INCIDENT REPORT – USE CASE 3

SSH Brute Force Detection and Blocking (Ubuntu Agent)

Incident ID: SOC-SSH-003
Incident Title: SSH Brute Force Attack Detected and Blocked
Date & Time: Jan 18, 2026 @ 19:20:46.706
Detection Source: Wazuh SIEM – SSH Authentication Monitoring

Affected Asset
Host: Ubuntu Agent
Asset Type: Linux Server
Severity: High

Incident Summary
Wazuh SIEM detected multiple failed SSH authentication attempts against the Ubuntu server from a single external source within a short time period. The activity was indicative of a brute force attack aimed at gaining unauthorized access. The attack was identified early, and blocking controls were applied to prevent further login attempts.

Detection Details
Detection Tool: Wazuh SIEM
Detection Module: SSH Authentication Logs
Event Type: Multiple Failed SSH Login Attempts
Target Service: SSH (Port 22)
Source IP: Kali Linux (Attacker Simulation)
Destination Host: Ubuntu Agent
Wazuh Rule ID: 5763 (SSH brute force related)
Rule Level: High

Investigation and Analysis
The SOC analyst reviewed authentication failure alerts in the Wazuh dashboard and observed repeated login attempts against the same user account originating from a single source IP. The frequency and pattern of attempts exceeded normal behavior and matched known brute force attack characteristics. Correlation checks confirmed no successful SSH login events occurred during or after the attack window.

Classification
True Positive – Authorized Attack Simulation

Root Cause
Intentional SSH brute force attack performed from a Kali Linux system to simulate unauthorized access attempts and validate SOC detection and response capabilities.

Impact Assessment
No unauthorized access was gained.
No system compromise or data exposure occurred.
The attack was limited to authentication attempts and was successfully detected and contained.

Response Actions
The alert was reviewed and confirmed by the SOC analyst.
The attacking source IP was blocked using host-based firewall controls (simulated).
The targeted user account was monitored for further activity.
The incident was documented according to SOC procedures.

Lessons Learned
SSH brute force attacks can be reliably detected by monitoring authentication failures. Early detection and automated or

manual blocking significantly reduce the risk of unauthorized access. Correlating failed and successful login events is essential to confirm whether an attack succeeded.

MITRE ATT&CK Mapping
Tactic: TA0006 – Credential Access
Technique ID: T1110
Technique Name: Brute Force

Incident Status
Closed – Contained (Test Case Validation)