INCIDENT RESPONSE REPORT

Prepared by: RAY OTIENO
Date: 01 SEPTEMBER 2025
Version: 1.0

1. Executive Summary

On 03 July 2025, SOC log analysis identified multiple suspicious activities: malware detections (rootkit, ransomware, worm attempts) and login anomalies (failed-to-success sequences). These indicate probable account compromise and active malware infections. Immediate containment measures included isolating hosts, resetting accounts, and blocking malicious IPs. Remediation and monitoring steps are ongoing.

2. Scope & Impact

Time Window: 2025-07-03 (04:00 – 09:30 UTC)
Affected Users: alice, bob
Hosts: 172.16.0.3, 198.51.100.42, 10.0.0.5
Business Impact: Potential ransomware risk and user account compromise. No confirmed data exfiltration.

3. Timeline of Events

Time (UTC)	Event/Observation	Source → Destination	Evidence
2025-07-03 04:19	Rootkit detected on alice's host	198.51.100.42 → local	incident_rootkit.png + Malv
2025-07-03 07:02	Failed login followed by success (alice)	203.0.113.77 → system	incident_alice_auth.png +
2025-07-03 09:10	Ransomware behavior detected (bob)	172.16.0.3 → local	incident_ransomware.png

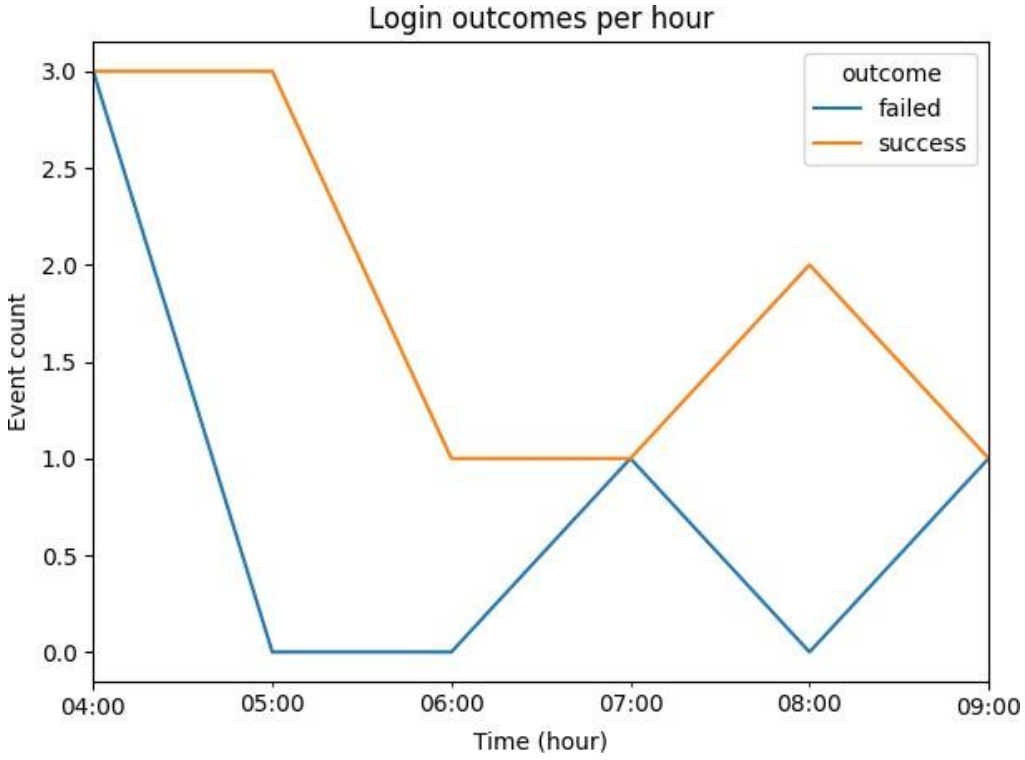
4. Evidence & IOCs

IPs: 198.51.100.42, 203.0.113.77
Users: alice, bob
Malware: Rootkit, Trojan, Worm Attempt, Ransomware

