Elastic SIEM + Sysmon Endpoint Detection

Project Type: Endpoint Detection Engineering / SOC Telemetry

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this project was to design, deploy, and validate endpoint detection and logging pipelines using Sysmon and Elastic SIEM. The goal was to establish high-fidelity visibility into process execution, network connections, and PowerShell activity, ensuring endpoint telemetry is centrally ingested, searchable, and actionable for SOC monitoring, detection engineering, and incident response.

Tools & Technologies

- Elastic Cloud (Elastic SIEM & Kibana)
- Elastic Agent (Fleet-managed)
- Sysmon (System Monitor)
- Windows PowerShell (Administrator)
- Windows Event Logs
- Kibana Discover & KQL

Technical Steps Performed

1. Elastic Agent Deployment

- Installed Elastic Agent on the Windows endpoint using PowerShell.
- Enrolled the agent into Elastic Cloud via Fleet.
- Verified that the agent service was successfully installed and running.

2. Sysmon Deployment & Configuration

- Installed Sysmon as a persistent system service.
- Enabled Sysmon operational logging to capture detailed endpoint telemetry.
- Confirmed Sysmon integration with Elastic Agent for centralized forwarding.

3. Telemetry Ingestion Validation

- Navigated to Kibana → Discover.
- Queried Sysmon data streams to validate ingestion of endpoint events.
- Confirmed visibility of:
    - Process creation events
    - Network connection events
    - PowerShell execution telemetry

4. Event Analysis in Elastic SIEM

- Reviewed ingested events using Kibana Query Language (KQL).
- Verified that endpoint activity was timestamped, structured, and correlated with host metadata.
- Confirmed continuous event flow from endpoint to Elastic SIEM.

Findings

Endpoint Visibility Findings

- Sysmon process creation events (Event ID 1) were successfully ingested.
- Sysmon network connection events (Event ID 3) were visible and correlated to originating processes.
- PowerShell activity was captured and searchable within Elastic SIEM.

SIEM Ingestion Findings

- Endpoint telemetry was indexed in the appropriate data streams.
- Events were searchable in near real time.
- No ingestion errors or gaps were observed.

Outcome

- Successfully deployed an endpoint detection pipeline using Sysmon and Elastic SIEM.
- Established centralized visibility into endpoint process, network, and PowerShell activity.
- Demonstrated SOC-relevant detection capabilities aligned with real-world endpoint monitoring workflows.
- Produced verifiable evidence supporting detection engineering, threat hunting, and incident response readiness.

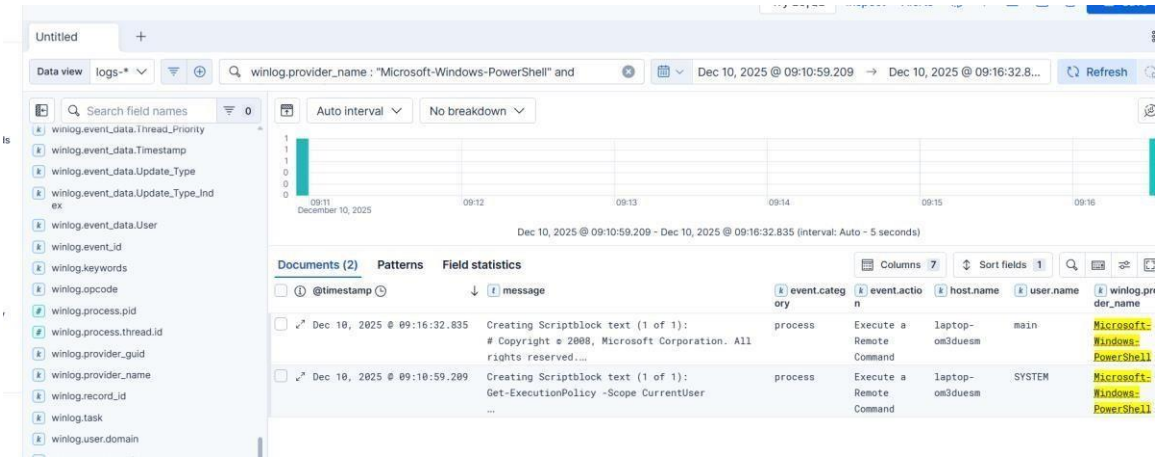
This project demonstrates experience building and validating endpoint detection telemetry pipelines using industry-standard SOC tooling.

