Alert Triage Report

1. Executive Summary

This report documents the investigation of a Suspicious File Download detected on a Windows endpoint. The alert was generated by Wazuh using File Integrity Monitoring (FIM) and was automatically ingested into TheHive, where it resulted in the creation of an incident case. The case was enriched using VirusTotal to validate the threat and support response decisions.

2. Alert Generation

Wazuh File Integrity Monitoring identified the creation of a previously unknown file in a user accessible directory. The alert was raised based on:

- Untrusted file origin
- Unrecognized file hash
- User-level execution context

At the time of detection, no endpoint antivirus verdict was available, requiring further investigation.

Alert ID	Description	Source IP	Priority	Status
005	Suspicious File Download	10.0.2.30	High	Open

Table 1: Alert

The alert indicated a potentially malicious downlod requiring further investigation and validation.

3. Initial Triage Actions

The alert automatically resulted in the creation of an investigation case in TheHive. Initial triage focused on determining whether the activity represented benign user behavior or a potential security threat.

Actions Performed:

- Reviewed alert metadata and timestamps.
- Validated host ownership and user context.
- Confirmed file location and extension.
- Extracted file hash for enrichment.

4. Observables Identified

The following observables were attached to the case during ingestion:

- **File Hash (SHA256)** – marked as IOC
- **Source IP Address** – internal endpoint
- **Hostname** – Windows workstation

These observables were prioritized for threat intelligence analysis.

5. VirusTotal Analysis

VirusTotal analysis of the suspicious file hash indicated multiple antivirus detections and a negative reputation score. The hash matched known malicious patterns, confirming suspicious behavior. Based on intelligence enrichment, the alert was validated as a true positive and required escalation for containment and remediation actions.

6. Investigation Findings

Category	Result
Initial Detection	Suspicious file creation
Intelligence Verdict	Malicious
Confidence Level	High
Alert Outcome	True Positive

Table 2: Result

The investigation confirmed that the suspicious download posed a legitimate security risk.

7. Recommended Response Actions

Recommended actions following validation:

- Isolate the affected Windows endpoint.
- Block the file hash across endpoint controls.
- Review user activity leading to the download.

8. Lessons Learned

- FIM-based alerts are effective early indicators of suspicious activity.
- Automated threat intelligence significantly reduces triage time.
- Alert-driven case creation improves investigation consistency.

9. Summary

A suspicious file download was detected on a Windows endpoint through Wazuh File Integrity Monitoring. The alert automatically generated an investigation case, where threat intelligence enrichment confirmed malicious indicators associated with the file hash. Based on these findings, the alert was classified as a true positive and the file hash was blocked.