Splunk Lab — Investigating Ransomware with Boss-of-the-SOC

Prepared by: Lokesh

Executive Summary

The Splunk “Investigating Ransomware” workshop provides a hands-on approach to understanding incident investigation within a Security Operations Center (SOC) environment. Leveraging the Boss-of-the-SOC (BOTS) dataset 1.0, this exercise simulates realistic ransomware activity in a controlled environment. The primary objective was to explore how Splunk can be used to monitor, detect, and investigate suspicious activity, gaining practical experience in analyzing security events, correlating logs, and extracting meaningful insights from alert data.
The lab emphasized the use of open-source threat intelligence to enrich event data, allowing for a better understanding of attack patterns and threat actor behavior. The exercise also reinforced key SOC concepts such as alert triage, incident classification, and documentation of findings.

Objective

The main goals of this exercise were to:

- Gain practical experience investigating simulated ransomware incidents using Splunk.
- Understand how to search and filter events to answer investigative questions.
- Learn to correlate alerts and logs to build a complete picture of an incident.
- Document findings in a structured manner suitable for SOC workflows.
- Explore the use of threat intelligence to validate and enrich alert data.

Background

In a real SOC, analysts must sift through a large volume of logs from multiple sources to detect and respond to incidents. The Splunk BOTS environment replicates this challenge by presenting a series of questions based on simulated events. Analysts must use Splunk searches and dashboards to investigate these events and answer scenario-specific questions.
This exercise highlights the importance of visibility, correlation, and timely decision-making. Analysts are trained to prioritize alerts, identify indicators of compromise, and map findings to potential threats. The hands-on approach ensures participants gain familiarity with real-world investigative workflows.

Methodology

The lab followed a structured investigation workflow:

1. **Scenario Familiarization:**
    - Reviewed the ransomware scenario and related BOTS dataset.
    - Understood the context of potential indicators of compromise and system activity patterns.
2. **Event Exploration and Analysis:**

    - Explored Splunk dashboards to visualize event trends.
    - Used searches to identify suspicious activity, including potential ransomware-related behaviors.
    - Cross-referenced events with open-source threat intelligence to validate anomalies.
3. **Investigation and Correlation:**
    - Correlated events across multiple sources to piece together the incident timeline.
    - Evaluated critical events and alerts to determine their relevance to the ransomware scenario.
    - Extracted insights regarding attack progression and potential impact.
4. **Documentation and Reporting:**
    - Captured screenshots of key dashboards and search results as evidence of analysis.
    - Summarized investigative findings, noting observations and conclusions drawn from the scenario.

Observations and Findings

- **Ransomware Indicators:** Certain events indicated potential ransomware activity, such as suspicious file modifications and anomalous process execution.
- **Alert Correlation:** By correlating multiple events, it was possible to reconstruct an approximate timeline of the simulated attack.
- **Threat Intelligence Integration:** Utilizing threat intelligence sources helped to contextualize observed activity and validate potential indicators of compromise.
- **Visualization Utility:** Splunk dashboards provided clear, actionable insights, making it easier to monitor trends and detect anomalies.

While not all exact queries and details of the exercise are captured, selected excerpts and screenshots from the lab environment are included to demonstrate the investigative process and highlight key learning points. These artifacts showcase the application of SOC principles in a practical setting.

Lessons Learned

- Structured investigation workflows are essential for efficiently analyzing security events.
- Event correlation across multiple sources enhances understanding of incident scope and impact.
- Dashboards and visualizations are powerful tools for monitoring and quickly identifying anomalies.
- Documenting findings, even in simulated exercises, reinforces good SOC practices.
- Integration of threat intelligence supports informed decision-making during investigations.

Conclusion

The Splunk Boss-of-the-SOC ransomware lab provided valuable hands-on experience in SOC operations, particularly in event investigation, alert analysis, and threat intelligence

application. The exercise strengthened foundational skills in ransomware detection and incident investigation. Screenshots and excerpts from the lab demonstrate engagement with the scenario, highlighting the ability to analyze and interpret security events in a structured manner.

Overall, this lab underscores the importance of Splunk as a central tool for SOC analysts, enabling visibility, detection, and effective response to potential threats. The exercise serves as a strong foundation for future hands-on SOC training and practical incident response exercises.