

Contents

Cybersecurity Telemetry Pipeline	1
Overview	1
Architecture	1
Components	2
Key Use Cases	2
Folder Structure (suggested)	2
Credits	2

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

High-level event flow:

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

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).

Folder Structure (suggested)

```
Cybersecurity-Telemetry-Pipeline/
 README.md
 lab-report/
   Cybersecurity_Telemetry_Pipeline_Report.docx
   Cybersecurity_Telemetry_Pipeline_Report.pdf  (optional)
 configs/
   sysmonconfig-export.xml
 scripts/
   splunk-forwarder-setup.ps1
   docker-splunk-startup.sh
 diagrams/
   architecture.png
   dataflow.png
 screenshots/
   sysmon-operational.png
   splunk-indexes.png
   uf-forward-server.png
```

Credits

- Sysmon: Microsoft Sysinternals

- Sysmon configuration: SwiftOnSecurity
- Splunk Enterprise and Universal Forwarder: Splunk Inc.
- Virtualization: Oracle VirtualBox

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