**Part 3: Creating Detection Rules and Examining Telemetry**

In Part 3, I delved into the world of detection rules and telemetry analysis using the LimaCharlie platform, honing my skills in identifying and responding to security incidents effectively. Here's a breakdown of what I accomplished and the skills I acquired:

1. **Telemetry Analysis:**
   * Explored the LimaCharlie platform, a powerful endpoint detection and response (EDR) solution, to analyze telemetry data generated by the compromised systems in the lab environment.
   * Gained insights into various telemetry attributes, including process information, network connections, and file system activities, to identify potential threats and anomalous behaviors.
2. **Sigma Rule Language:**
   * Developed a strong understanding of Sigma, a rule-based language used to create detection rules within the LimaCharlie platform.
   * Acquired the skills to craft custom detection rules by defining conditions, event types, process names, command line arguments, and other relevant attributes to identify specific threat activities effectively.
3. **Custom Detection Rules:**
   * Created custom detection rules using Sigma syntax to identify and flag specific behaviors and activities associated with potential security incidents.
   * Enhanced my ability to proactively detect and respond to threats by leveraging custom detection rules tailored to the organization's environment and threat landscape.
4. **Threat Intelligence Integration:**
   * Leveraged threat intelligence sources and IOCs (Indicators of Compromise) to augment detection rules and enhance the identification of potential threats.
   * Developed proficiency in integrating external threat intelligence feeds and leveraging open-source intelligence (OSINT) to enrich telemetry analysis and improve threat detection capabilities.