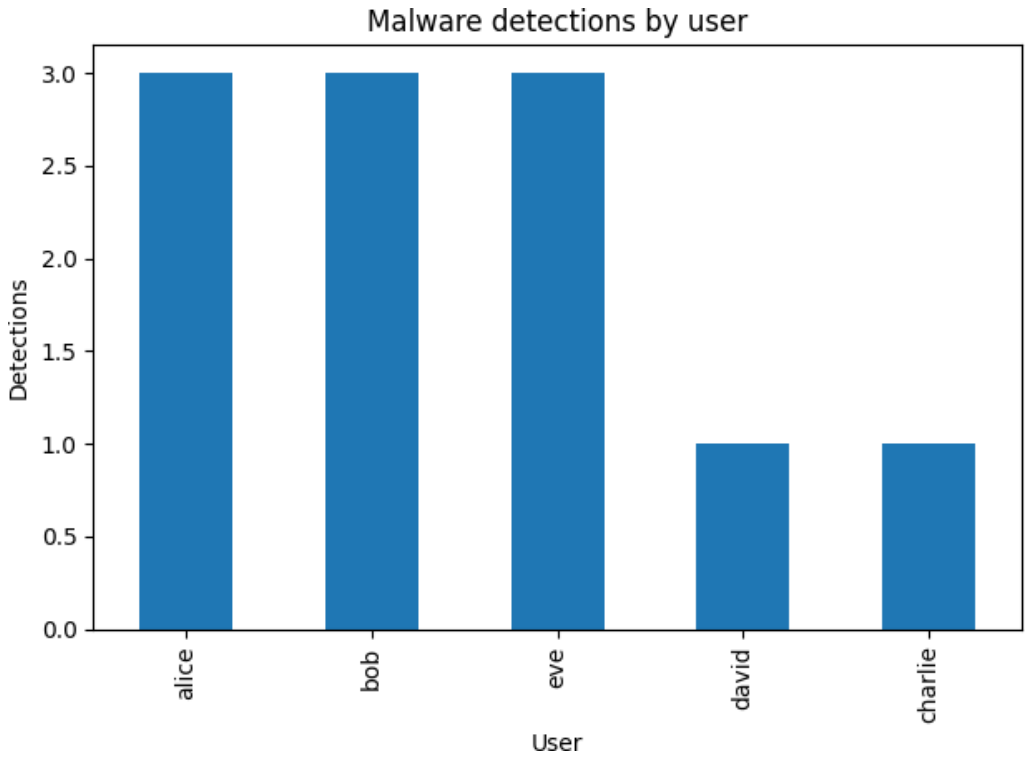
5. SIEM Dashboard Evidence

The following charts and dashboard were generated from the SOC Task 2 logs:

