Alert Triage with Threat Intelligence Report

Introduction

Alert triage is the process of analyzing and validating security alerts to determine their severity, legitimacy, and required response actions. In this task, a suspicious PowerShell execution alert was investigated and validated using external threat intelligence sources.

Alert ID	Description	Source IP	Priority	Status
004	Suspicious PowerShell Execution	192.168.1.101	High	Open

Initial Triage Analysis

The alert indicated suspicious PowerShell execution activity originating from host 192.168.1.101. PowerShell is frequently used by attackers for lateral movement, payload execution, and persistence. Due to its potential impact, the alert was classified as High priority for further validation.

IOC Validation

The source IP address 192.168.1.101 was checked against VirusTotal and AlienVault OTX threat intelligence feeds.

VirusTotal Results:
No widespread malicious detection, but historical reports indicate suspicious behavior.

AlienVault OTX Results:
The IP was associated with reconnaissance and scanning activity in prior community reports.

Threat intelligence validation showed limited but concerning activity associated with the source IP. While not globally flagged as malicious, its historical scanning behavior suggests potential reconnaissance. Continuous monitoring and deeper endpoint analysis are recommended before escalating further.

Final Decision

The alert remains classified as High priority due to the use of PowerShell and suspicious activity indicators. The endpoint should undergo further investigation, including process tree analysis and user activity review. Escalation to Tier 2 is recommended if additional malicious artifacts are discovered.

MITRE ATT&CK Mapping

Technique: T1059.001 – PowerShell
Tactic: Execution

Mapping alerts to MITRE ATT&CK provides standardized classification and improves detection strategy alignment.