**Part 1 - Setup LimaCharlie**

LimaCharlie is a **SecOps Cloud Platform** that provides **EDR capabilities, log ingestion, and a threat detection engine**. The following steps outline the installation and configuration process for deploying LimaCharlie on a Windows VM.

**Installation Process**

1. **Creating a LimaCharlie Account**
   * Signed up for a **free LimaCharlie account**.
   * Created an **organization**, ensuring the name was unique.
   * Selected the nearest **data residency** option.
2. **Adding a Sensor**
   * Navigated to **"Add Sensor"** in the LimaCharlie dashboard.
   * Selected **Windows** as the platform.
   * Provided a description (e.g., *Windows VM - Lab*).
   * Created an **installation key**.
3. **Installing the Agent on the Windows VM**
   * Downloaded the **x86-64 (.exe) sensor**.
   * Opened **Command Prompt as Administrator** on the Windows VM.
   * Navigated to the directory where the **sensor was downloaded**.
   * Executed the installation command:

lc\_sensor.exe -i [installation\_key]

* + Confirmed installation by checking the **LimaCharlie Web UI** for the reporting sensor.

1. **Configuring Sysmon Log Collection**
   * Added an **Artifact Collection Rule** in LimaCharlie.
   * Set the following parameters:
     + Name: windows-sysmon-logs
     + Platforms: Windows
     + Path Pattern: wel://Microsoft-Windows-Sysmon/Operational:\*
     + Retention Period: 10 days
   * Enabled Sysmon log ingestion to supplement LimaCharlie’s EDR telemetry.
2. **Enabling Sigma Rules**
   * Navigated to **LimaCharlie’s Extensions menu**.
   * Searched for **Sigma rules** (ext-sigma).
   * Subscribed to the **open-source Sigma ruleset** for enhanced detection.

**Conclusion**

LimaCharlie was successfully installed on the Windows VM, with **Sysmon log collection and Sigma rule-based threat detection enabled**. The setup allows for **endpoint monitoring, log analysis, and security event detection**.