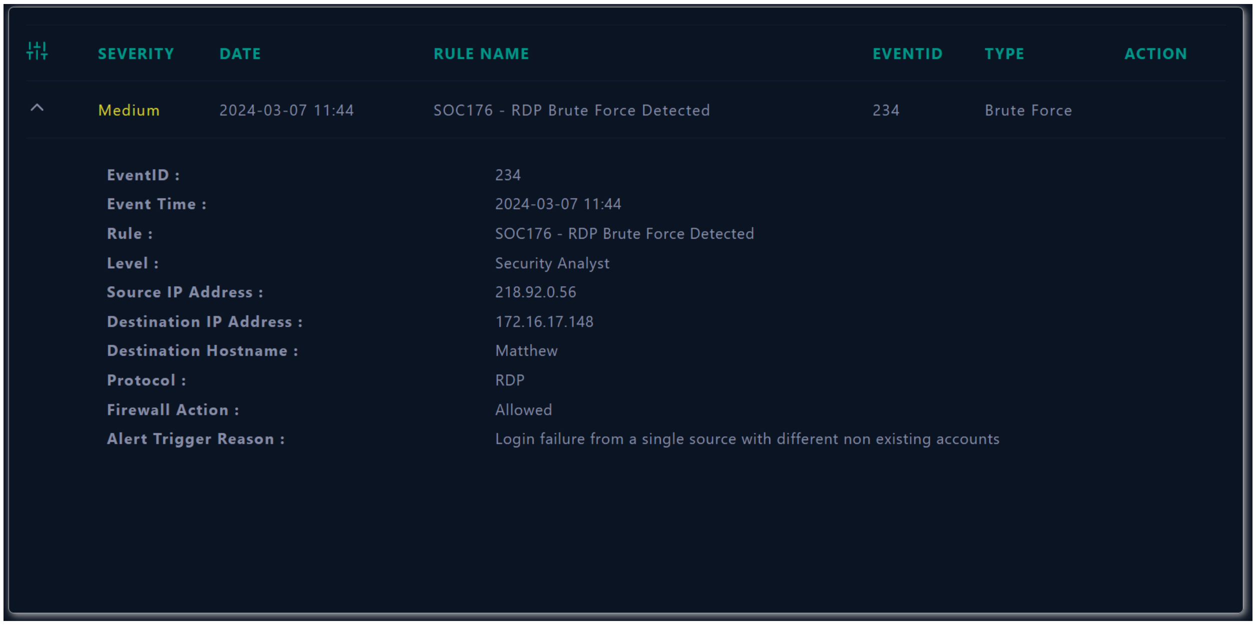
Alert

Based on the information that the alert provided, it appears that there are suspicious login failure events detected on a host named "**Matthew**" with an IP address of **172.16.17.148**. The Alert is triggered by the **SOC176** rule for **RDP Brute Force Detected**.

> *RDP brute force refers to* ***a type of cyberattack in which an attacker systematically attempts to gain unauthorized access to a network by repeatedly guessing or "brute forcing" the password of an RDP account****.*

Explanation of RDP BruteForce by PaloAlto

The firewall action is marked as "**Allowed**", indicating that no action was taken by the firewall to prevent or block the related requests.



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	2024-03-07 11:44	SOC176 - RDP Brute Force Detected	234	Brute Force	

EventID :	234
Event Time :	2024-03-07 11:44
Rule :	SOC176 - RDP Brute Force Detected
Level :	Security Analyst
Source IP Address :	218.92.0.56
Destination IP Address :	172.16.17.148
Destination Hostname :	Matthew
Protocol :	RDP
Firewall Action :	Allowed
Alert Trigger Reason :	Login failure from a single source with different non existing accounts

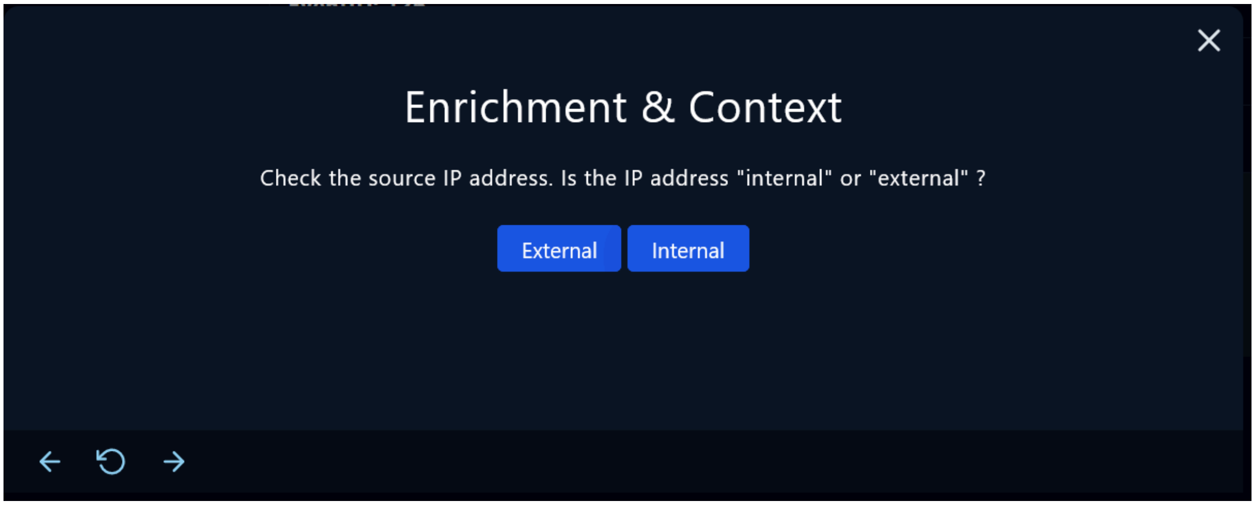
The alert suggests that there were login attempts from the source IP address (218.92.0[.]56) to the destination host named "Matthew" (172.16.17.148) over RDP. The firewall allowed this traffic. However, the attempts triggered an alert due to repeated login failures from the same source, indicating attempts to access non-existing accounts.

This activity was flagged as the detection of multiple login failures from a single source, leading to the triggering of an alert. This behavior could be indicative of a potential security threat and needs to be investigated.

Detection

Enrichment & Context

As the playbook suggests we can start investigating the alert by verifying that the IP address is “internal or “external”.



Enrichment & Context

Check the source IP address. Is the IP address "internal" or "external" ?

