SKILLS FOR CYBER SECURITY ANALYST L1 TO STEP UP THEIR GAME

BY IZZMIER IZZUDDIN

BREAKDOWN OF SKILL NEEDED

1. Advanced Threat Detection and Analysis

- **Skills Required:**
  - **Knowledge of Threats:** Understanding of advanced persistent threats (APTs), malware types, and sophisticated attack vectors.
  - **Detection Techniques:** Proficiency in using SIEM, IDS/IPS systems to detect and analyse complex threats.
  - **Threat Intelligence:** Ability to leverage threat intelligence feeds and reports.
  - **Forensic Analysis:** Skills in forensic analysis to investigate and understand the scope of attacks.
  - **Behavioural Analysis:** Identifying unusual patterns and behaviours indicative of advanced threats.
- **Tools and Technologies:**
  - SIEM platforms (Splunk, QRadar, etc.)
  - IDS/IPS systems (Snort, Suricata)
  - Threat intelligence platforms

2. Incident Response and Handling

- **Skills Required:**
  - **Incident Management:** Knowledge of the incident response lifecycle (identification, containment, eradication, recovery).
  - **Playbook Creation:** Ability to develop and implement incident response playbooks.
  - **Forensic Skills:** Competence in conducting forensic investigations and preserving evidence.
  - **Coordination:** Skills in coordinating with different teams (IT, management, legal).
- **Tools and Technologies:**
  - Incident response platforms
  - Forensic tools (EnCase, FTK, etc.)
  - Communication and documentation tools

3. Use Case Creation

- **Skills Required:**
  - **Use Case Development:** Ability to identify and define security use cases for detecting specific threats.
  - **Rule Creation:** Proficiency in creating and implementing detection rules within SIEM systems.
  - **Testing and Tuning:** Skills in testing use cases and tuning them for accuracy.
  - **Data Analysis:** Ability to analyse data and adjust use cases based on evolving threats.

- **Tools and Technologies:**
  - SIEM platforms (Splunk, QRadar)
  - Query languages (e.g., SPL, AQL)

4. **Whitelisting**

- **Skills Required:**
  - **Whitelist Management:** Knowledge of how to implement and manage whitelists in a SIEM system.
  - **False Positive Reduction:** Ability to identify and whitelist benign activities to reduce false positives.
  - **Rule Configuration:** Skills in configuring rules and exceptions for whitelisting.
  - **Continuous Monitoring:** Competence in monitoring and adjusting whitelists as necessary.
- **Tools and Technologies:**
  - SIEM platforms (Splunk, QRadar)
  - Firewall and network monitoring tools

5. **Advanced OSINT Tools**

- **Skills Required:**
  - **OSINT Techniques:** Proficiency in using advanced open-source intelligence tools to gather and analyse information.
  - **Data Collection:** Ability to collect data from various sources (social media, public records, forums).
  - **Analysis:** Skills in analysing and correlating OSINT data for threat intelligence.
  - **Tool Utilization:** Familiarity with specific OSINT tools and platforms.
- **Tools and Technologies:**
  - OSINT platforms (Maltego, Shodan)
  - Social media monitoring tools

6. **Log Analysis and Correlation**

- **Skills Required:**
  - **Log Analysis:** Ability to analyse logs from various sources to identify patterns and anomalies.
  - **Correlation:** Skills in correlating log data to identify potential security incidents.
  - **Query Writing:** Proficiency in writing queries and custom searches within SIEM systems.
  - **Pattern Recognition:** Recognizing and interpreting patterns and trends in log data.
- **Tools and Technologies:**
  - SIEM platforms (Splunk, QRadar)
  - Log management tools

7. **Network Security Monitoring**

- **Skills Required:**
  - **Traffic Analysis:** Ability to analyse network traffic for signs of malicious activity.
  - **Protocol Knowledge:** Understanding of network protocols and their normal behaviour.
  - **Tool Usage:** Proficiency in using network monitoring tools and interpreting their outputs.
  - **Incident Detection:** Skills in detecting and responding to network-based attacks.
- **Tools and Technologies:**
  - Network monitoring tools (Wireshark, Zeek, Snort)
  - Network security appliances

