Suspicious Activity Detected: Failed Logins, Malware Events, Connection attempts

16/9/25 09:22 AM

Rahul Salaria

Splunk(Free Trial) – SOC\_Task2\_Sample\_Logs

The SIEM detected failed login attempts ,malware activity and connection attempts across user accounts , The report summarizes the host , source IPs, severity levels and recommended remediation

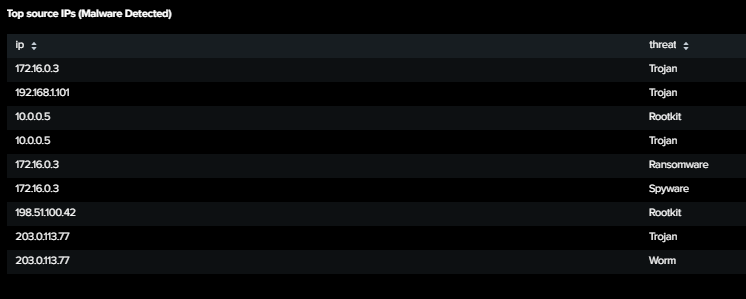
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TIME | USER | IP | ACTIONS | SEVERITY |
| 04:23:14 | charlie | 198.51.100.42 | Login failed | LOW |
| 04:23:14 | Bob | 172.16.0.3 | Login failed | MID |
| 04:47:14 | Bob | 10.0.0.5 | Login failed | MID |
| 7:45:14 | Charlie/bob(2 user from same IP) | 172.16.0.3 | Malware detected/Trojan detected | High/ multiple attack |
| 7:15:14 | Eve/Bob(2 user from same ip) | 10.0.0.5 | Malware detected/Rootkit signature | High |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 07:44:14 | Bob/charlie | 203.0.113.77/192.168.1.101 | Connection attempt | High |
| 08:21:14 | david | 172.16.0.3 | Connection attempt | MID |
|  |  |  |  |  |

1)Repeated failed login attempt from same user name but different IP

2)multiple malware detection from same IP-172.16.0.3, 10.0.0.5

3)Unusual connection attempts from same user but different Ips



\*Multiple failed logins were observed from user bob from different Ips, malware detected were observed on IP 172.16.0.3 and IP 10.0.0.5- indicating potential compromise

Remediations:

For login failures:

1. Enable multi factor authentications for all accounts
2. Notify user of suspicious login failures
3. Try suggestion of password change

For malware detected:

1. Isolate affected endpoints
2. Add updates to OS and applications
3. Run full malware scan

For connection attempt:

1. Block suspicious source Ips at firewall/Ips
2. Deploy IPS/IDS
3. Review VPN/remote access logs