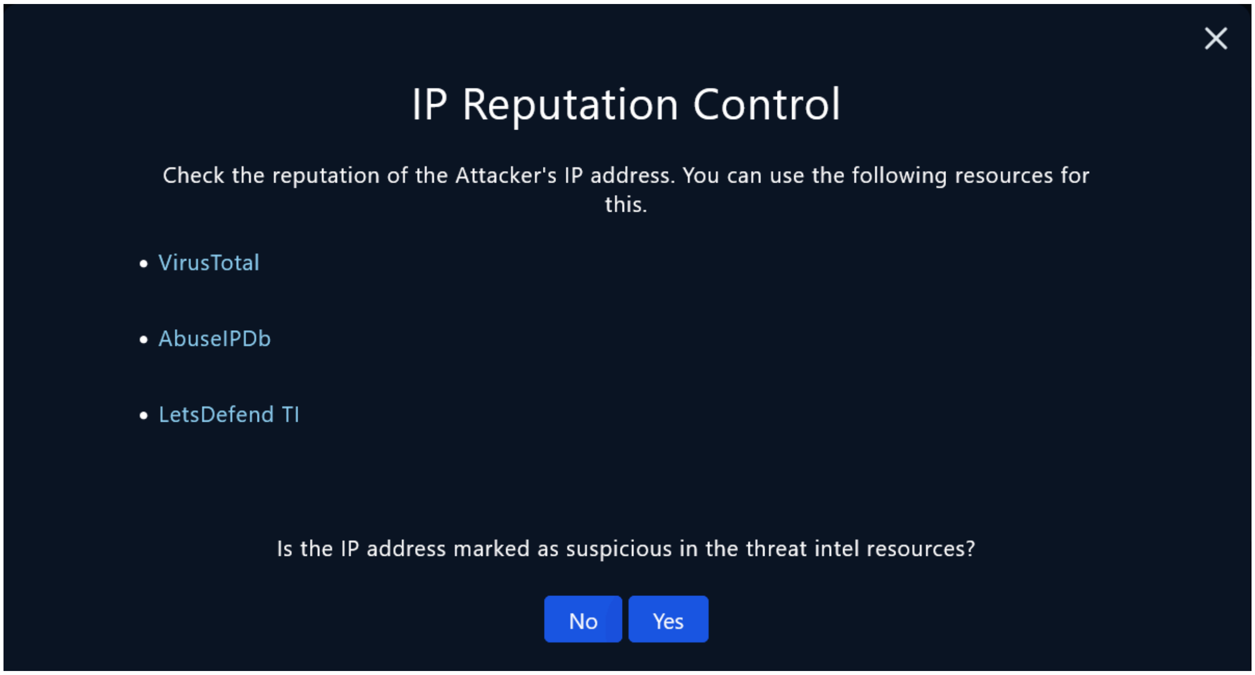
The alert details provide information about the source and destination IP addresses involved in the suspicious network traffic:

Source IP Address	218.92.0[.]56
Destination IP Address	172.16.17.148 (Matthew)

As seen in the alert details, source IP address 218.92.0[.]56 is **external** and may indicate a potential security threat. We can proceed with the next step of the playbook.

IP Reputation Control

The second step of the playbook recommends performing an IP reputation check of the attacker's IP address.



IP Reputation Control

Check the reputation of the Attacker's IP address. You can use the following resources for this.

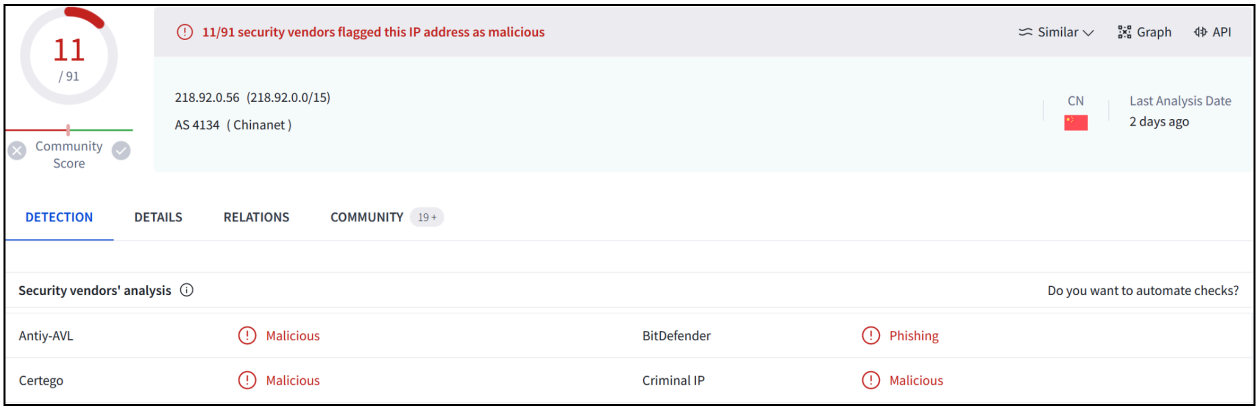
- VirusTotal
- AbuseIPDb
- LetsDefend TI

Is the IP address marked as suspicious in the threat intel resources?

This can be achieved by utilizing the following resources:

- VirusTotal
- AbuseIPDB
- LetsDefend TI

These platforms provide valuable insights into the reputation and history of IP addresses.
Based on the information provided by VirusTotal, the IP address originating from China has been flagged as malicious by 11 antivirus engines.



11/91 security vendors flagged this IP address as malicious

218.92.0.56 (218.92.0.0/15)
AS 4134 (Chinanet)

CN

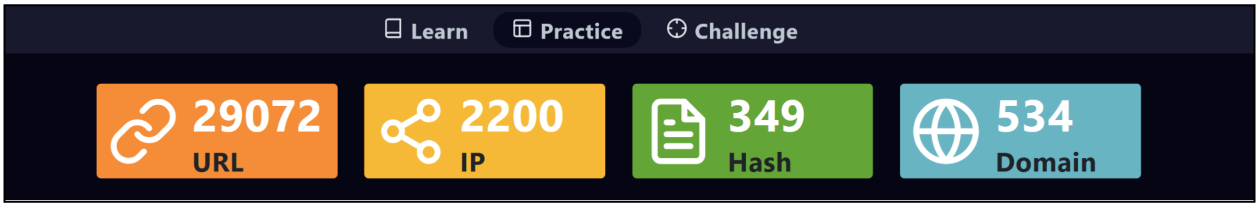
Last Analysis Date
2 days ago

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
Certego	Malicious	Criminal IP	Malicious

On the LetsDefend threat intel tab, you'll find a comprehensive database dedicated to cataloging maliciously used information, such as IP addresses, domains, and other indicators of compromise.



