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

16/9/25 09:22 AM

Rahul Salaria

Splunk(Free Trial) – SOC_Task2_Sample_Logs

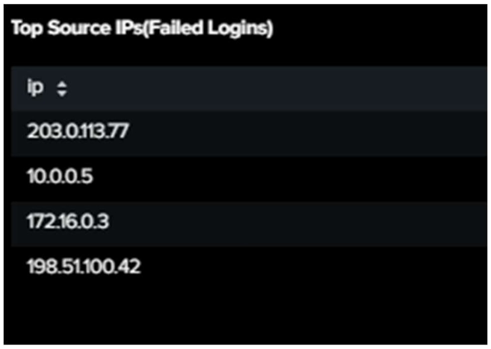
The SIEM detected failed login attempts ,malware activity and connection attempts across user accounts , The report summarizes the host , source IPs, severity levels and recommended remediation

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

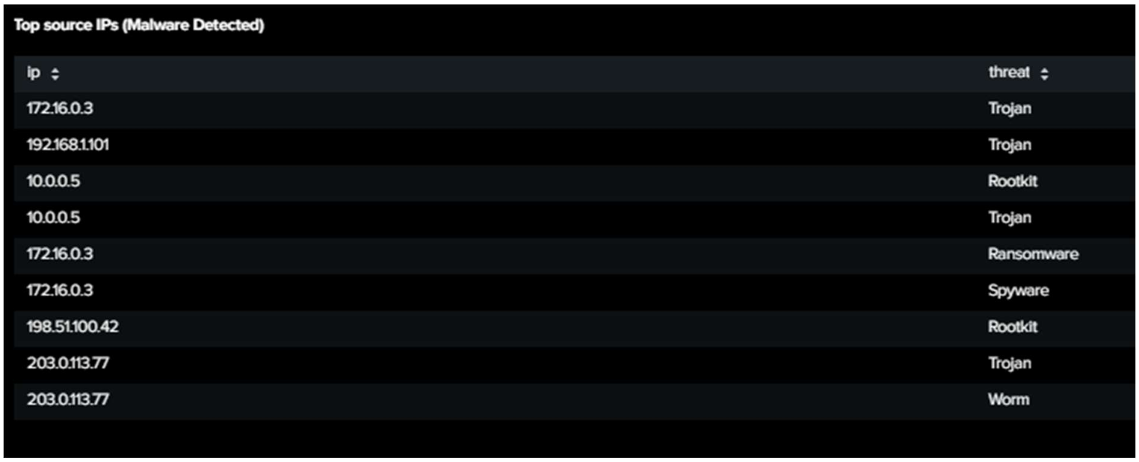
2)multiple malware detection from same IP-172.16.0.3, 10.0.0.5

3)Unusual connection attempts from same user but different Ips



Top Source IPs(Failed Logins)

ip
203.0.113.77
10.0.0.5
172.16.0.3
198.51.100.42



Top source IPs (Malware Detected)

ip	threat
172.16.0.3	Trojan
192.168.1.101	Trojan
10.0.0.5	Rootkit
10.0.0.5	Trojan
172.16.0.3	Ransomware
172.16.0.3	Spyware
198.51.100.42	Rootkit
203.0.113.77	Trojan
203.0.113.77	Worm

*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) Require Password rest for impacted accounts

