Chapter 2

**Research about cybersecurity use cases which align with work of current employer**

Following are some of the cybersecurity uses cases used in the organization: -

1. Classification of email as spam and non-spam, phishing and non-phishing.
2. Analyzing Indicators of Compromise (IOCs) for intrusion detection system.
3. Identifying potential threats in network traffic.
4. UEBA for anomaly detection
5. Inadvertent Data Disclosure (IDD)

# Classification email as spam and non-spam, phishing and non-phishing: -

* + 1. All employees in the organization have an option to report a suspicious email received by them.
    2. Once an email is reported, it goes to respective cybersecurity team and parsed against different set of rules.
    3. Based on the outcome of parsing, the email is classified as spam or non-spam, phishing or non- phishing.
    4. If there are no issues observed, the email is classified as clean.
    5. In the background, there is an automated email checker which keeps track of all emails

received by employees, and validates if it’s an authentic email or a suspicious email.

* + 1. For suspicious emails, it checks more of its meta data for further analysis and actions.
    2. Most of the times, it checks for credential harvester attack since its one of the most common cyberattacks observed over email.

# Analyzing Indicators of Compromise for intrusion detection system: -

* + 1. Matching and fetching details of IOCs is essential to build detection rules and models for intrusion detection system.
    2. Some of the examples of types of IOCs: IP address, Domain name, File hash, Email address, URL.
    3. Building IOC scanner helps to quickly detect cyber threats and enable SOC team to get details faster for their usage to handle and resolve the issue in less turnaround time.
    4. IOC for Incident Response: When a breach is suspected: -
       1. A list of all relevant IOCs is made.
       2. All logs are scanned to check for presence of the list of IOCs.
       3. The IOCs that match in the logs are determined and their details are fetched such as:-
          1. First seen
          2. Last seen
          3. Count
          4. Number of distinct users against which it was observed
          5. Number of distinct hosts against which it was observed
       4. Based on the data, impacted systems are analyzed.
       5. The timeline and scope of breach is determined.
    5. IOC for threat hunting: -
       1. An IOC is searched across all logs.
       2. The list of IOCs is made based on historical threats that are previously observed and documented. Thus, it is built based on Advanced Persistent Threats (APTs).
       3. Among the list of known IOCs, the IOCs that match in logs are analyzed by fetching the meta data such as: -
          1. First seen
          2. Last seen
          3. Count
          4. Number of distinct users against which it was observed
          5. Number of distinct hosts against which it was observed
       4. As per the requirements, more details are fetched
       5. If the events observed in logs are classified as malicious, then actions such as quarantining and isolation are carried out.
       6. Since logs are generated at run time, fetching all the relevant information and computing statistics can be time consuming.
       7. Thus, in order to improve efficiency, summary tables are built and maintained for each type of IOC, and searched are performed on those summary tables. This helps to fasten the searches and reduce turn-around time while searching on vast volume of data or searching data across long time range.

# Identifying potential threats in network traffic: -

* + 1. In network traffic, there are logs generated based on user activities.
    2. But sometimes, we observe logs having spikes at unusual hours. For example, transaction activities carried out 2 am.
    3. Thus, such events require macro and micro level monitoring and analysis to identify such events.
    4. Many times, most of the activities tracked as unusual are normal events, caused due events like: -
       1. Some batch job which was executed after resolving its error.
       2. Activities carried out in business hours of another time-zone.
    5. Thus, the occurrence of malicious events are rare, but identifying them is extremely critical.

# UEBA for anomaly detection: -

* + 1. Here the focus is on homogenous population in the organization that have similar and repetitive patterns of behavior.
    2. For creating baseline of users, we try to find users who are similar and then form a baseline based on their behavior pattern.
    3. Along with the anomaly, its rank in terms of impact will also be computed and used to reduce the alerts, prioritize the most important issues among all the alerts.

# Inadvertent Data Disclosure (IDD): -

* + 1. It is used for detecting and preventing misdirected emails.
    2. Example: Detecting sensitive data such as SSNs.
    3. It also used Titus classification for automated identification of sensitive data in email

and in attachments attached in the email.

* + 1. The scanning is also carried out for data that is stored in the system of employees. Thus, if some employee has data which contains PII information of users, it detects the file name and file path and generates email to notify the employee and the manager about and ask to take actions such as moving data out from employee’s storage or deleting the files if they are not required.