29072 URL

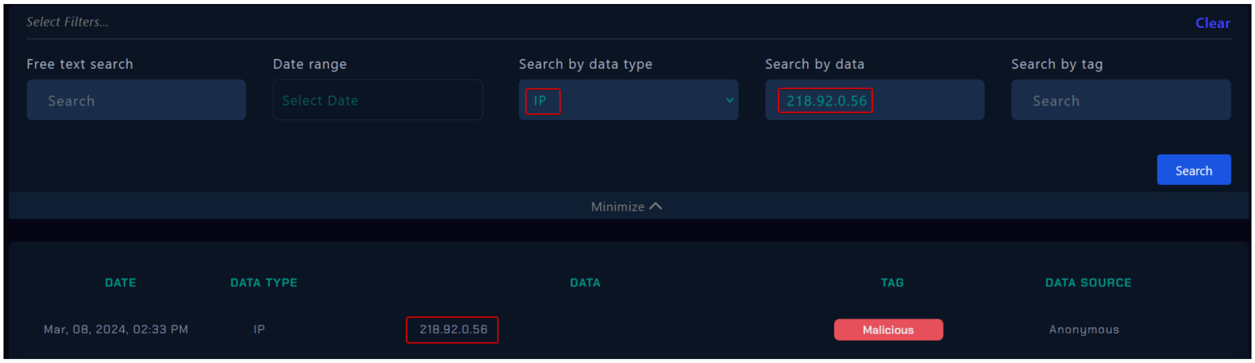
2200 IP

349 Hash

534 Domain

https://app.letsdefend.io/threath-intelligence-feed

Upon cross-referencing the source IP address mentioned in the alert with the Threat Intel tab, it was determined that the address had been categorized as malicious.



Free text search: Search

Date range: Select Date

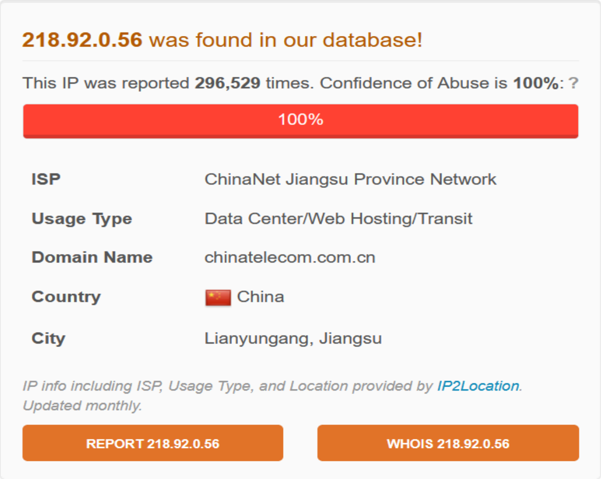
Search by data type: IP

Search by data: 218.92.0.56

Search by tag: Search

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Mar, 08, 2024, 02:33 PM	IP	218.92.0.56	Malicious	Anonymous

By cross-referencing the IP address with threat intelligence platforms such as Abuseip or Virustotal, we discovered that the IP address is malicious and reported many times.



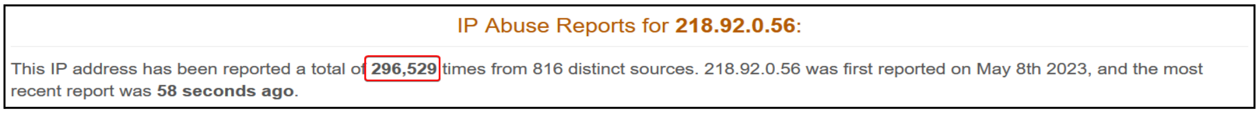
218.92.0.56 was found in our database!

This IP was reported **296,529** times. Confidence of Abuse is **100%**: ?

100%

ISP	ChinaNet Jiangsu Province Network
Usage Type	Data Center/Web Hosting/Transit
Domain Name	chinatelecom.com.cn
Country	China
City	Lianyungang, Jiangsu

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.



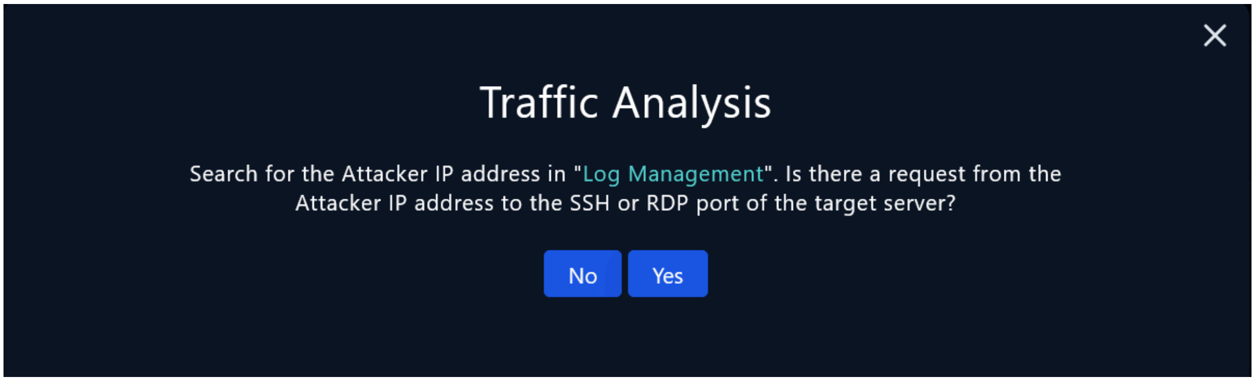
IP Abuse Reports for **218.92.0.56**:

This IP address has been reported a total of **296,529** times from 816 distinct sources. 218.92.0.56 was first reported on May 8th 2023, and the most recent report was **58 seconds ago**.

Analysis

Traffic Analysis

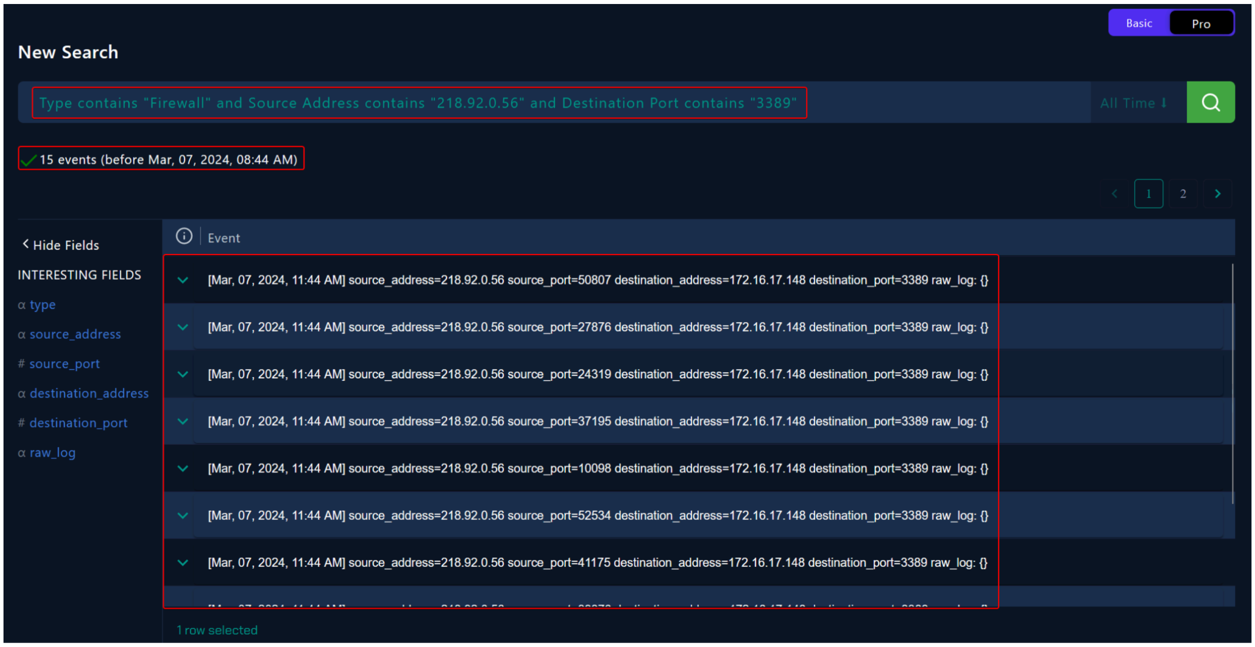
The third step of the playbook involves traffic analysis. Specifically, it suggests searching for the attacker's IP address within the log management system. From there, it's important to determine if there have been any requests to the server's SSH/RDP/VPN ports originating from the attacker's IP address.