8. **Reporting**

- **Skills Required:**
  - **Report Generation:** Ability to generate detailed and accurate security reports.
  - **Documentation:** Skills in documenting incidents, findings, and responses.
  - **Communication:** Proficiency in presenting findings to technical and non-technical audiences.
  - **Analysis:** Ability to analyse data and provide actionable insights.
- **Tools and Technologies:**
  - Reporting tools (JIRA, Confluence)
  - Data visualization tools

9. **Understanding Cybersecurity Frameworks**

- **Skills Required:**
  - **Framework Knowledge:** Familiarity with common cybersecurity frameworks (e.g., NIST, ISO 27001, CIS Controls).
  - **Implementation:** Ability to apply frameworks to organizational security practices.
  - **Compliance:** Understanding of compliance requirements and how frameworks support them.
  - **Assessment:** Skills in assessing and auditing security practices against frameworks.
- **Tools and Technologies:**
  - Framework documentation
  - Compliance assessment tools

10. **Communication and Collaboration**

- **Skills Required:**

    - **Effective Communication:** Ability to communicate clearly and effectively with team members and stakeholders.
    - **Collaboration:** Skills in working collaboratively with cross-functional teams.
    - **Reporting:** Proficiency in creating and delivering clear, actionable reports and updates.
    - **Conflict Resolution:** Handling conflicts and facilitating productive discussions.
- **Tools and Technologies:**
    - Collaboration tools (Slack, Microsoft Teams)
    - Presentation tools (PowerPoint, Google Slides)

EXAMPLES AND SIMULATIONS

1. Advanced Threat Detection and Analysis

- **Skill Development:** Learn how to identify, analyse and respond to advanced persistent threats (APTs), malware and other sophisticated attacks.

Example:

Scenario: Advanced Persistent Threat (APT) Infiltration via Phishing Campaign

Background: An organisation has been targeted by an APT group known for using spear-phishing emails to infiltrate networks. The group typically sends emails containing malicious attachments or links to lure employees into downloading malware that establishes a foothold in the network. The malware then communicates with a Command and Control (C2) server, allowing attackers to exfiltrate sensitive data and move laterally within the network.

Objective: To identify, analyse and respond to the APT infiltration using SIEM, IDS/IPS and threat intelligence tools like Splunk, QRadar and Wireshark.

Step 1: Detection of Suspicious Activity

1. **Initial Alert:**
    - The SIEM (Splunk) generates an alert for a suspicious email received by an employee, containing an attachment named "Invoice_2024.doc".
    - The attachment, when opened, triggers a download of a secondary payload from a remote server.
2. **Splunk Search Query:**
    - A search is conducted in Splunk for the email and its associated activities:

      ```
      index=email_logs sourcetype="exchange" subject="Invoice_2024.doc" | stats count by sender, recipient, attachment_name
      ```

      Result:

      ```
      2024-08-12 08:45   attacker@example.com   user@company.com
      Invoice_2024.doc     Invoice_2024.doc
      2024-08-12 08:47   attacker@example.com   user@company.com
      Invoice_2024.doc     Invoice_2024.doc
      ```

    - Another search checks for suspicious network traffic post-email reception:

      ```
      index=network_logs sourcetype="bro" uri_path="*/download*" | table _time, src_ip, dest_ip, uri_path
      ```

Result:

```
2024-08-12 08:50   192.168.1.10  203.0.113.45   /malware_payload.exe
GET    200
2024-08-12 09:10   192.168.1.10  203.0.113.45   /c2_communication
POST   200
2024-08-12 09:30   192.168.1.10  203.0.113.45   /data_exfiltration
POST   200
```

3. **Analysis:**
    - It shows that the user received an email from the attacker with a malicious attachment named "Invoice_2024.doc".The user's machine (192.168.1.10) accessed a remote IP (203.0.113.45) to download a payload and then engaged in C2 communication and data exfiltration.

