Incident Response Report

Identify 3–5 Suspicious Alerts from Logs

Suspicious Alerts Identified

Alert No.	Event	Reason
1	Malware detected – Ransomware Behavior	Critical threat
2	Malware detected – Trojan Detected	System compromise
3	Multiple login failed attempts	Possible brute-force

Alerts categorized (High / Medium / Low)

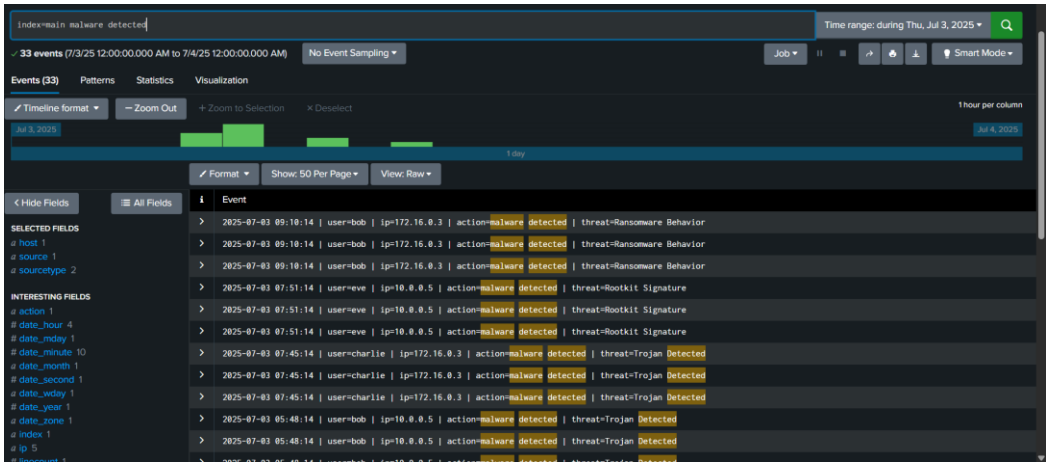
Severity Classification Table

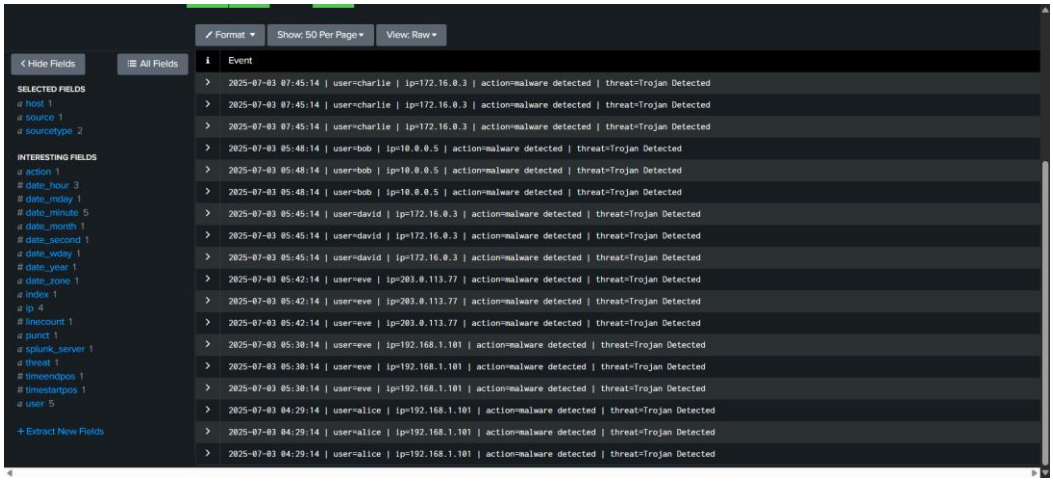
Severity	Alert Type	Action Required
High	Malware, Ransomware, Rootkit	Immediate response
Medium	Failed logins, suspicious IPs	Investigate
Low	Login success, file access	Monitor

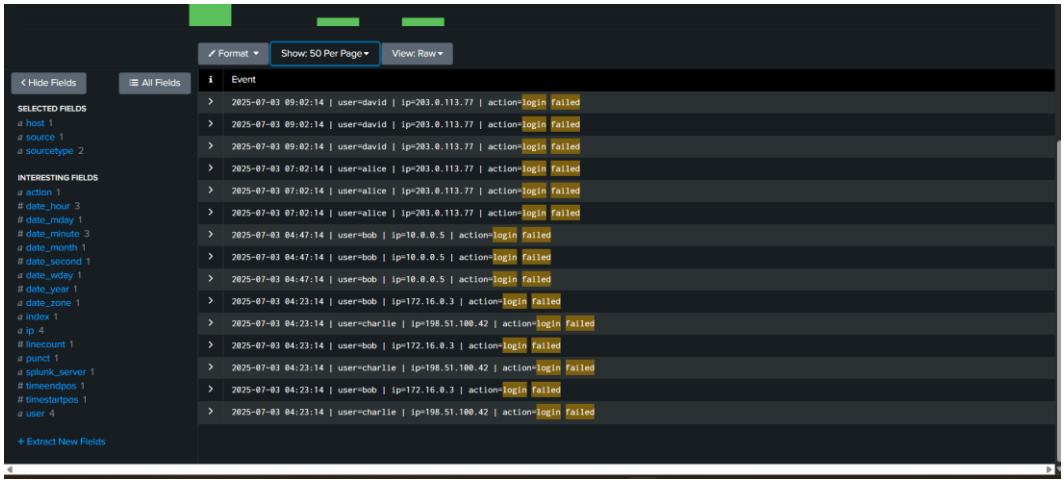
Detailed Incident Response Report

Time	Event
09:10:14	Malware detected on user bob
09:02:14	Failed login attempt detected
07:45:14	Trojan Dedected on user charlie

SIEM dashboard screenshot attached







(Optional) Communication email included

Dear Management Team,

During routine SOC monitoring, multiple high-severity security alerts were detected, including malware and ransomware-related activities.

Affected systems were identified and containment actionshave been initiated to reduce risk.

A detailed incident response report has been prepared,

including impact analysis and remediation recommendations.

Please let us know if further action is required.

Regards,

SOC Analyst