EventID@234- SOC176 - RDP Brute Force Detected

1. Alert Overview

- **Event ID:** 234
- **Alert Time:** March 07, 2024 — 11:44 AM
- **Alert Rule:** SOC176 – RDP Brute Force Detected
- **Alert Level:** Security Analyst
- **Source IP:** 218[.]92[.]0[.]56
- **Destination IP:** 172[.]16[.]17[.]148
- **Destination Host:** Matthew
- **Protocol:** RDP (Port 3389)
- **Firewall Action:** Allowed
- **Alert Trigger Reason:** Login failure from a single source with different non-existing accounts

EventID :	234
Event Time :	Mar, 07, 2024, 11:44 AM
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
Show Hint	

---

2. Alert Summary

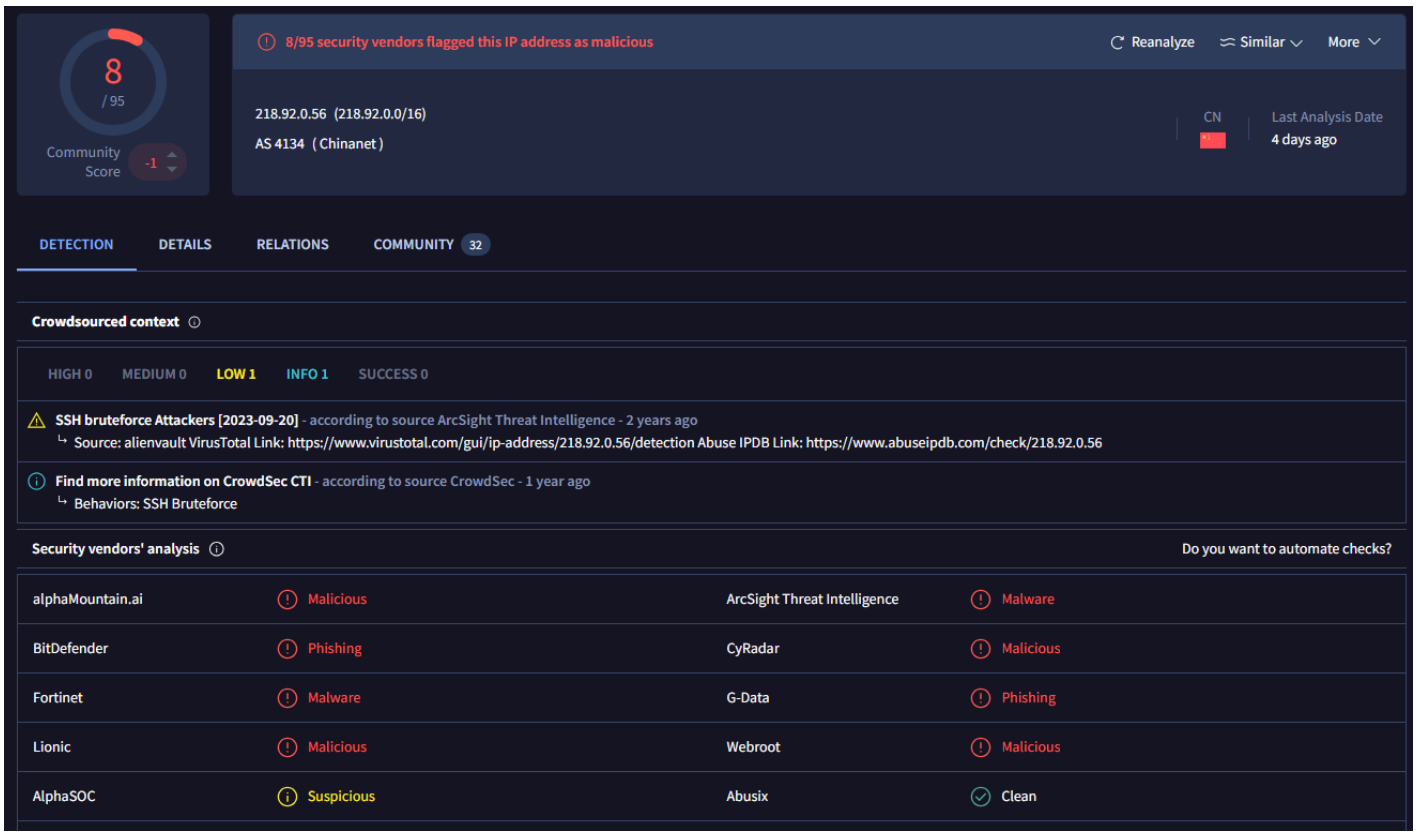
This alert indicates repeated failed RDP login attempts from a single IP address `218[.]92[.]0[.]56` to the internal host `Matthew` with IP Address `172[.]16[.]17[.]148`.
This behavior suggested that the attacker was attempting to gain unauthorized access through commonly used credentials to gain unauthorized access.

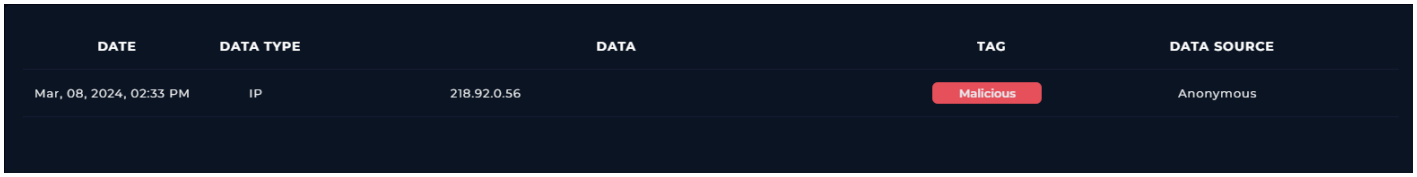
---

3. Investigation Steps

Source Validation

- The external source IP address 218[.]92[.]0[.]56 indicates a potential security threat on the network.

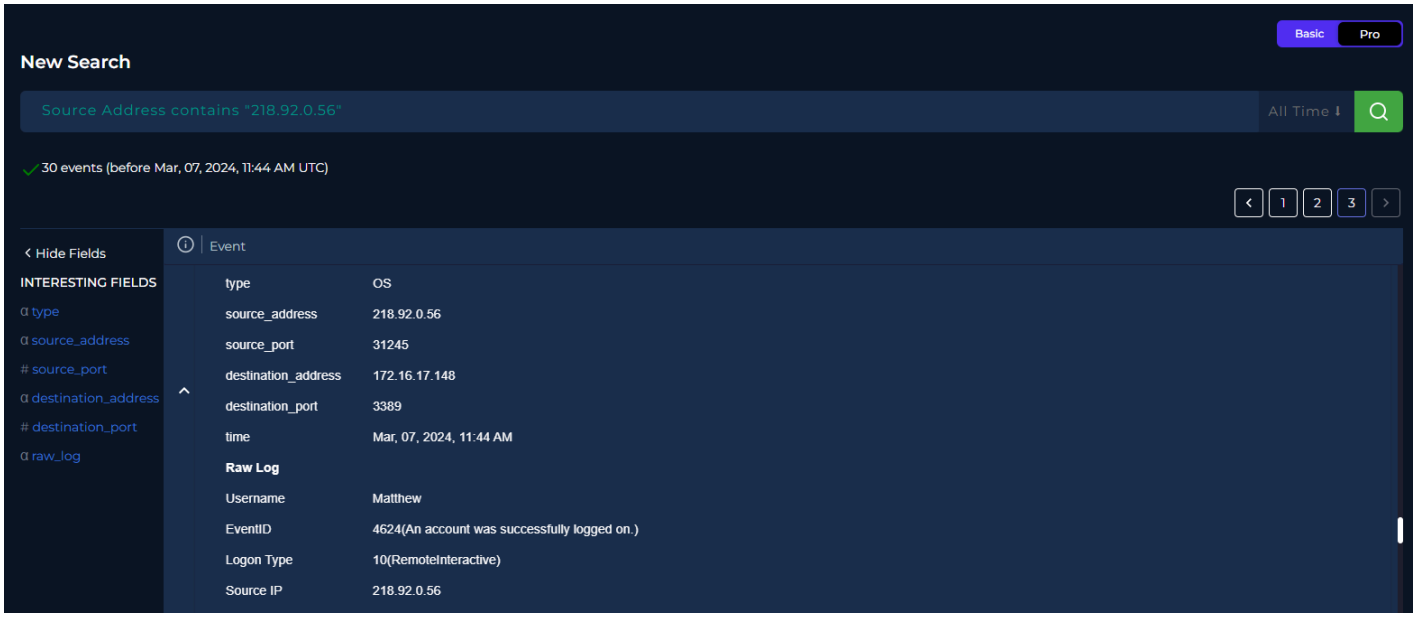




DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Mar, 08, 2024, 02:33 PM	IP	218.92.0.56	Malicious	Anonymous

Log Correlation

- 15 login attempts from 218[.]92[.]0[.]56 to `172[.]16[.]17[.]148` with host named `Mathew` to port 3389.
- There was detected both failed and successful login events:
- This indicates a successful brute force attack.