Step 2: Analysing the Network Traffic (Wireshark)

1. **Capture Network Traffic:**
    - Use Wireshark to analyse the packet capture (PCAP) files related to the suspicious IP 203.0.113.45.
    - Apply the following filter:

      ```
      ip.addr == 203.0.113.45
      ```

      Result:

      ```
      35   9.520107   192.168.1.10    203.0.113.45    HTTP    671    POST
      /c2_communication HTTP/1.1
      36   9.520608   203.0.113.45    192.168.1.10    HTTP    255    HTTP/1.1 200
      OK
      ```

2. **Identification of C2 Communication:**
    - Wireshark analysis shows repetitive HTTP POST requests to the suspicious IP address. The payload contains encrypted data, indicating C2 communication.
3. **Analysis of Data Exfiltration:**
    - Further investigation shows that large volumes of data were exfiltrated over HTTPS, disguised as legitimate traffic.

Step 3: Investigating IDS/IPS Logs (QRadar)

1. **Suspicious Activity Detection:**
    - QRadar's IDS/IPS logs show multiple alerts for potential command and control activities:
        - **Alert 1:** Anomaly in DNS queries indicating domain generation algorithm (DGA) activity.
        - **Alert 2:** Excessive failed login attempts, potentially indicating lateral movement attempts.
2. **QRadar Query:**

  - Query the log for specific indicators of compromise (IoCs):

    ```
    SELECT * FROM events WHERE source_ip='192.168.1.10' AND
    event_type='C2 Activity'
    ```

    Result:

    ```
    2024-08-12 09:15   192.168.1.10  203.0.113.45   Suspicious C2 Activity
    High
    2024-08-12 09:20   192.168.1.10  10.0.0.15     Brute Force Login Attempt
    Medium
    2024-08-12 09:25   192.168.1.10  10.0.0.25     Lateral Movement Detected
    High
    ```

3. **Analysis:**
   - The IDS logs confirm that the suspicious DNS activity and C2 traffic correlate with the timeline of the detected malware execution.

Step 4: Threat Intelligence Correlation

1. **Threat Intelligence Platform (TIP) Correlation:**
   - Correlate the detected IP address (203.0.113.45) and domain with known threat actor activity.
   - The TIP identifies the IP and domain as associated with a known APT group.
2. **MITRE ATT&CK Framework:**
   - Map the activities to the MITRE ATT&CK framework:
     - **Execution:** User execution via spear-phishing link.
     - **Persistence:** Registry Run keys and startup folders.
     - **Command and Control:** C2 via HTTP/S.
     - **Exfiltration:** Data exfiltration over encrypted channels.

Step 5: Response and Mitigation

1. **Containment:**
   - Isolate the affected host (192.168.1.10) from the network.
   - Block all outbound traffic to the C2 IP (203.0.113.45).
2. **Eradication:**
   - Use endpoint detection and response (EDR) tools to remove malware.
   - Reset passwords and enforce multi-factor authentication (MFA) across the organisation.
3. **Recovery:**
   - Restore affected systems from clean backups.
   - Monitor network traffic for any signs of re-infection or residual activity.
4. **Post-Incident Analysis:**
   - Conduct a thorough review of the incident.

- Implement additional security measures, such as enhanced email filtering and user training.

2. Incident Response and Handling

- **Skill Development:** Understand the full incident response lifecycle, from identification to recovery.

Example:

Scenario: Ransomware Attack on Corporate Network

Background: A corporate network has been compromised by ransomware, which encrypted critical data on multiple servers. The attackers demand a ransom in cryptocurrency for the decryption key. The incident was first detected when users reported being unable to access files on shared drives and an extortion message appeared on their screens.

