Lab #2

You are working as a Cyber Security Analyst in the Security Operations Center (SOC) of a mid-sized enterprise organization that operates a hybrid on-premises and cloud environment. During routine monitoring, the SOC observes irregular firewall activity originating from both internal and external IP addresses.

Initial observations:

- A spike in denied inbound connection attempts from an external IP targeting internal system
- Unusual outbound connections from an internal host to unfamiliar external IP addresses using non-standard ports
- Periods of high outbound data transfer that may indicate either legitimate business operations or potential data exfiltration

At this stage, it is unclear whether the observed behavior represents a confirmed security incident, benign operational activity, or a false positive. To support further investigation, the SOC has extracted a sample firewall log covering the time window of interest and has requested your assistance in analyzing the data.

Your task is to analyze the data and provide some insight into what it means. Please note that You are not required to identify a confirmed breach; rather, the objective is to analyze the data, identify suspicious patterns, and justify whether the activity is benign or potentially malicious.

Activities:

1. **Data Ingestion:** Import the raw firewall log into a data analysis tool of your choice (Splunk, ELK Stack, Graylog, Wazuh, Jupiter Notebook etc.). The focus is on analysis and reasoning, not the tool itself. In this step you understand the structure of the logs and become familiar with the available fields.

2. **Data Preprocessing:** clean the data by addressing missing values, handling irrelevant columns, and converting timestamps to a consistent format.

3. **Anomaly Detection:** Identify anomalous patterns such as traffic spikes, repeated denied connections, unusual ports, or unexpected source/destination IP behavior.

4. **Threat Correlation:** Participants cross-reference their findings with known threat indicators, such as IP addresses associated with malicious activities. They assess whether any identified anomalies align with existing threat profiles. You must explain why an anomaly is likely benign or malicious, even if no confirmed threat is identified.

5. **Data Analysis Report:** Based on the analysis, create a data analysis report. This includes recommended actions to mitigate threats, isolate compromised systems, and communicate with relevant stakeholders.

6. **Reporting and Documentation:** compile the findings, analysis into a concise report suitable for presentation to management or a cybersecurity team.

Objectives:

The lab exercise aims to achieve the following learning objectives:

- Data preprocessing: Participants will clean and prepare the raw network logs for analysis.
- Anomaly detection: Participants will identify unusual patterns and potential security breaches within the network traffic.
- Threat identification: Participants will correlate findings with known threat indicators and assess their severity.
- Incident response: Participants will formulate a analysis report based on their analysis findings.

Outcome:

- Familiar with hands-on experience in dissecting security data to identify potential threats and vulnerabilities.
- Familiar with the various stages of data preprocessing, anomaly detection, threat correlation, and incident response planning, participants enhance their ability to recognize and respond to cybersecurity incidents effectively.

Deliverables

- Submit a data analysis report on Brightspace by **February 15, 2026, 11:59 PM.**
- You must include screenshots of the **Steps 2,3 and 4** in your final report as evidence of your data analysis activities
- Submission must be in the PDF format
- Name your submission file as **Firstname_Lastname_Lab2.pdf**
- Late submission will be penalized by 10% for each day after the submission deadline.