Contents

PDF version available:
Download README.pdf

Cybersecurity Telemetry Pipeline

This repository documents and supports a virtualized cybersecurity lab built around a Windows-Sysmon-Splunk telemetry pipeline. The goal of this lab is learning, experimentation, and graduate-level research—not production deployment or job hunting.

Overview

The lab consists of: - A **Windows 10** virtual machine instrumented with **Sysmon** and a **Splunk Universal Forwarder**. - An **Ubuntu** virtual machine running **Splunk Enterprise** inside a **Docker** container. - A telemetry pipeline that delivers detailed endpoint events from Sysmon into Splunk for search and analysis.

Although the author is retired and not pursuing employment, this environment is designed with professional rigor and can be reused for teaching, mentoring, or research.

Architecture

This diagram provides a high-level overview of the full telemetry architecture, including VirtualBox, the Windows VM, Sysmon, the Splunk Universal For-

warder, the Ubuntu VM, and Splunk Enterprise.

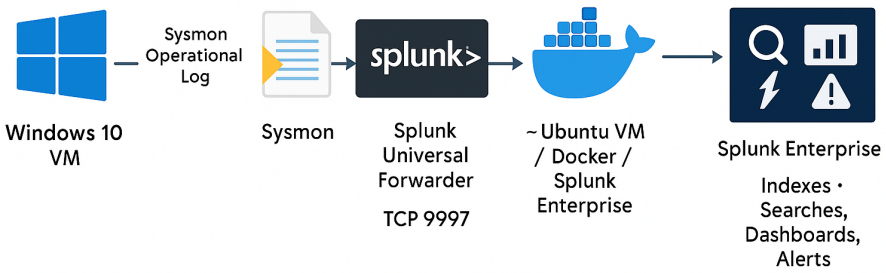

Figure 1: Architecture Diagram

Network Diagram

This diagram shows the virtual network layout connecting VirtualBox, the Windows VM, Sysmon, the Universal Forwarder, the Ubuntu VM, and Splunk Enterprise.

High-Level Event Flow

```
[ Windows 10 VM ]
   Sysmon → Sysmon Operational Log
      → Splunk Universal Forwarder
         → TCP 9997
            → [ Ubuntu VM / Docker / Splunk Enterprise ]
               → Indexing → Searching → Dashboards → Alerts
```

Data Flow Diagram

This diagram illustrates the end-to-end path of telemetry as it leaves Sysmon on the Windows VM, moves through the Splunk Universal Forwarder, is transmitted over TCP 9997, and is finally indexed and searchable inside Splunk Enterprise.

