## INCIDENT REPORT – USE CASE 7
## Malware Detection with VirusTotal Integration (Ubuntu Agent)

Incident ID: SOC-MAL-007
Incident Title: Malware Detected on Ubuntu System via VirusTotal Integration
Date & Time: Jan 19, 2026 @ 15:33:46.515
Detection Source: Wazuh SIEM – VirusTotal Integration

**Affected Asset**
Host: ubuntuserver
Asset Type: Linux Server
Operating System: Ubuntu Linux
Severity: High

**Incident Summary**
Wazuh SIEM detected a malicious file on an Ubuntu Linux system and validated the threat using VirusTotal threat intelligence. The detected file was identified as malicious by multiple antivirus engines, indicating a high-confidence malware detection. This incident demonstrates the SOC's ability to enrich alerts with external threat intelligence and assess execution-related risk.

**Detection Details**
Detection Tool: Wazuh SIEM
Detection Type: Host-based Malware Detection
Threat Intelligence Source: VirusTotal
File Name: eicar.com
File Path: /root/eicar.com
VirusTotal Detection Result: 64 antivirus engines detected this file
Wazuh Rule ID: 87105
Rule Level: 12
Detection Module: VirusTotal

**Investigation and Analysis**
Reviewed the malware alert in the Wazuh dashboard and examined the VirusTotal enrichment data included in the alert. The file hash was automatically submitted to VirusTotal, which returned a positive detection from multiple antivirus engines. Further investigation confirmed that the detected file was the standard EICAR test file created intentionally for malware detection validation in a controlled lab environment. Correlation with other security events, including file integrity monitoring, command execution logs, and network activity, showed no evidence of malware execution, persistence mechanisms, or lateral movement.

**Classification**
True Positive – Authorized Activity (Malware Detection Test Case Validation)

**Root Cause**
Intentional creation of a standard EICAR test file on the Ubuntu system to validate Wazuh malware detection and VirusTotal threat intelligence integration.

**Impact Assessment**
No system compromise occurred.
No malicious code execution was observed.
No persistence, privilege escalation, or network-based malicious activity was detected.
Security controls successfully detected and validated the simulated malware file.

**Response Actions**
The alert was reviewed and validated by the SOC analyst.

The detected file was documented and removed from the system (simulated).
The affected system was monitored for additional malware-related activity.
No further remediation actions were required due to the controlled test scenario.

**Lessons Learned**

Integrating SIEM alerts with threat intelligence platforms such as VirusTotal significantly improves detection confidence. Malware detection controls effectively identified a suspicious file and provided execution-related context even before any malware execution occurred.

**MITRE ATT&CK Mapping**

Tactic: TA0002 – Execution
Technique ID: T1203
Technique Name: Exploitation for Client Execution

**Incident Status**

Closed – Informational (Malware Detection Test Case Validation)