Traffic Analysis

Search for the Attacker IP address in "Log Management". Is there a request from the Attacker IP address to the SSH or RDP port of the target server?

There are **15 firewall logs** recorded from the IP address 218.92.0[.]56 attempting to connect to the host named "**Matthew**" at IP address 172.16.17.148. These logs specifically detail attempts to access **port 3389**, commonly used for **Remote Desktop Protocol (RDP)** connections.

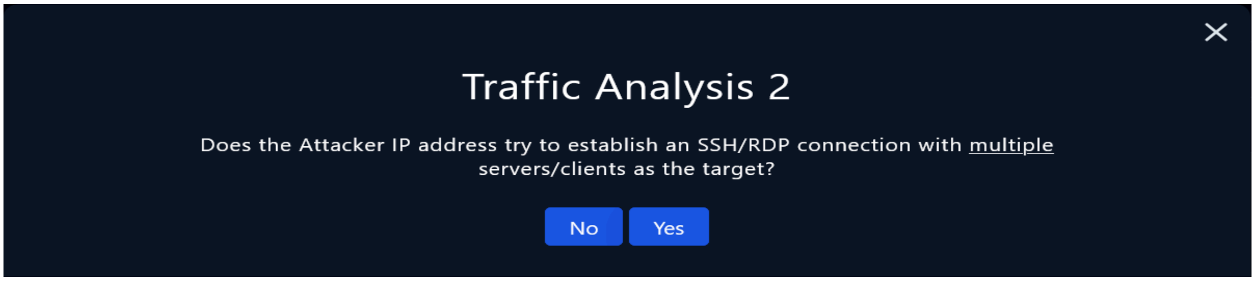


Type contains "Firewall" and Source Address contains "218.92.0.56" and Destination Port contains "3389"

15 events (before Mar, 07, 2024, 08:44 AM)

```
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=50807 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=27876 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=24319 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=37195 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=10098 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=52534 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=41175 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
```

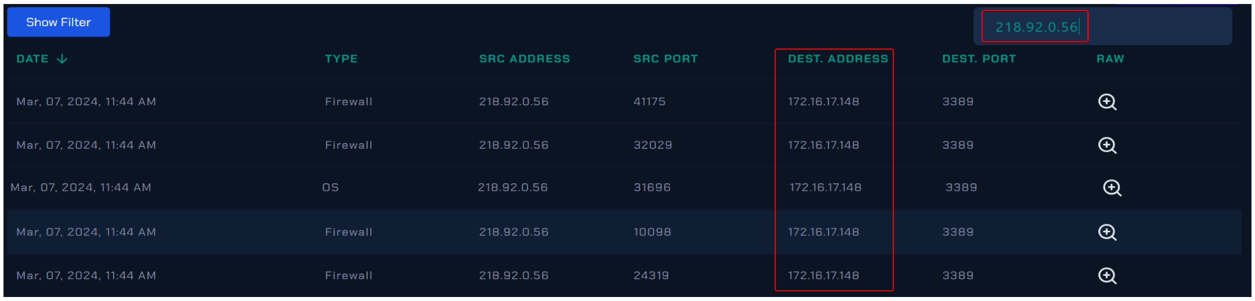
The next step in the playbook involves investigating whether the attacker's IP address has attempted to establish SSH/RDP connections with multiple servers or clients as the target. This step aims to determine if the attack is targeted toward a single specific server or if multiple servers or clients are being targeted simultaneously.



Traffic Analysis 2

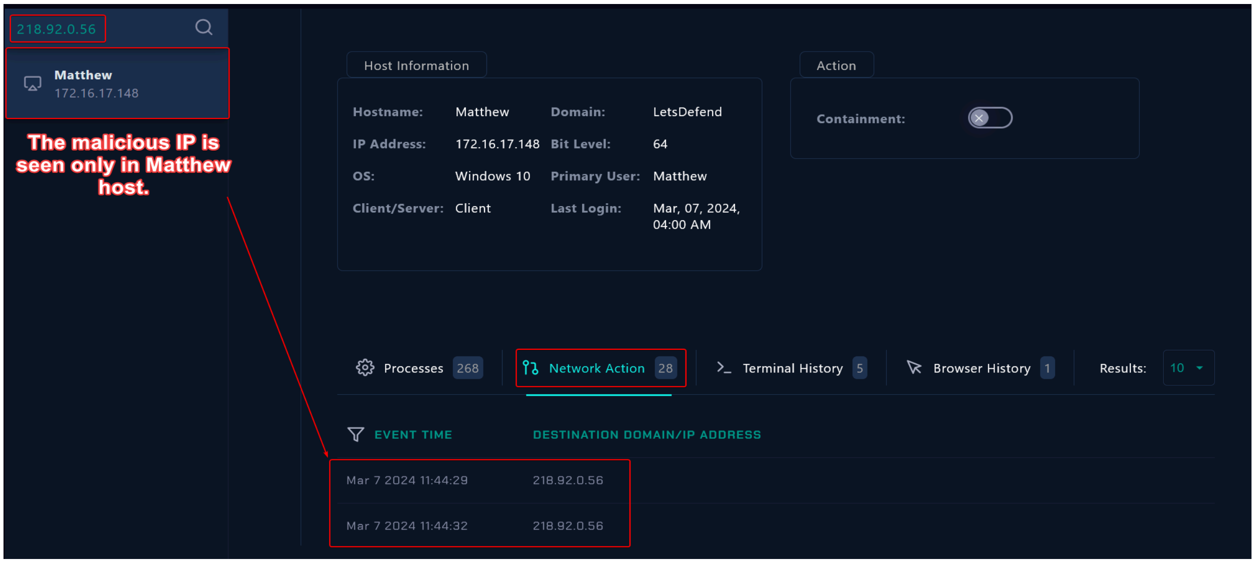
Does the Attacker IP address try to establish an SSH/RDP connection with multiple servers/clients as the target?

