**TheHive Case: Tier-2 Escalation for Authentication Anomalies**

**Case Summary:**

On 19 September 2025 at 15:59 UTC, Elastic Security generated multiple high-priority alerts for coordinated authentication anomalies against critical infrastructure. Source IP 192.168.1.100 executed a sequence of failed login attempts (Event ID 4625) followed by successful authentication (Event ID 4624) and explicit credential logon (Event ID 4648) to database server DB-SRV01. Concurrent firewall denials suggest attempted command and control communication to external DNS servers.

Immediate Containment Completed:

* Isolated affected systems DB-SRV01 and WIN-SRV01 from network
* Applied emergency firewall rules blocking source IP 192.168.1.100
* Initiated credential reset procedures for administrator accounts
* Implemented network segmentation to prevent lateral movement

Evidence Collected with Chain of Custody:

* Windows Security Event Logs: Hash a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6
* Network Connection Data: Hash b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7
* System Process Lists: Hash c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8
* Threat Intelligence Analysis: IP reputation flagged as suspicious in AlienVault OTX

Request for Tier-2 Analysis:

* Perform comprehensive disk and memory imaging of DB-SRV01 and WIN-SRV01
* Conduct detailed timeline analysis and root-cause investigation
* Review network captures for evidence of lateral movement or data exfiltration
* Correlate with additional threat intelligence sources for campaign attribution
* Prepare detailed forensic report with recommendations for security improvement

Priority: HIGH - Critical infrastructure potentially compromised

Preserve: All volatile evidence with cryptographic verification

Contact:SOC on-call manager immediately for coordination and evidence transfer upon leadership request