
malware alert report

malware attack detecting while SOC monitoring using splunk

Time	Event
2025-07-03T09:10:14-0500	2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior
2025-07-03T07:51:14-0500	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature
2025-07-03T07:45:14-0500	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected
2025-07-03T05:48:14-0500	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected
2025-07-03T05:45:14-0500	2025-07-03 05:45:14 user=david ip=172.16.0.3 action=malware detected threat=Trojan Detected
2025-07-03T05:42:14-0500	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected
2025-07-03T05:30:14-0500	2025-07-03 05:30:14 user=eve ip=192.168.1.101 action=malware detected threat=Trojan Detected
2025-07-03T05:06:14-0500	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt
2025-07-03T04:41:14-0500	2025-07-03 04:41:14 user=alice ip=172.16.0.3 action=malware detected threat=Spyware Alert
2025-07-03T04:29:14-0500	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected
2025-07-03T04:19:14-0500	2025-07-03 04:19:14 user=alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature