SOC_Analysis_Demo

Global Time Range

All time

Failed Loginss

_bkt	_cd	_indextime	_raw	_serial	_si	_sourcetype	_time	host	index	linecount	source	sourcetype	splunk_server
main~0~D7DF6934-3D6A-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~D7DF6934-3D6A-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~D7DF6934-3D6A-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~D7DF6934-3D6A-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

< Prev 1 2 3 4 Next >

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

Top source IPs (Malware Detected)

10.0.0.5	Rootkit	3
10.0.0.5	Trojan	3
172.16.0.3	Ransomware	3
172.16.0.3	Spyware	3
198.51.100.42	Rootkit	3
203.0.113.77	Trojan	3
203.0.113.77	Worm	3

Connection Attempt

< Prev 1 2 3 4 Next >

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