Security Operations Center (SOC) — Incident Response Report

Organization: Future Interns CyberSOC
Analyst: Robith Abraham
Date: 2025-10-19

Executive Summary

During monitoring, five notable security incidents were identified and triaged within a 24-hour window. Immediate containment and mitigation steps were taken for high-severity incidents (brute-force, SQL injection indicators, and malware detection).

Incident Findings & Classification

Incident ID	Category	Severity	Source IP	Timestamp	Short Description	Status
INC-001	Brute Force	High	45.23.190.77	2025-10-18 09:15:22	Multiple failed admin login attempts detected	Blocked/Investiga
INC-002	SQL Injection Attempt	High	10.0.0.21	2025-10-18 09:18:55	Suspicious DB query 'select * from users'	Monitoring/Foren
INC-003	Malware Infection	High	185.231.250.100	2025-10-18 09:25:14	Trojan.Win32 detected on Endpoint-07	Isolated
INC-004	TOR Outbound	Medium	172.16.0.34	2025-10-18 09:40:10	Outbound connection to known TOR exit node	Blocked
INC-005	Account Lockout	Medium	45.23.190.77	2025-10-18 09:16:03	Admin account locked after repeated failures	Credentials Rese

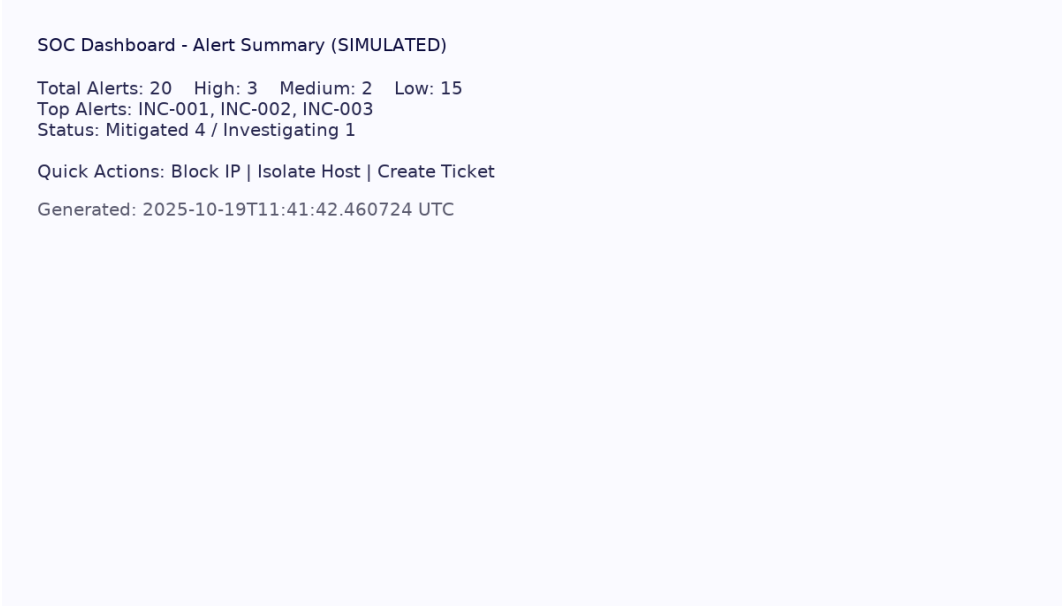
Incident Timeline

09:15 UTC - Multiple failed login attempts from 45.23.190.77 detected (brute-force). IP blocked and admin account locked. 09:18 UTC - Suspicious DB query from 10.0.0.21 detected; DB monitoring activated and query source under investigation. 09:25 UTC - Malware (Trojan.Win32) detected on Endpoint-07; host isolated and AV scan initiated. 09:40 UTC - Outbound connection to TOR exit node observed from 172.16.0.34; outbound traffic blocked and endpoint investigated.