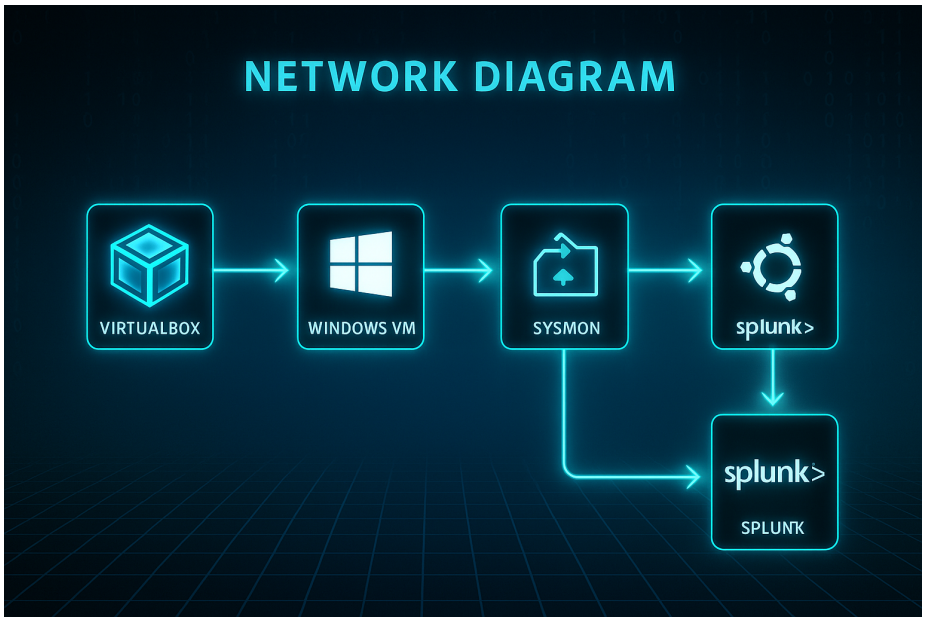

Figure 2: Network Diagram

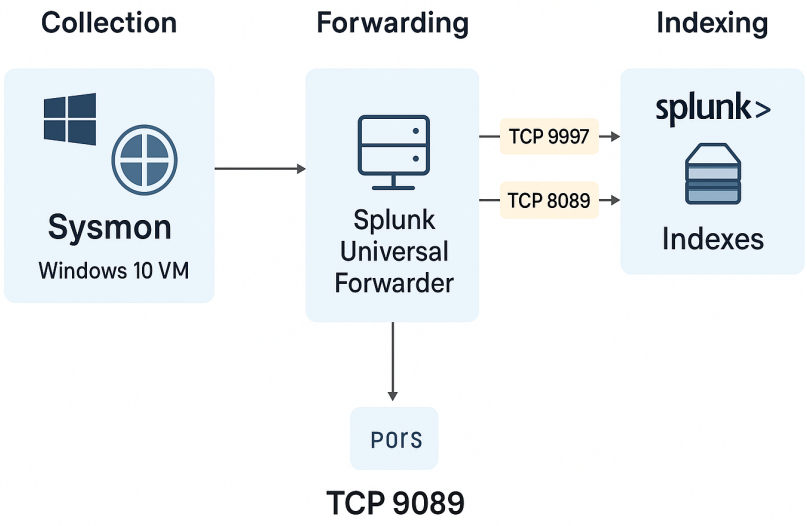

Figure 3: Data Flow Diagram

Sysmon Event Lifecycle

This diagram illustrates how a Windows event is created on the endpoint, captured and enriched by Sysmon, forwarded by the Splunk Universal Forwarder, transmitted across the virtual network, parsed and indexed by Splunk Enterprise, and ultimately made searchable for analysis.

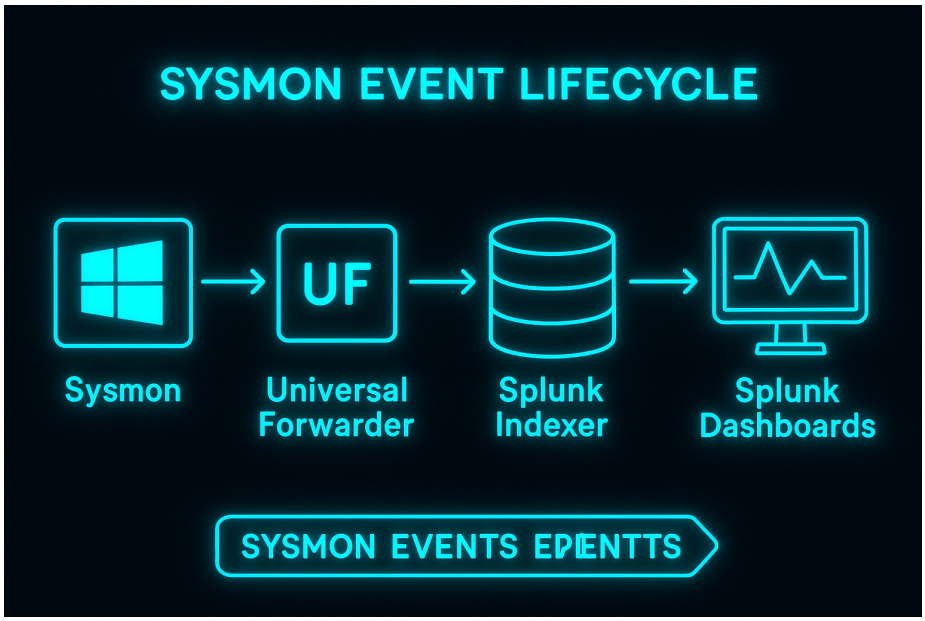

Figure 4: Sysmon Event Lifecycle

Components

- **VirtualBox**: Hypervisor for both Windows and Ubuntu VMs.
- **Windows 10 VM**: Endpoint under observation.
- **Sysmon**: Provides detailed host telemetry.
- **Splunk Universal Forwarder**: Ships logs from Windows to Splunk.
- **Ubuntu VM + Docker**: Host environment for Splunk Enterprise.
- **Splunk Enterprise**: Indexes and analyzes telemetry sent by the forwarder.

Key Use Cases

- Study process creation, network connections, registry modifications, and DNS activity.
- Practice digital forensics and incident response workflows.
- Experiment with building detection logic in Splunk.

- Use as a foundation for graduate projects or future research (e.g., ransomware profiling, anomaly detection).

SPL Query Pipeline (Optional)

This diagram illustrates how Splunk processes SPL queries through parsing, optimization, dispatching, search pipelines, and visualization. It highlights how raw Sysmon telemetry becomes fully searchable and actionable inside Splunk.