The answer is "**No**", only one client is targeted. Upon inspecting the log management and filtering for the attacker's source address, it reveals only one destination IP address, which is 172.16.17.148, corresponding to the host named "Matthew."



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	41175	172.16.17.148	3389	⊕
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	32029	172.16.17.148	3389	⊕
Mar, 07, 2024, 11:44 AM	OS	218.92.0.56	31696	172.16.17.148	3389	⊕
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	10098	172.16.17.148	3389	⊕
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	24319	172.16.17.148	3389	⊕

The Indicator of Compromise (IOC) is only detected in the network activities of the host machine named "Matthew."



Host Information

Hostname:	Matthew	Domain:	LetsDefend
IP Address:	172.16.17.148	Bit Level:	64
OS:	Windows 10	Primary User:	Matthew
Client/Server:	Client	Last Login:	Mar, 07, 2024, 04:00 AM

Action

Containment: ○

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Mar 7 2024 11:44:29	218.92.0.56
Mar 7 2024 11:44:32	218.92.0.56

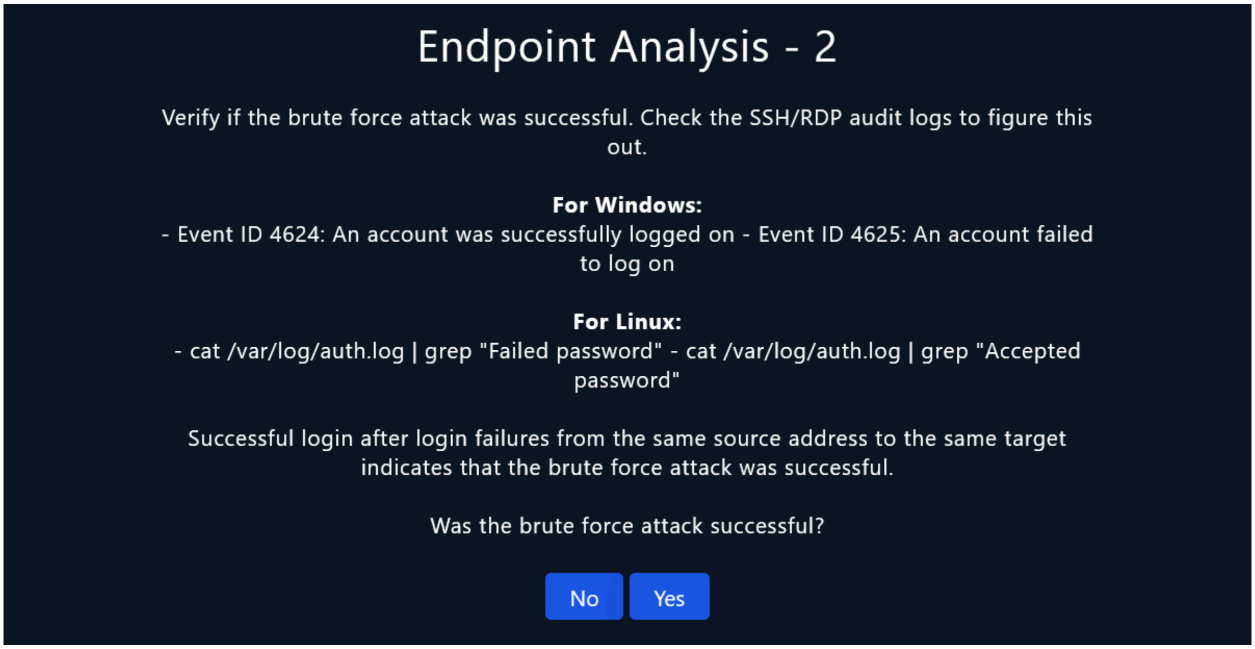
Endpoint Analysis

To determine if the brute force attack was successful, we need to analyze the SSH/RDP audit logs. Here's how to do it for both Windows and Linux systems:

For Windows:

- Look for Event ID 4624, which indicates a successful login.
- Also, examine Event ID 4625, which signifies a failed login attempt.

If successful logins are recorded after multiple failed login attempts from the same source address to the same target, it indicates that the brute force attack was successful.



Endpoint Analysis - 2

Verify if the brute force attack was successful. Check the SSH/RDP audit logs to figure this out.

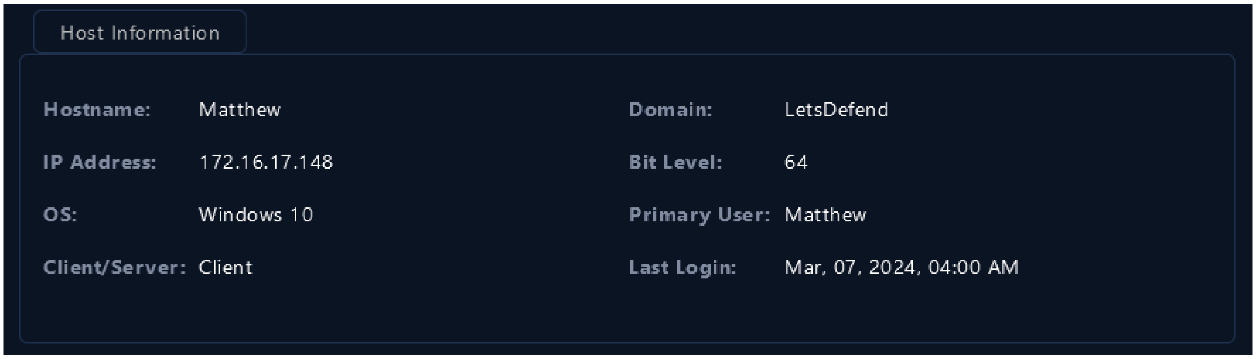
For Windows:
- Event ID 4624: An account was successfully logged on - Event ID 4625: An account failed to log on

For Linux:
- cat /var/log/auth.log | grep "Failed password" - cat /var/log/auth.log | grep "Accepted password"

Successful login after login failures from the same source address to the same target indicates that the brute force attack was successful.

Was the brute force attack successful?

By searching the host's IP address on the Endpoint Security we can access the host.