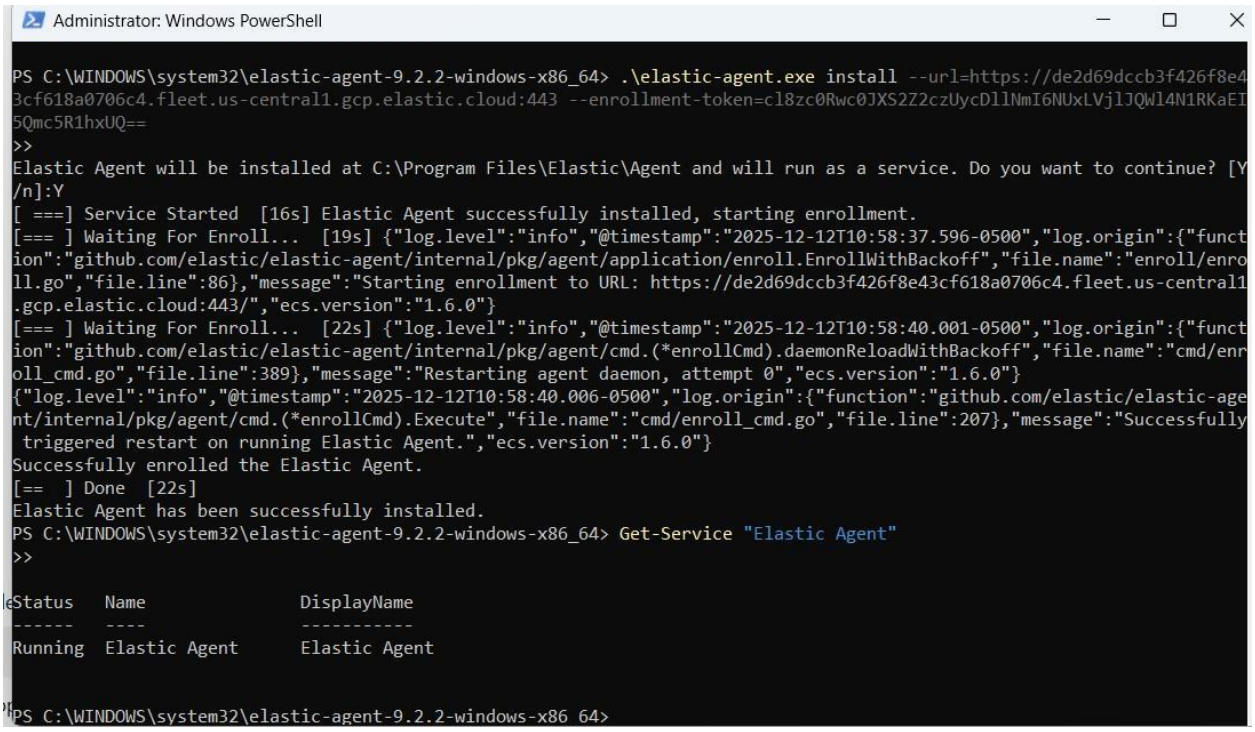
Portfolio Status

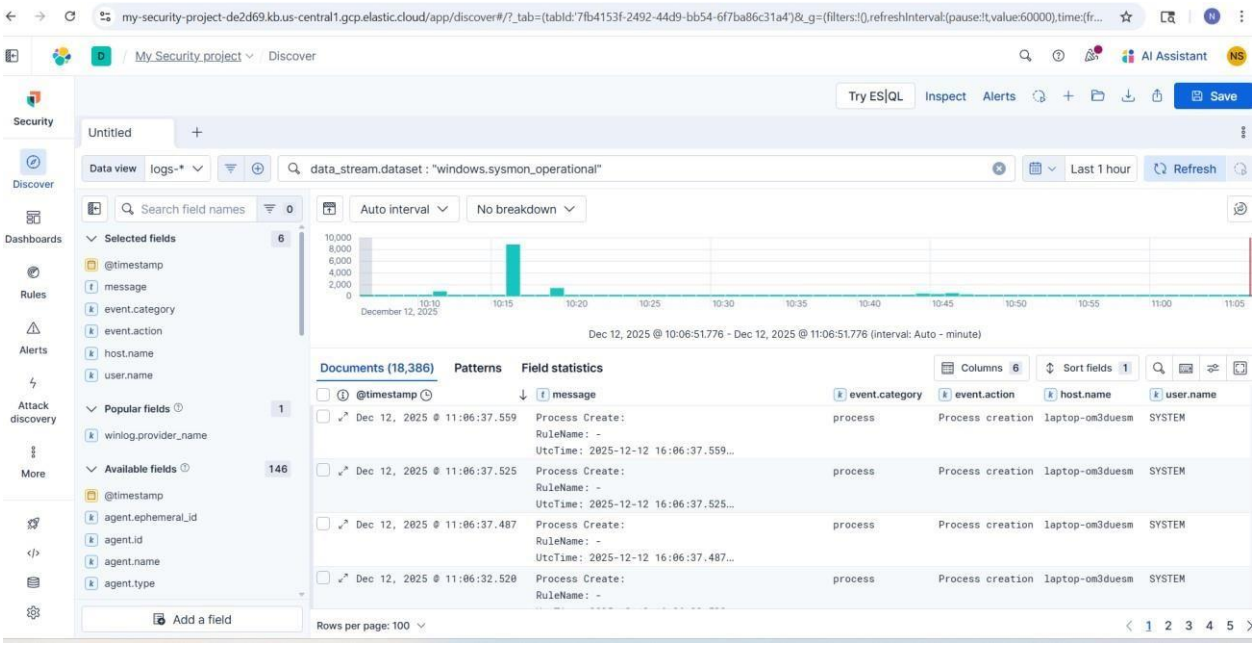
Project Status: Completed

Deliverable: Endpoint_Detection_Elastic_Sysmon.pdf

Evidence: Elastic Agent installation output, Sysmon event ingestion, Kibana Discover validation


