INCIDENT REPORT – USE CASE 3
Network Intrusion Detection (Suricata IDS + Wazuh)

Incident ID: SOC-NID-002
Incident Title: Network Reconnaissance Detected via Port Scanning
Date & Time: Jan 18, 2026 @ 17:48:24.331
Detection Source: Suricata IDS (Integrated with Wazuh SIEM)

Affected Asset
Host: Ubuntu Agent (Network Sensor)
Asset Type: Linux Server
Severity: Medium

Incident Summary
Suricata IDS detected network reconnaissance activity targeting the Ubuntu host. Multiple connection attempts to different ports from a single external source were identified, indicating port scanning behavior. The alerts were centrally collected and analyzed in Wazuh SIEM. Early detection of reconnaissance activity is critical to prevent follow-on attacks and host-level compromise.

Detection Details
Detection Tool: Suricata IDS
Detection Type: Network-based Intrusion Detection
Alert Category: Network Scan / Suspicious Traffic
Source IP: Kali Linux (Attacker Simulation)
Destination IP: Ubuntu Agent
Protocol: TCP
Detection Log Source: eve.json
SIEM Platform: Wazuh

Investigation and Analysis
The SOC analyst reviewed Suricata alerts ingested into the Wazuh dashboard and identified repeated connection attempts from the same source IP across multiple ports within a short time frame. This behavior was consistent with network reconnaissance activity. Correlation checks were performed against host-based logs, including SSH authentication and File Integrity Monitoring alerts, to determine whether the scan led to any host-level activity. No evidence of successful exploitation or unauthorized access was observed.

Classification
True Positive – Authorized Activity (Attack Simulation)

Root Cause
Intentional network scanning performed from a Kali Linux system to simulate attacker reconnaissance behavior as part of SOC detection testing.

Impact Assessment
No service disruption was observed.
No unauthorized access or host compromise occurred.
The activity was limited to reconnaissance and did not progress to exploitation.

Response Actions
Alerts were reviewed and validated by the SOC analyst.
Source IP and scanning behavior were documented.
No blocking or remediation actions were required due to the activity being part of a controlled test scenario.

Lessons Learned

Network-based intrusion detection is effective for identifying early-stage attacker behavior. Correlating IDS alerts with host-based logs helps SOC analysts determine whether reconnaissance activity has progressed to exploitation or compromise.

MITRE ATT&CK Mapping

Tactic: TA0043 – Reconnaissance
Technique ID: T1046
Technique Name: Network Service Scanning

Incident Status

Closed – Informational (Test Case Validation)