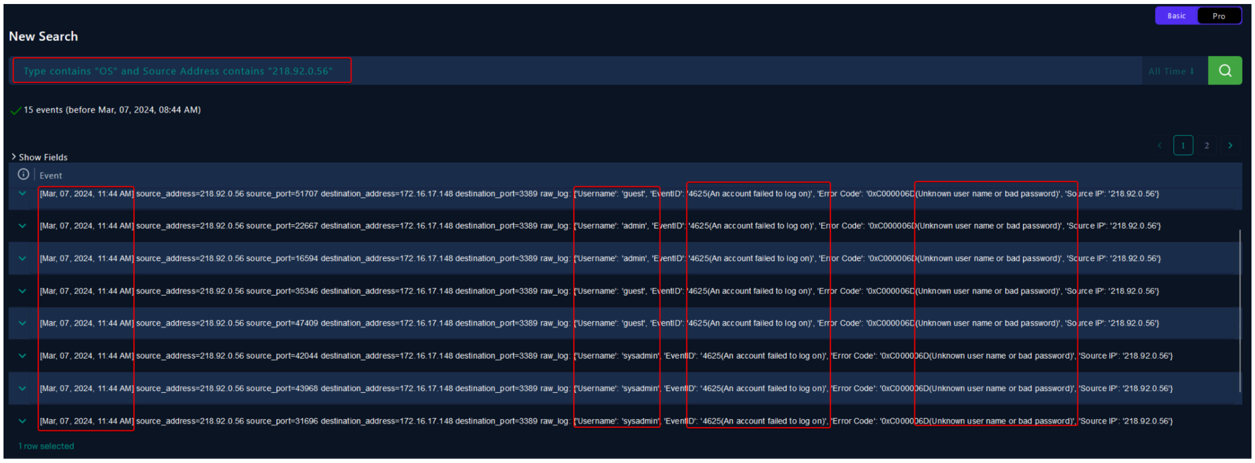


Host Information

Hostname:	Matthew	Domain:	LetsDefend
IP Address:	172.16.17.148	Bit Level:	64
OS:	Windows 10	Primary User:	Matthew
Client/Server:	Client	Last Login:	Mar, 07, 2024, 04:00 AM

On March 7, 2024, at 11:44 AM, several failed logon events were observed.

- Several failed logon events observed
- Usernames attempted: "sysadmin," "admin," "guest"
- Event ID: 4625 (An account failed to log on)
- Error Code: 0xC000006D (Unknown user name or bad password)



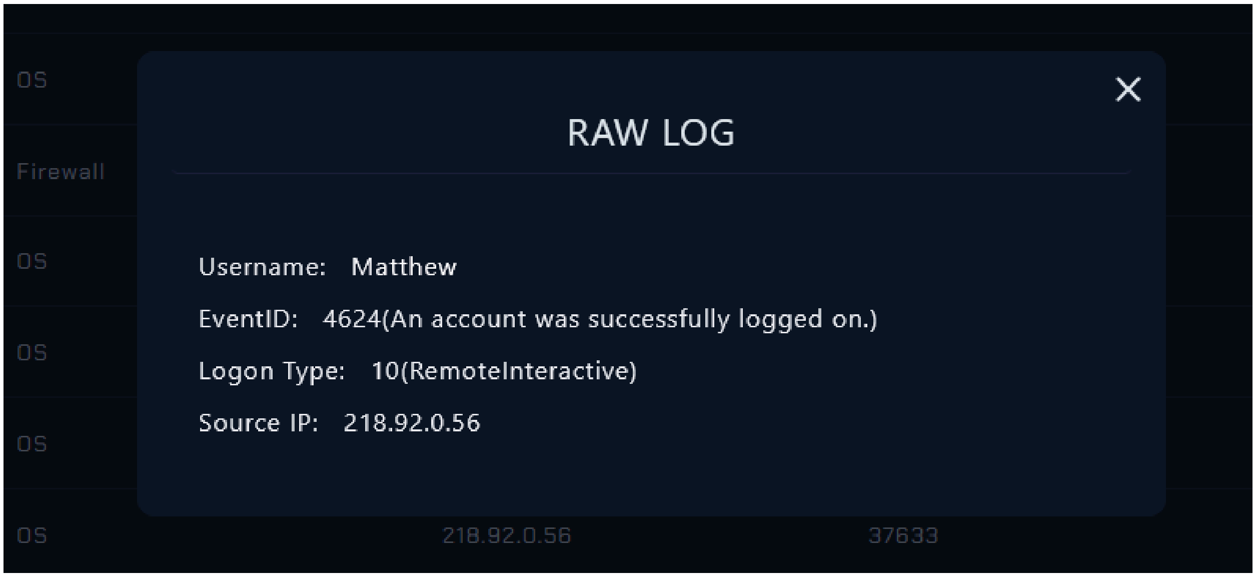
```
Type contains "OS" and Source Address contains "218.92.0.56"
```

15 events (before Mar, 07, 2024, 08:44 AM)

```
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=51707 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'guest', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=22667 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'admin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=16594 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'admin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=35346 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'guest', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=47409 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'guest', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=42044 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'sysadmin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=43968 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'sysadmin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=31696 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'sysadmin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or bad password)', 'Source IP': '218.92.0.56'}
```

1 row selected

These failed logon attempts indicate potential unauthorized access attempts or a brute force attack targeting the system. The use of generic usernames like "sysadmin," "admin," and "guest" suggests an attempt to exploit common account names.



RAW LOG

Username: Matthew

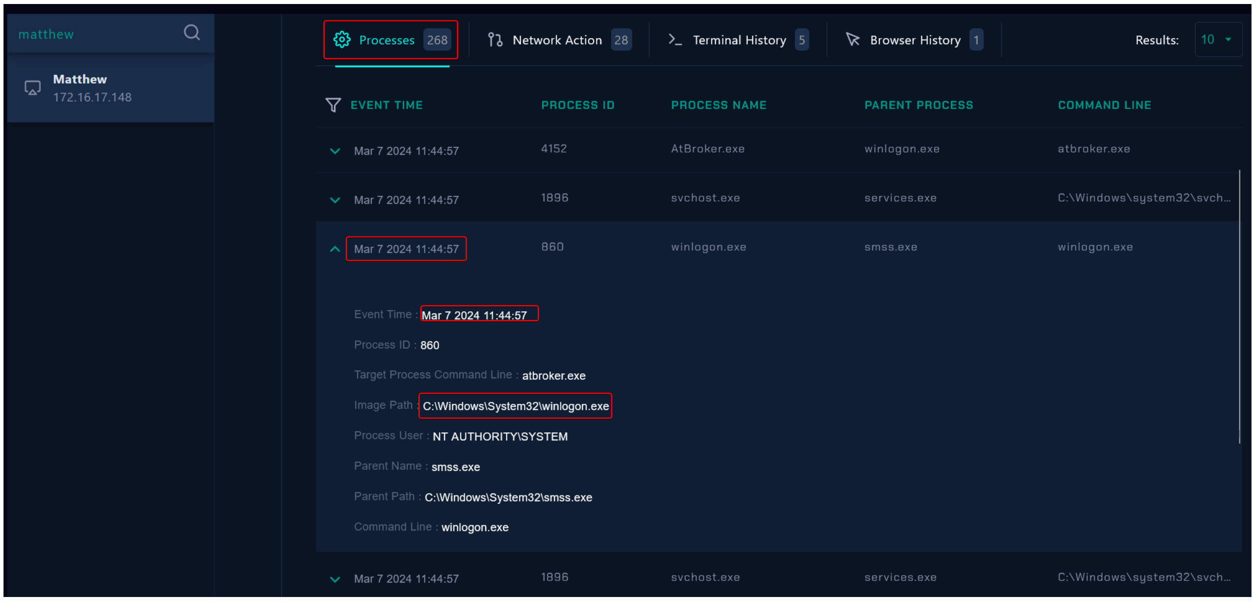
EventID: 4624(An account was successfully logged on.)