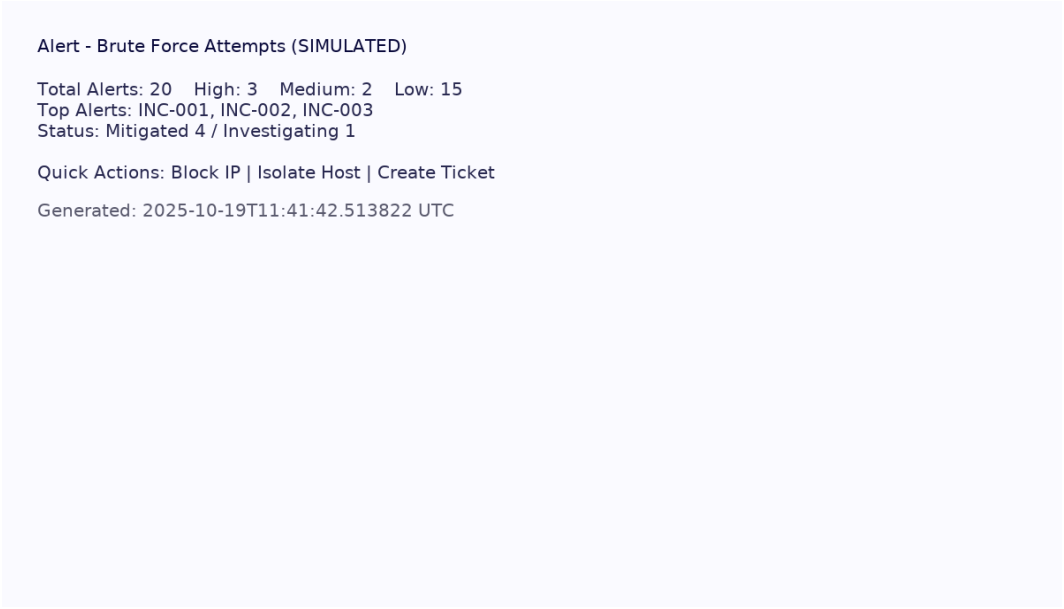
Impact Assessment & Recommendations

Impact: Potential credential compromise, data exfiltration, and host compromise. Recommendations: 1. Enforce MFA for admin accounts. 2. Patch and validate input on database-facing applications. 3. Reimage infected hosts after forensic capture. 4. Block TOR exit nodes at firewall and monitor for proxying. 5. Enhance SIEM rules for brute-force and abnormal DB queries.

SOC Dashboard - Alert Summary (SIMULATED)

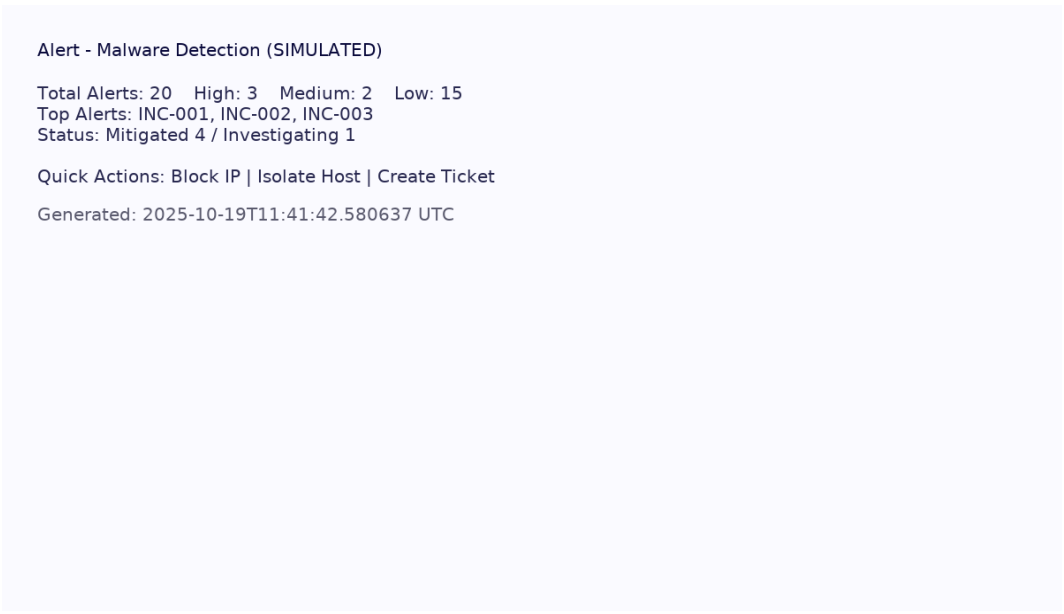


Alert - Brute Force Attempts (SIMULATED)



Alert - Suspicious SQL Query (SIMULATED)

Alert - Malware Detection (SIMULATED)



Stakeholder Communication (Email Draft)

To: IT Security Manager
Subject: [URGENT] High-Severity Incidents Detected — Immediate Action Required

Dear Team,

During today’s SOC monitoring, we identified multiple high-severity security alerts including a brute-force login attempt, SQL injection indicators, and a confirmed malware infection.

Actions Taken:
- Attacker IP blocked
- Malware host isolated
- DB monitoring enabled

Requesting confirmation for forensic analysis and system reimaging where necessary.

Regards,
Robith Abraham
SOC Intern — Future Interns