

Incident Response Report

1. Executive Summary

A high-priority alert was generated in Wazuh for suspicious PowerShell execution on a Windows endpoint. The activity originated from an internal system (10.0.2.19) and targeted the victim machine (10.0.2.22). Threat intelligence checks confirmed no malicious verdict from VirusTotal, and the incident was escalated based on behavioral risk rather than reputation alone.

Alert ID	Description	Source IP	Priority	Status
004	PowerShell Execution	10.0.2.19	High	Open

Table 1: Alert

2. Timeline

Time (UTC)	Event
2025-12-18 14:00	Suspicious PowerShell execution detected
2025-12-18 14:02	Wazuh generated Alert ID 004
2025-12-18 14:05	Victim system identified as 10.0.2.22
2025-12-18 14:08	Source activity traced to 10.0.2.19
2025-12-18 14:12	VirusTotal IOC validation completed (no malicious findings)
2025-12-18 14:15	AlienVault OTX threat context reviewed
2025-12-18 14:18	Risk assessment performed
2025-12-18 14:20	Alert escalated to SOC L2

Table 2: Timeline

3. IOC Validation

Indicators Reviewed:

- Source IP:** 10.0.2.19
- Victim IP:** 10.0.2.22
- Technique Observed:** Suspicious PowerShell execution

Although no malicious indicators were identified through VirusTotal or OTX, the alert remains significant due to behavior-based detection. Internal network attacks often use infrastructure that has not yet been reported to public intelligence feeds.

4. Impact Analysis

The observed PowerShell activity may indicate unauthorized command execution and potential post-exploitation behavior. Even without confirmed malicious IOCs, such activity poses a risk of lateral movement, privilege escalation, or persistence if not contained promptly.

5. Remediation Steps

- Isolated the victim machine (10.0.2.22) for further analysis
- Restricted PowerShell execution and enforced execution policies
- Reviewed Windows Event ID 4688 for suspicious command lines
- Conducted environment-wide threat hunting for similar behavior
- Escalated the alert to SOC L2 for deeper investigation

6. Lessons Learned

This incident demonstrates that IOC validation alone is insufficient for threat detection. Behavioral monitoring, internal network visibility, and contextual analysis are essential when public intelligence sources show no malicious reputation.