Logon Type: 10(RemoteInteractive)

Source IP: 218.92.0.56

Following numerous failed logon attempts, the attacker successfully accessed the host using the username "Matthew."

After the checking processes on the Matthew host through Endpoint security on March 7, 2024, 11:44:57, we observed the Winlogon.exe process, which correlates with the 4624 successful logon identified in the log management system.



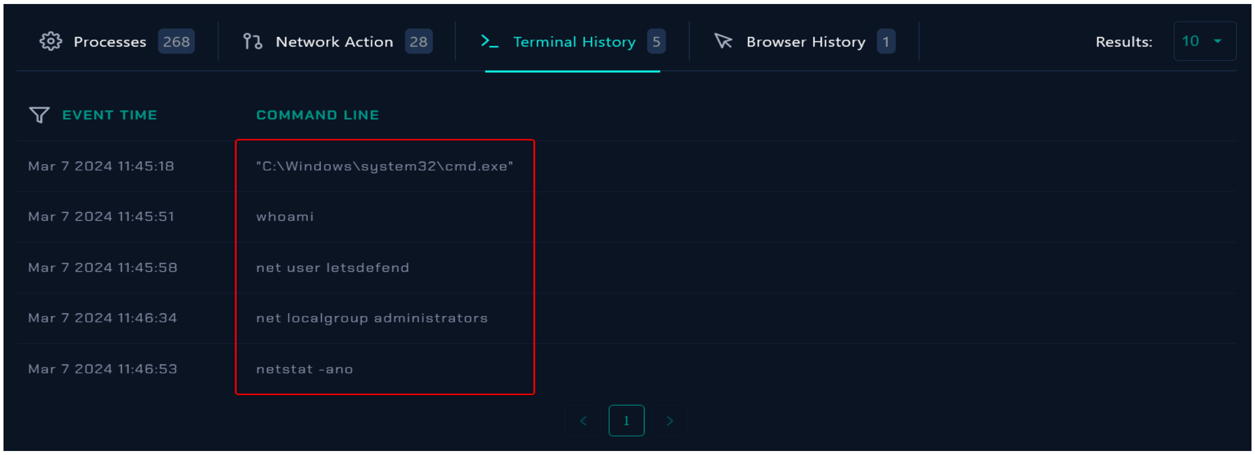
EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
Mar 7 2024 11:44:57	4152	AtBroker.exe	winlogon.exe	atbroker.exe
Mar 7 2024 11:44:57	1896	svchost.exe	services.exe	C:\Windows\system32\svch...
Mar 7 2024 11:44:57	860	winlogon.exe	smss.exe	winlogon.exe
Mar 7 2024 11:44:57	1896	svchost.exe	services.exe	C:\Windows\system32\svch...

Event Time : Mar 7 2024 11:44:57
Process ID : 860
Target Process Command Line : atbroker.exe
Image Path : C:\Windows\System32\winlogon.exe
Process User : NT AUTHORITY\SYSTEM
Parent Name : smss.exe
Parent Path : C:\Windows\System32\smss.exe
Command Line : winlogon.exe

After the successful logon, the attacker executed the following commands on the host.

- March 7, 2024, 11:45:18
  - Command: "C:\Windows\system32\cmd.exe"
  - Command: whoami
  - Command: net user letsdefend
  - Command: net localgroup administrators
  - Command: netstat -ano

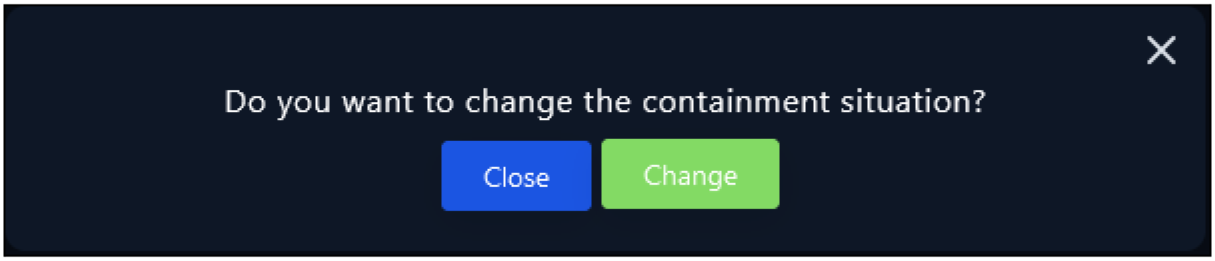
These commands indicate the attacker's attempt to gain information about the system, users, and network connections, potentially for further malicious activities.



EVENT TIME	COMMAND LINE
Mar 7 2024 11:45:18	"C:\Windows\system32\cmd.exe"
Mar 7 2024 11:45:51	whoami
Mar 7 2024 11:45:58	net user letsdefend
Mar 7 2024 11:46:34	net localgroup administrators
Mar 7 2024 11:46:53	netstat -ano

Containment

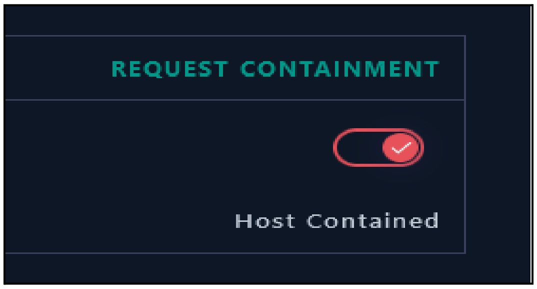
Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Do you want to change the containment situation?

Isolation of the host can be made from the endpoint security tab.

Hostname	Matthew
IP Address	172.16.17.148



REQUEST CONTAINMENT

Host Contained

After the containment, we can close the alert from the investigation channel.

Summary

The alert report highlights the detection of a suspicious web attack targeting the host named Matthew (IP: 172.16.17.148). The attack was triggered by the SOC176 - RDP Brute Force Detected rule, indicating a potential vulnerability that threat actors exploit to gain unauthorized access to machines via RDP (Remote Desktop Protocol).