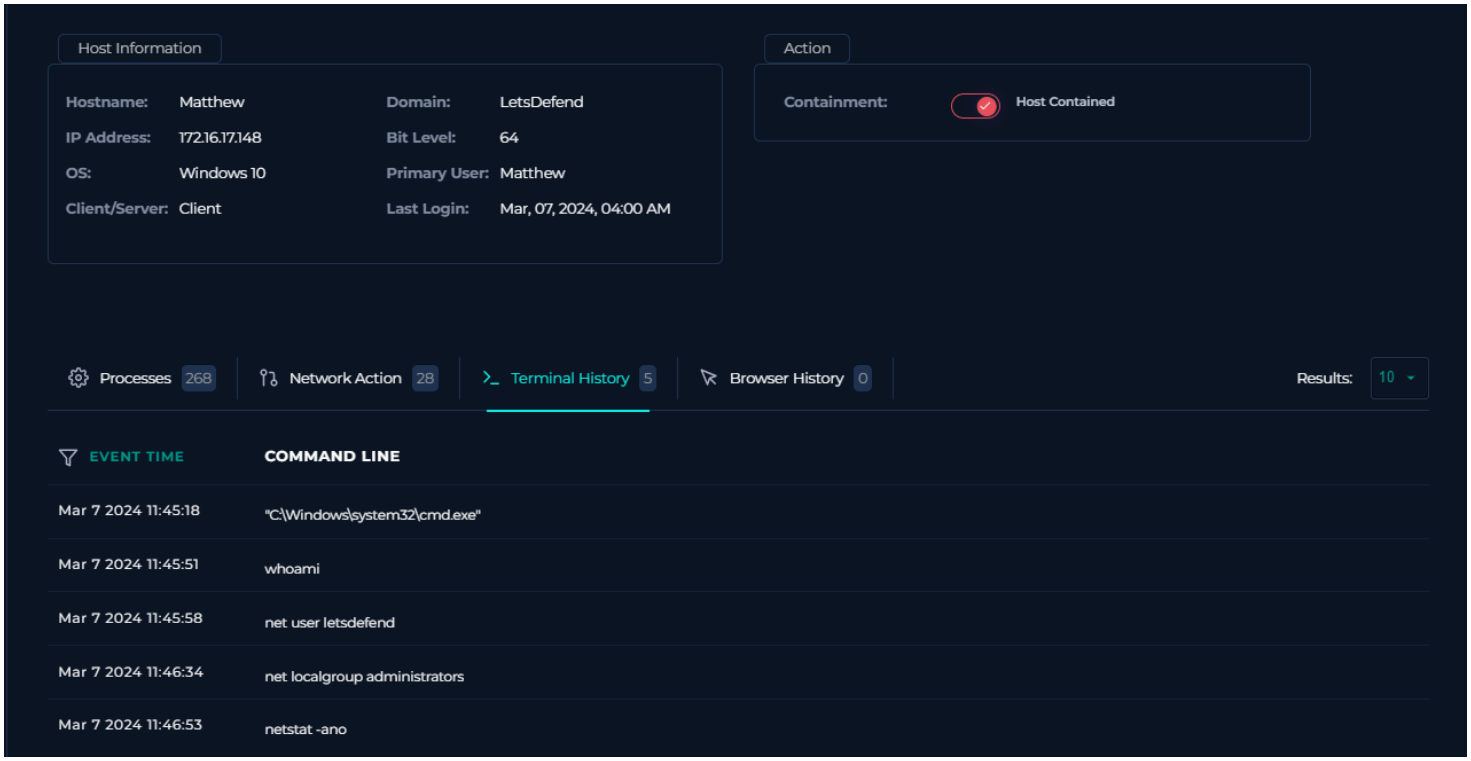


Endpoint Analysis

- Endpoint logs shows that commands was executed after successful login event.

```
C:\Windows\system32\cmd.exe
whoami
net user letsdefend
```

```
net localgroup administrators
netstat -ano
```



- This indicates post-compromise reconnaissance activity.

4. Investigation Artifacts

- 218[.]92[.]0[.]56 - Source IP Address
- 172[.]16[.]17[.]148 - Destination IP Address
- Matthew - Destination Hostname

---

5. Response & Remediations

Immediate Action

- **Action:** Isolated affected host (`Matthew`) from the network.
- **Reason:** Prevent lateral movement and data exfiltration.
- **Firewall:** Source IP blocked at the perimeter firewall.
  Recommended Next Step
- Reset and secure the compromise user account(**Matthew**).
- Enforce strong password policies.
- Implement Multi-Factor Authentication (MFA) for RDP access.
- Restrict RDP access to trusted VPN users or internal network only.
- Conduct full endpoints scan for persistence mechanisms and malicious binaries.
- Review other hosts for failed RDP login attempts from the same source.

---

8. MITRE ATT&CK Mapping

Tactic	Technique ID	Technique	Evidence
Initial Access	T1110	Brute Force	Multiple 4625 failures
Execution	T1059	Command-Line Interface	`cmd.exe` execution
Discovery	T1082	System Information Discovery	`whoami`, `net user`
Lateral Movement	T1021	Remote Services (RDP)	RDP login success

---

7. Lessons Learned

- Exposed RDP ports remain a major entry vector for brute-force attacks.
- Lack of MFA and weak credential hygiene were key enabling factors.
- IP reputation checks can rapidly validate external threats.
- Regular auditing and log monitoring are crucial to detect brute-force behavior early.