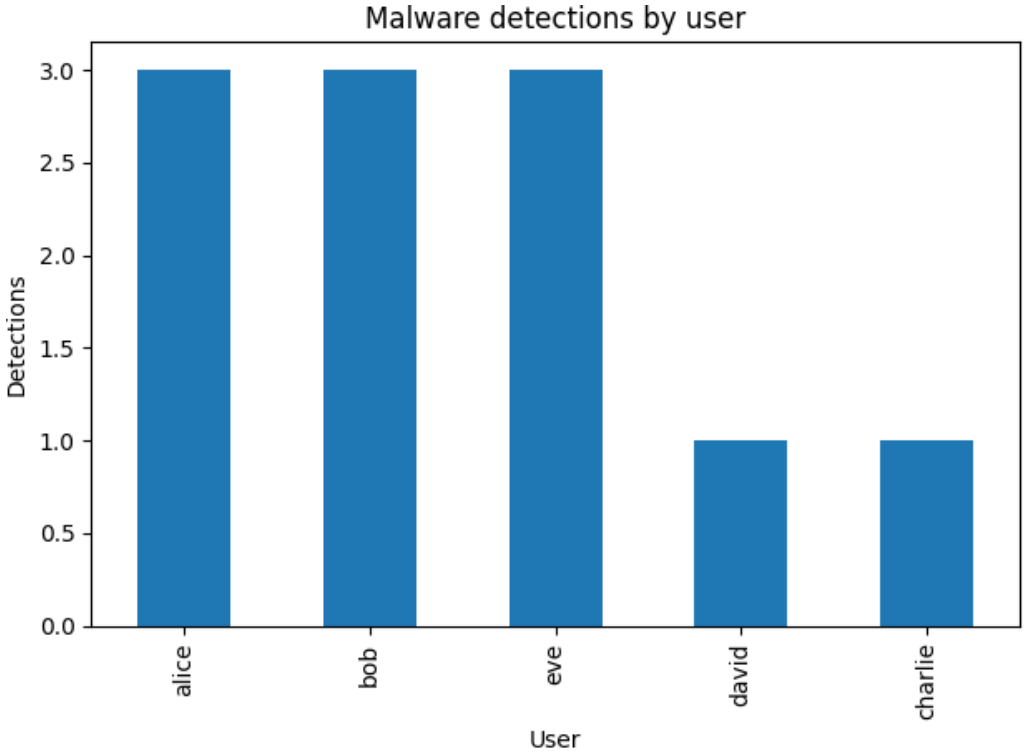
■ *Login Outcomes per Hour*

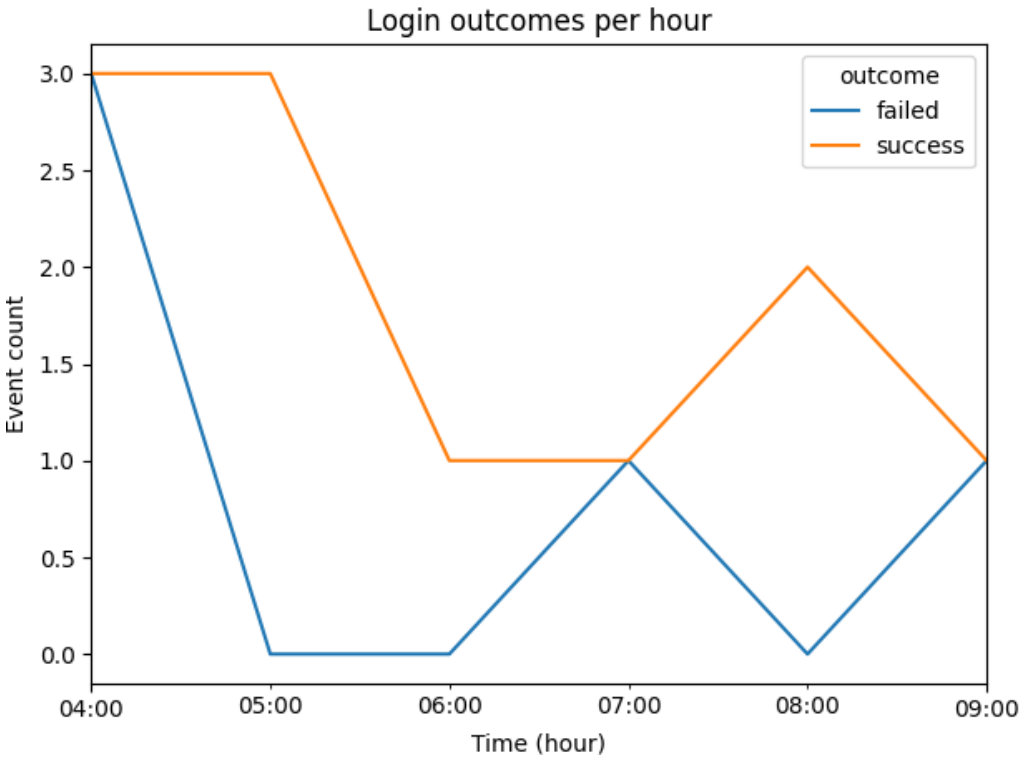


■ ***Malware Detections by User***



■ ***Combined Security Dashboard***





6. Analysis

Why it is suspicious: user alice logged in successfully after multiple failures from the same external IP.
Root Cause (if known): weak password.

False Positive Checks: confirmed no misconfigurations or travel.

7. Response Actions

Containment: Isolated affected hosts, blocked malicious IPs.
Eradication: Ran EDR/AV scans, removed malware.
Recovery: Reset credentials, enforced MFA, restored clean backups.
Monitoring: Created SIEM alerts for suspicious patterns.

8. Recommendations

1. Enforce MFA across all accounts.
2. Apply stricter lockout policies.
3. Patch systems and run regular malware scans.
4. Conduct user awareness training.

9. MITRE ATT&CK; Mapping

T1110: Brute Force (login anomalies)
T1078: Valid Accounts (alice/bob compromise)
T1486: Ransomware (bob's host)
T1059: Command & Scripting (rootkit execution)
T1105: Ingress Tool Transfer (worm attempt)

10. Appendix

Screenshots: incident_xxx.png, chart_xxx.png
Queries Used: paste KQL/SPL if using Elastic or Splunk.