The report outlines a series of suspicious activities targeting a host named "Matthew" with the IP address 172.16.17.148. The incident was triggered by the SOC176 rule for RDP Brute Force Detection, highlighting repeated login failures from the external source IP address 218.92.0[.]56.

Upon investigation, it was discovered that the source IP address had a malicious reputation according to multiple threat intelligence platforms, indicating potential security risks. Additionally, 15 firewall logs recorded attempts to connect to the host "Matthew" over RDP, suggesting a concerted effort to gain unauthorized access.

Despite failed login attempts, the attacker successfully logged in using the username "Matthew." Subsequent analysis revealed a series of command executions, including attempts to gather system information and escalate privileges.

Lesson Learned

- Effective monitoring and alerting systems are essential for detecting and responding to suspicious activities promptly.

- Monitoring for specific indicators of compromise (IOCs) helps detect potential security threats, but they should be supplemented with in-depth analysis.

- Rapid response to security incidents is critical for minimizing the impact of cyber threats.

- Educating users and administrators about common attack vectors, such as brute force attacks, helps mitigate risks associated with unauthorized access attempts.

- Enabling and collecting logs from operating systems can significantly enhance visibility into your network's security posture.

Remediation Actions

- Enforce strong password policies, including the use of complex passwords and regular password changes, to mitigate the risk of brute force attacks. Consider implementing multi-factor authentication (MFA) for an added layer of security.

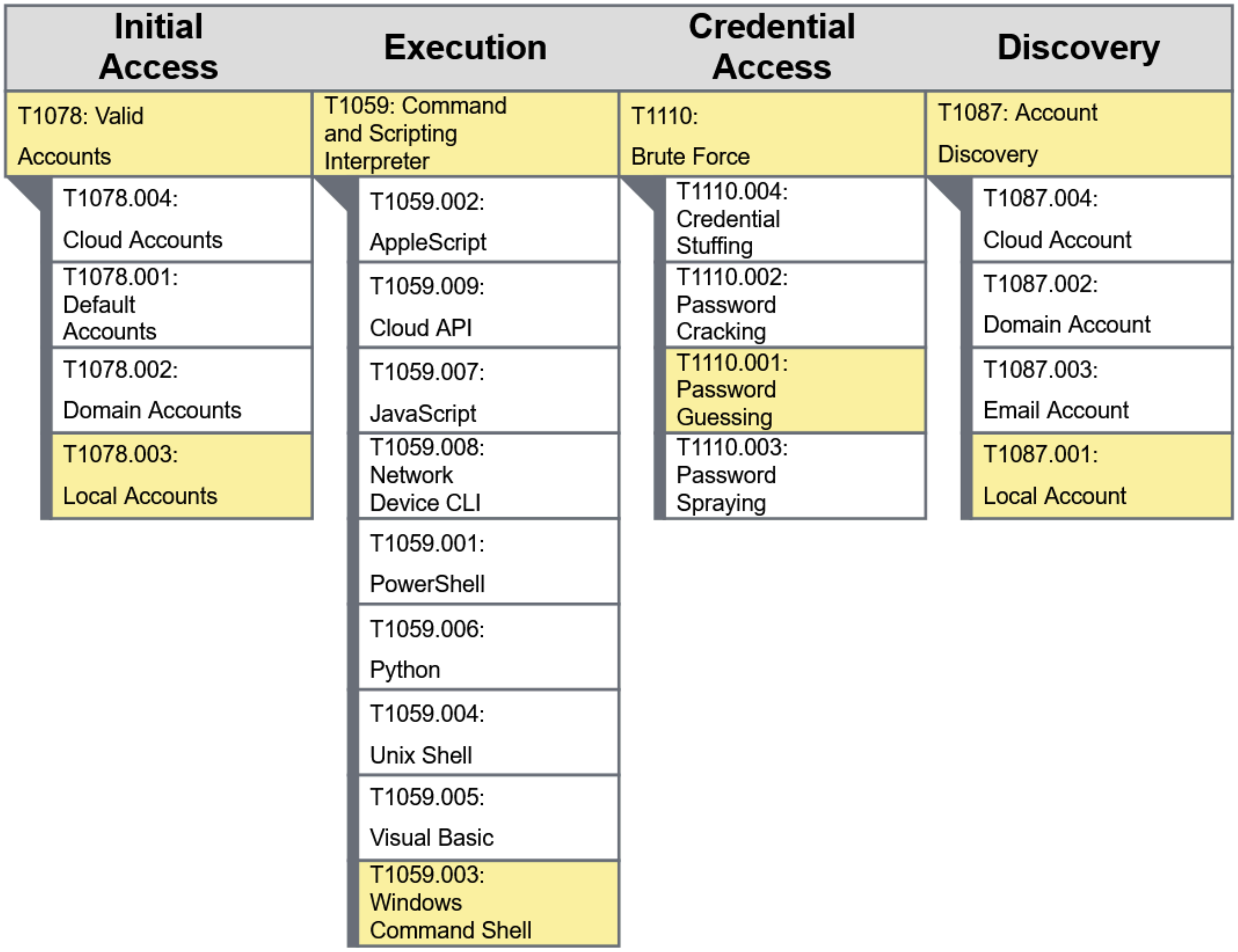
- Restrict external network access to Matthew and Server instances accessible via the public internet, until the necessary upgrades can be performed

- Set up a VPN solution to provide secure remote access to the network. VPNs encrypt data transmitted between remote devices and the network, reducing the risk of interception or unauthorized access.

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

Appendix

MITRE ATT&CK



Initial Access	Execution	Credential Access	Discovery
T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1110: Brute Force	T1087: Account Discovery
T1078.004: Cloud Accounts	T1059.002: AppleScript	T1110.004: Credential Stuffing	T1087.004: Cloud Account
T1078.001: Default Accounts	T1059.009: Cloud API	T1110.002: Password Cracking	T1087.002: Domain Account
T1078.002: Domain Accounts	T1059.007: JavaScript	T1110.001: Password Guessing	T1087.003: Email Account
T1078.003: Local Accounts	T1059.008: Network Device CLI	T1110.003: Password Spraying	T1087.001: Local Account
	T1059.001: PowerShell		
	T1059.006: Python		
	T1059.004: Unix Shell		
	T1059.005: Visual Basic		
	T1059.003: Windows Command Shell		

MITRE Tactics	MITRE Techniques
Initial Access	T1078: Valid Accounts
Discovery	T1087: Account Discovery
Execution	T1059: Command and Scripting Interpreter
Credential Access	T1110: Brute Force
Discovery	T1087: Account Discovery

Artifacts

IOC TYPE	VALUE
IPv4	218.92.0[.]56
Username	admin
Username	guest
Username	sysadmin
Username	Matthew