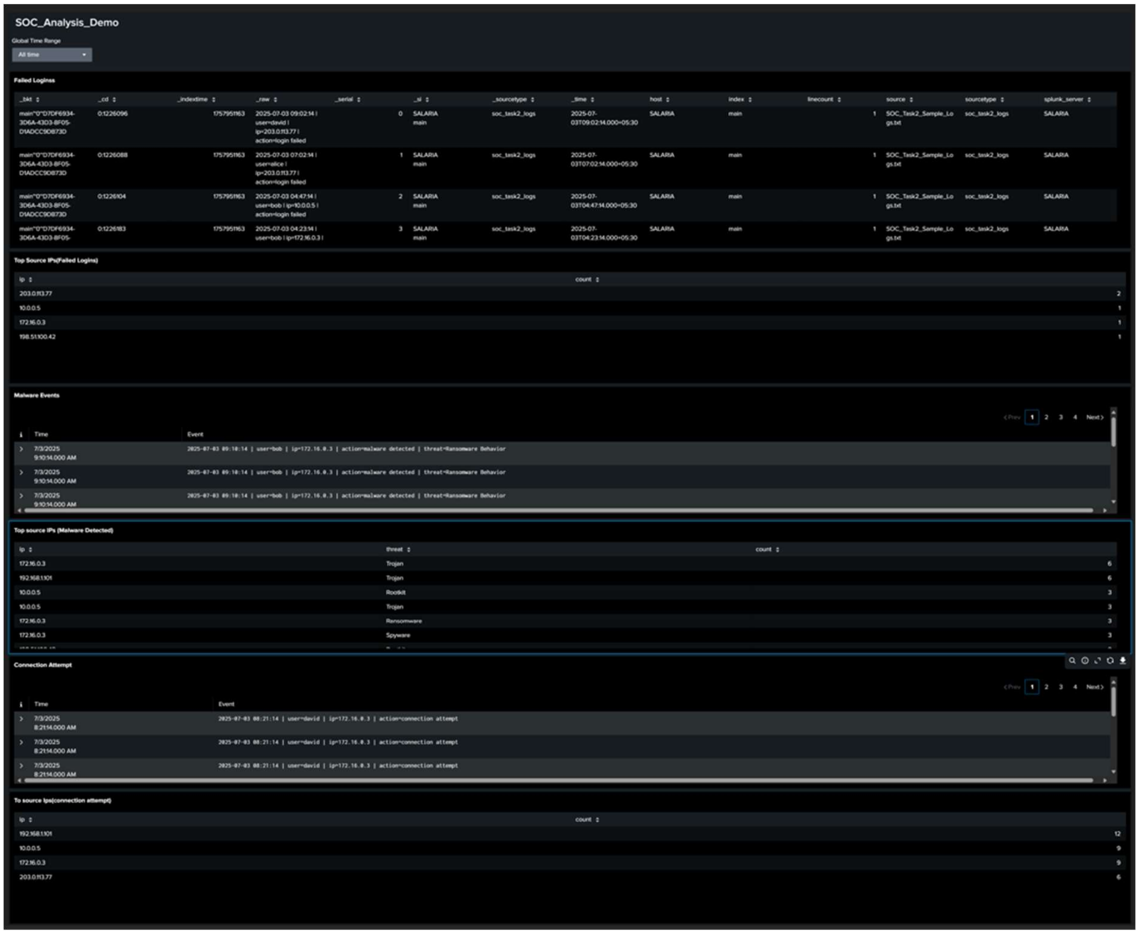
For malware detected:

1) Isolate infected 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



SOC_Analysis_Demo

Global Time Range: All time

Failed Logins

_bkt	_cd	_indextime	_raw	_serial	_si	_sourcetype	_time	host	index	linecount	source	sourcetype	splunk_server
main~0~D7DF6934-306A-43D3-8F05-D1ADCC9DB73D	0:1226096	1757951163	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed	0	SALARIA main	soc_task2_logs	2025-07-03T09:02:14.000+05:30	SALARIA	main	1	SOC_Task2_Sample_Logs.txt	soc_task2_logs	SALARIA
main~0~D7DF6934-306A-43D3-8F05-D1ADCC9DB73D	0:1226088	1757951163	2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed	1	SALARIA main	soc_task2_logs	2025-07-03T07:02:14.000+05:30	SALARIA	main	1	SOC_Task2_Sample_Logs.txt	soc_task2_logs	SALARIA
main~0~D7DF6934-306A-43D3-8F05-D1ADCC9DB73D	0:1226104	1757951163	2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed	2	SALARIA main	soc_task2_logs	2025-07-03T04:47:14.000+05:30	SALARIA	main	1	SOC_Task2_Sample_Logs.txt	soc_task2_logs	SALARIA
main~0~D7DF6934-306A-43D3-8F05-	0:1226183	1757951163	2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 |	3	SALARIA main	soc_task2_logs	2025-07-03T04:23:14.000+05:30	SALARIA	main	1	SOC_Task2_Sample_Logs.txt	soc_task2_logs	SALARIA

Top Source IPs(Failed Logins)

ip	count
203.0.113.77	2
10.0.0.5	1
172.16.0.3	1
198.51.100.42	1

Malware Events

i	Time	Event
›	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
›	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
›	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior

Top source IPs (Malware Detected)

ip	threat	count
172.16.0.3	Trojan	6
192.168.1.101	Trojan	6
10.0.0.5	Rootkit	3
10.0.0.5	Trojan	3
172.16.0.3	Ransomware	3
172.16.0.3	Spyware	3

Connection Attempt

i	Time	Event
›	7/3/2025 8:21:14.000 AM	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
›	7/3/2025 8:21:14.000 AM	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
›	7/3/2025 8:21:14.000 AM	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt

To source Ips(connection attempt)

ip	count
192.168.1.101	12
10.0.0.5	9
172.16.0.3	9
203.0.113.77	6