Microsoft Sentinel MITRE ATT&CK Brute-Force Attack Detection & Automated Azure VM Shutdown (SOAR)

Role: Security Operations (SOC) Analyst – Lab Project

Tools: Microsoft Sentinel, Microsoft Defender for Cloud, Azure Monitor Agent, Logic Apps (SOAR), Azure Virtual Machines, Outlook 365

Frameworks: MITRE ATT&CK (T1110 – Brute Force), ISO/IEC 27001:2022

Project Summary

Built and tested a cloud-native incident detection and automated response workflow in Microsoft Sentinel to identify brute-force login attacks (MITRE ATT&CK T1110) and immediately isolate the target system by shutting down the affected Azure VM. Automated SOC notifications ensure rapid awareness and response, mapped to ISO/IEC 27001:2022 security controls.

Objectives

• Detect high-frequency failed authentication attempts in Windows Security logs.

• Create a Sentinel Analytics Rule to generate incidents on detection.

• Trigger a Logic App playbook (SOAR) to power off tagged Azure VMs and alert the SOC.

• Align detection and response workflows to ISO 27001:2022 controls for logging, monitoring, and access control.

Scope

• Monitors Windows Security logs for repeated failed logins (Event ID 4625 bursts).

• Creates Sentinel incident via KQL detection logic.

• Automation Rule triggers Logic App (Managed Identity) to shut down only VMs with safety tag AutoShutdown=true.

• Sends SOC notification email via Outlook connector.

Implementation Steps

1. Log Ingestion: Onboarded Azure VM to Sentinel using Azure Monitor Agent for SecurityEvent collection.

2. Detection Logic: Custom KQL rule detects brute-force authentication attempts, mapped to MITRE ATT&CK T1110.

3. Incident Creation: Configured Analytics Rule to run every 5 minutes, triggering an incident for confirmed events.

4. Automation Rule & SOAR Playbook: Automation Rule invokes Logic App on incident creation, sends SOC email alert, and powers off tagged VM.

5. Security Safeguards: Least-privilege Managed Identity, VM shutdown limited to tagged non-production assets, exclusions for trusted sources.

ISO/IEC 27001:2022 Control Mapping

Control	Goal	Coverage
A.8.15 – Logging	Ensure security-relevant events are recorded and investigable.	SecurityEvent logs ingested into Sentinel; KQL rule detects excessive failed logins; logs retained per policy with access controls.
A.8.16 – Monitoring Activities	Continuously monitor for suspicious activity and respond quickly.	Analytic rule executes every 5 minutes; automation triggers Logic App within 60 seconds; workbook visualises incidents and MTTR/MTTD.
A.5.15 – Access Control	Allow only authorised access and revoke it upon risk detection.	Automatically powers off tagged VMs; Logic App operates under least privilege; exclusions applied for authorised sources.

Results & Impact

• Mean Time to Detect (MTTD): < 1 minute from attack onset.

• Mean Time to Respond (MTTR): < 3 minutes from detection to VM shutdown.

• Containment Success: 100% in lab brute-force simulations.

• Compliance: Supports ISO/IEC 27001:2022 control objectives for logging, monitoring, and access control.

Key Skills Demonstrated

• SIEM configuration & advanced detection engineering (Microsoft Sentinel, KQL).

• Security orchestration, automation, and response (SOAR) via Logic Apps.

• Azure infrastructure isolation & incident response playbook design.

- MITRE ATT&CK alignment for SOC operational workflows.
- ISO/IEC 27001:2022 control mapping and compliance reporting.