SOC Incident Simulation Report

Analyst: Alexander T. Ramos | Date: October 05, 2025

Incident Title: Suspicious PowerShell Execution

Severity: Medium-High | **Status:** Resolved

1. Objective
This report outlines the analysis and response to a simulated PowerShell-based attack detected via Splunk and Security Onion. The exercise demonstrates SOC-level event triage, cross-tool investigation, and incident containment following NIST 800-61 procedures.

2. Detection Summary
Splunk triggered an alert for a suspicious PowerShell command utilizing the EncodedCommand flag. The event originated from a Windows 10 workstation, suggesting potential script-based execution by an attacker.

Phase	Action	Description
Containment	Isolated the endpoint	Used EDR tools to disconnect affected host from the network.
Eradication	Removed malicious profiles	Deleted PowerShell startup scripts and disabled persistence mecha
Recovery	Restored clean image	Validated system integrity and rejoined host to internal network.
Reporting	Documented workflow	Captured Splunk query and findings for supervisor review.

3. Splunk Query Used
index=win_eventlog sourcetype=WinEventLog:Security | search powershell EncodedCommand | stats count by user, ComputerName, Process_CommandLine

Type	Indicator	Source
Process CommandLine	powershell.exe -EncodedCommand JAB...	Splunk Security Logs
Parent Process	explorer.exe	Windows Event ID 4688
Destination IP	185.199.110.153	Security Onion NetFlow
File Hash	8fa90eac2f21e...	VirusTotal

4. Findings Summary
- Single endpoint triggered the alert.
- No evidence of lateral movement.
- No credential dumping detected.
- User training and PowerShell policy hardening recommended.

5. Outcome
Incident contained within 30 minutes of initial alert. Demonstrated ability to correlate Splunk event data with Security Onion logs, execute proper containment, and produce structured reporting for SOC leadership.

Prepared by: Alexander T. Ramos – SOC Analyst in Training