**Report: Capstone Project**

**Executive Summary**

On 19 September 2025 at 15:59 UTC, the SOC conducted a comprehensive security workflow simulation involving advanced log analysis, threat intelligence integration, and incident response procedures. The exercise successfully demonstrated the detection of authentication anomalies from source IP 192.168.1.100, including failed login attempts followed by successful authentication and explicit credential usage on critical database server DB-SRV01. Elastic Security generated high-priority alerts mapped to MITRE Techniques T1078 (Valid Accounts) and T1110 (Brute Force), triggering structured incident handling processes. Containment was achieved through immediate system isolation, credential resets, and network segmentation. The incident was escalated to Tier-2 with comprehensive evidence collection and forensic analysis preparation. No data exfiltration was confirmed during the incident timeframe.

**Timeline**

• 15:59:45 UTC: Initial reconnaissance activity detected, firewall denial logged for TCP traffic from 192.168.1.100 to 8.8.8.8:53 • 16:00:01 UTC: Failed login attempt (Event ID 4625) from 192.168.1.100 targeting WIN-SRV01 with username "admin" • 16:00:15 UTC: Successful authentication (Event ID 4624) from 192.168.1.100 to WIN-SRV01 with administrator credentials • 16:01:00 UTC: Explicit credential logon (Event ID 4648) detected from 192.168.1.100 to DB-SRV01 with administrator account • 16:01:30 UTC: Network connection analysis completed, suspicious patterns identified • 16:02:00 UTC: Incident classified as High-priority (INC-2025-0919-001), immediate containment initiated • 16:05:00 UTC: Evidence collection completed, chain of custody established • 16:10:00 UTC: Escalation to Tier-2 with comprehensive case documentation in TheHive

**Recommendations**

**Immediate Actions:**

* Reset all potentially compromised administrator credentials across affected systems
* Apply latest security patches to authentication services and implement additional monitoring
* Conduct memory forensics on DB-SRV01 and review access logs for signs of data access
* Implement network segmentation to isolate critical database servers

**Long-term Improvements:**

* Deploy multi-factor authentication for all administrative accounts
* Enhance automated threat intelligence integration for real-time IOC matching
* Establish continuous security monitoring with behavioral analytics
* Create automated response playbooks for similar authentication anomaly scenarios