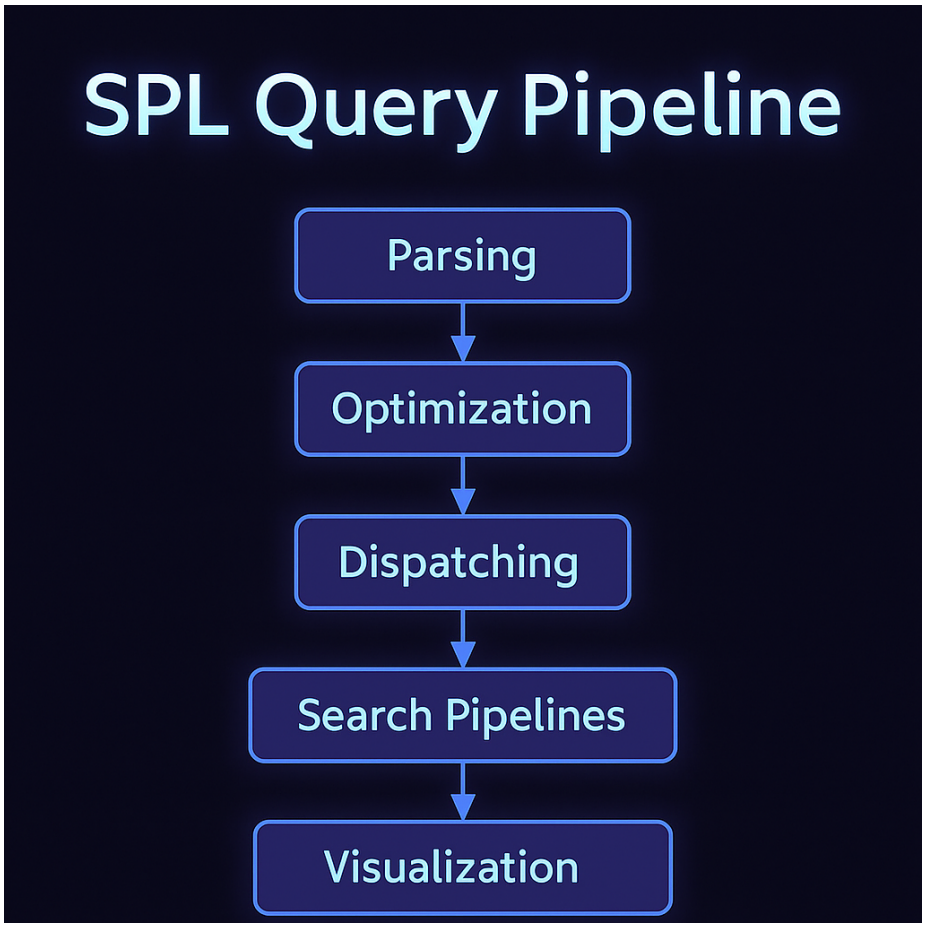

Figure 5: SPL Query Pipeline

Folder Structure (suggested)

```
Cybersecurity-Telemetry-Pipeline/
   README.md
   Cybersecurity_Telemetry_Pipeline_Report.docx
```

```
Cybersecurity_Telemetry_Pipeline_Report.pdf  (optional)
Architecture Diagram.png
Network Diagram.png
Data Flow Diagram.png
Sysmon Event Lifecycle Diagram.png
SPL Query Pipeline Diagram.png
configs/                (optional, for future use)
    sysmonconfig-export.xml
```

Credits

Sysmon — Microsoft Sysinternals
Provides advanced endpoint telemetry including process creation, network connections, file operations, and registry events.
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon Configuration — SwiftOnSecurity
Widely-used community configuration optimized for noise reduction and security analytics.
https://github.com/SwiftOnSecurity/sysmon-config

Splunk Universal Forwarder — Splunk Inc.
Lightweight agent responsible for securely forwarding Windows telemetry to Splunk Enterprise.
https://www.splunk.com/en_us/download/universal-forwarder.html

Splunk Enterprise — Splunk Inc.
Indexes, parses, and analyzes the telemetry generated in this lab environment, supporting dashboards, searches, alerts, and analytics.
https://www.splunk.com/en_us/download/splunk-enterprise.html

Virtualization Platform — Oracle VirtualBox
Provides the virtual environment for both Windows and Ubuntu systems used in this telemetry pipeline.
https://www.virtualbox.org/

Acknowledgments

This project leverages open-source and community-driven tooling to support cybersecurity education.
Special thanks to the Sysinternals team, Splunk community researchers, and SwiftOnSecurity for maintaining high-quality resources.

This project is intended for personal development, FIU graduate coursework, and exploratory cybersecurity research.

References (APA 7th Edition)

Microsoft. (2024). *Sysmon - System Monitor*. Microsoft Sysinternals. https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

SwiftOnSecurity. (2023). *Sysmon configuration*. GitHub repository. https://github.com/SwiftOnSecurity/sysmon-config

Splunk Inc. (2024). *Splunk Universal Forwarder*. https://www.splunk.com/en_us/download/universal-forwarder.html

Splunk Inc. (2024). *Splunk Enterprise*. https://www.splunk.com/en_us/download/splunk-enterprise.html

Oracle. (2024). *VirtualBox virtualization platform*. https://www.virtualbox.org/