Untitled
Data view
logs-*
winlog.provider_name : "Microsoft-Windows-PowerShell" and
Dec 10, 2025 @ 09:10:59.209
Dec 10, 2025 @ 09:16:32.8...
Refresh
Search field names
Auto interval
No breakdown
winlog.event_data.Thread_Priority
winlog.event_data.Timestamp
winlog.event_data.Update_Type
winlog.event_data.Update_Type_Index
winlog.event_data.User
winlog.event_id
winlog.keywords
winlog.opcode
winlog.process.pid
winlog.process.thread.id
winlog.provider_guid
winlog.provider_name
winlog.record_id
winlog.task
winlog.user.domain
09:11
December 10, 2025
09:12
09:13
09:14
09:15
09:16
Dec 10, 2025 @ 09:10:59.209 - Dec 10, 2025 @ 09:16:32.835 (interval: Auto - 5 seconds)
Documents (2)
Patterns
Field statistics
Columns 7
Sort fields 1
@timestamp
message
event.category
event.action
host.name
user.name
winlog.provider_name
Dec 10, 2025 @ 09:16:32.835
Creating Scriptblock text (1 of 1):
Copyright © 2008, Microsoft Corporation. All rights reserved....
process
Execute a Remote Command
laptop-om3duesm
main
Microsoft-Windows-PowerShell
Dec 10, 2025 @ 09:10:59.209
Creating Scriptblock text (1 of 1):
Get-ExecutionPolicy -Scope CurrentUser
...
process
Execute a Remote Command
laptop-om3duesm
SYSTEM
Microsoft-Windows-PowerShell


Administrator: Windows PowerShell
PS C:\WINDOWS\system32\elastic-agent-9.2.2-windows-x86_64> .\elastic-agent.exe install --url=https://de2d69dccb3f426f8e43cf618a0706c4.fleet.us-central1.gcp.elastic.cloud:443 --enrollment-token=cl8zc0Rwc0JXS2Z2czUycDllNmI6NUxLVjlJQWl4N1RKaEI5Qmc5R1hxUQ==
>>
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:Y
[===] Service Started [16s] Elastic Agent successfully installed, starting enrollment.
[===] Waiting For Enroll... [19s] {"log.level":"info","@timestamp":"2025-12-12T10:58:37.596-0500","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/application/enroll.EnrollWithBackoff","file.name":"enroll/enroll.go","file.line":86},"message":"Starting enrollment to URL: https://de2d69dccb3f426f8e43cf618a0706c4.fleet.us-central1.gcp.elastic.cloud:443/","ecs.version":"1.6.0"}
[===] Waiting For Enroll... [22s] {"log.level":"info","@timestamp":"2025-12-12T10:58:40.001-0500","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":389},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-12-12T10:58:40.006-0500","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":207},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[==] Done [22s]
Elastic Agent has been successfully installed.
PS C:\WINDOWS\system32\elastic-agent-9.2.2-windows-x86_64> Get-Service "Elastic Agent"
>>
Status Name DisplayName
------ ---- -----------
Running Elastic Agent Elastic Agent
PS C:\WINDOWS\system32\elastic-agent-9.2.2-windows-x86_64>


my-security-project-de2d69.kb.us-central1.gcp.elastic.cloud/app/discover#/?_tab=(tabId:'7fb4153f-2492-44d9-bb54-6f7ba86c31a4')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(fr...
My Security project
Discover
AI Assistant
Try ES|QL
Inspect
Alerts
Save
Untitled
Data view
logs-*
data_stream.dataset : "windows.sysmon_operational"
Last 1 hour
Refresh
Search field names
Auto interval
No breakdown
Selected fields
@timestamp
message
event.category
event.action
host.name
user.name
Popular fields
winlog.provider_name
Available fields
agent.ephemeral_id
agent.id
agent.name
agent.type
Add a field
Dec 12, 2025 @ 10:06:51.776 - Dec 12, 2025 @ 11:06:51.776 (interval: Auto - minute)
Documents (18,386)
Patterns
Field statistics
Columns
Sort fields
Process Create:
RuleName: -
Process creation
laptop-om3duesm
SYSTEM
Rows per page: 100