Incident Response Report

Executive Summary

This report provides an overview of detected security incidents, classified by priority (High, Medium, Low). The incidents include malware alerts and failed login attempts. The objective is to highlight potential risks, assess impact, and recommend remediation actions.

Incident Classification

Priority Level	Number of Incidents
High	14
Medium	2
Low	0

Timeline of Major Events

- 2025-07-03T04:19:14.000+0530 | User: alice | IP: 198.51.100.42 | Event: Malware Alert | Priority: High
- 2025-07-03T04:23:14.000+0530 | User: bob | IP: 172.16.0.3 | Event: Failed Login | Priority: Medium
- 2025-07-03T04:23:14.000+0530 | User: charlie | IP: 198.51.100.42 | Event: Failed Login | Priority: High
- 2025-07-03T04:29:14.000+0530 | User: alice | IP: 192.168.1.101 | Event: Malware Alert | Priority: High
- 2025-07-03T04:41:14.000+0530 | User: alice | IP: 172.16.0.3 | Event: Malware Alert | Priority: High
- 2025-07-03T04:47:14.000+0530 | User: bob | IP: 10.0.0.5 | Event: Failed Login | Priority: Medium
- 2025-07-03T05:06:14.000+0530 | User: bob | IP: 203.0.113.77 | Event: Malware Alert | Priority: High
- 2025-07-03T05:30:14.000+0530 | User: eve | IP: 192.168.1.101 | Event: Malware Alert | Priority: High
- 2025-07-03T05:42:14.000+0530 | User: eve | IP: 203.0.113.77 | Event: Malware Alert | Priority: High
- 2025-07-03T05:45:14.000+0530 | User: david | IP: 172.16.0.3 | Event: Malware Alert | Priority: High
- 2025-07-03T05:48:14.000+0530 | User: bob | IP: 10.0.0.5 | Event: Malware Alert | Priority: High

- 2025-07-03T07:02:14.000+0530 | User: alice | IP: 203.0.113.77 | Event: Failed Login | Priority: High
- 2025-07-03T07:45:14.000+0530 | User: charlie | IP: 172.16.0.3 | Event: Malware Alert | Priority: High
- 2025-07-03T07:51:14.000+0530 | User: eve | IP: 10.0.0.5 | Event: Malware Alert | Priority: High
- 2025-07-03T09:02:14.000+0530 | User: david | IP: 203.0.113.77 | Event: Failed Login | Priority: High
- 2025-07-03T09:10:14.000+0530 | User: bob | IP: 172.16.0.3 | Event: Malware Alert | Priority: High

Impact Assessment

High priority incidents indicate potential account compromises or malware infections, posing a direct risk to system integrity and sensitive data. Medium priority incidents suggest possible brute-force attempts from internal IPs. Low priority incidents are minor, but continued monitoring is necessary.

Recommendations

- Immediately isolate systems flagged in high-priority incidents.
- Conduct malware scans and block suspicious IP addresses.
- Reset credentials of affected accounts.
- Increase monitoring of failed login attempts.
- Provide security awareness to users involved.
- Maintain ongoing log review to detect anomalies early.

Appendix: Detailed Incidents

Incident: Malware Alert (High)

Timestamp: 2025-07-03T09:10:14.000+0530

User: bob

IP Address: 172.16.0.3

Incident: Malware Alert (High)

Timestamp: 2025-07-03T07:51:14.000+0530

User: eve

IP Address: 10.0.0.5

Incident: Malware Alert (High)
Timestamp: 2025-07-03T07:45:14.000+0530

User: charlie

IP Address: 172.16.0.3

Incident: Malware Alert (High)
Timestamp: 2025-07-03T05:48:14.000+0530

User: bob

IP Address: 10.0.0.5

Incident: Malware Alert (High)
Timestamp: 2025-07-03T05:45:14.000+0530

User: david

IP Address: 172.16.0.3

Incident: Malware Alert (High)
Timestamp: 2025-07-03T05:42:14.000+0530

User: eve

IP Address: 203.0.113.77

Incident: Malware Alert (High)
Timestamp: 2025-07-03T05:30:14.000+0530

User: eve

IP Address: 192.168.1.101

Incident: Malware Alert (High)
Timestamp: 2025-07-03T05:06:14.000+0530

User: bob

IP Address: 203.0.113.77

Incident: Malware Alert (High)
Timestamp: 2025-07-03T04:41:14.000+0530

User: alice

IP Address: 172.16.0.3

Incident: Malware Alert (High)
Timestamp: 2025-07-03T04:29:14.000+0530

User: alice

IP Address: 192.168.1.101

Incident: Malware Alert (High)
Timestamp: 2025-07-03T04:19:14.000+0530

User: alice

IP Address: 198.51.100.42

Incident: Failed Login (High)
Timestamp: 2025-07-03T09:02:14.000+0530

User: david

IP Address: 203.0.113.77

Incident: Failed Login (High)
Timestamp: 2025-07-03T07:02:14.000+0530

User: alice

IP Address: 203.0.113.77

Incident: Failed Login (Medium)
Timestamp: 2025-07-03T04:47:14.000+0530

User: bob

IP Address: 10.0.0.5

Incident: Failed Login (Medium)
Timestamp: 2025-07-03T04:23:14.000+0530

User: bob

IP Address: 172.16.0.3

Incident: Failed Login (High)
Timestamp: 2025-07-03T04:23:14.000+0530

User: charlie

IP Address: 198.51.100.42