Objective: To handle the incident response lifecycle, from identification to recovery, using real data simulation. This includes understanding best practices, creating incident response playbooks, conducting forensic analysis and coordinating with different teams.

Step 1: Identification

1. **Detection of the Incident:**
    - Users report unusual behaviour on their systems. Files are inaccessible and a ransom note is displayed.
    - The security operations centre (SOC) receives alerts from the endpoint detection and response (EDR) system, indicating the presence of ransomware.
2. **Initial Analysis:**
    - **Splunk Query:**

      ```
      index=edr_logs sourcetype="endpoint" threat_name="*ransomware*" |
      stats count by host, file_path, threat_name
      ```

    - **Output:**

      ```
      Server01     C:\Users\Public\Documents   Locky Ransomware
      Server02     C:\HR\Payroll           Locky Ransomware
      ```

    - **Analysis:**
        - The query reveals the presence of "Locky Ransomware" on multiple servers.

Step 2: Containment

1. **Immediate Actions:**
    - Isolate affected systems from the network to prevent the spread of ransomware.

   - Disable shared drives and network connections on the compromised servers.
2. **Network Containment:**
   - **Splunk Query to Identify Other Potentially Affected Systems:**

     ```
     index=network_logs sourcetype="bro" dest_port=445 | table _time,
     src_ip, dest_ip, action
     ```

   - **Output:**

     ```
     2024-08-12 10:10   192.168.1.15  192.168.1.20   BLOCK
     2024-08-12 10:12   192.168.1.25  192.168.1.30   BLOCK
     ```

   - **Analysis:**
     - The query shows that lateral movement attempts using SMB (port 445) were blocked, containing the spread of ransomware.

Step 3: Eradication

1. **Malware Removal:**
   - Use antivirus/anti-malware tools to remove ransomware from infected systems.
   - **Command Used on Endpoints:**

     ```
     C:\> Remove-MalwareTool.exe /scan /clean
     ```

   - **Output:**

     ```
     Scanning for malware...
     Malware found: Locky Ransomware
     Removing malware...
     Malware removed successfully.
     ```

2. **Patch Vulnerabilities:**
   - Apply security patches to close the vulnerabilities that allowed the ransomware to enter the network.

Step 4: Recovery

1. **Data Restoration:**
   - Restore data from clean backups. Ensure that backups are free from ransomware before restoring.
   - **Splunk Query to Monitor Backup Restoration:**

     ```
     index=backup_logs sourcetype="restore" status="success" | stats count
     by host, file_path, backup_date
     ```

   - **Output:**

```
Server01     C:\Users\Public\Documents  2024-08-10     success
Server02     C:\HR\Payroll              2024-08-10     success
```

2. **Reintegrating Systems:**
    - Reconnect cleaned and restored systems to the network.
    - Monitor for any signs of re-infection or residual threats.

Step 5: Post-Incident Analysis and Reporting

1. **Root Cause Analysis:**
    - Conduct a forensic analysis to determine how the ransomware entered the network.
    - **Forensic Tools:**
        - **Disk Analysis:** Use FTK Imager to analyse disk images.
        - **Memory Analysis:** Use Volatility to analyse RAM for traces of ransomware execution.
2. **Splunk Query for User Activity Analysis:**

    ```
    index=authentication_logs sourcetype="windows" user="*" | table _time, user, action, host
    ```

    - **Output:**

        ```
        2024-08-12 08:00   izzmier     login_success    Server01
        2024-08-12 08:15   izzmier     open_file        Server01
        ```

    - **Analysis:**
        - The query shows user activities that may have contributed to the ransomware infection, such as opening a suspicious file.
3. **Incident Report Creation:**
    - Compile all findings, actions taken and lessons learned into an incident report.
    - Share the report with stakeholders and conduct a post-incident review meeting.

Step 6: Review and Update Incident Response Playbook

1. **Incident Response Playbook Update:**
    - Review the existing playbook for handling ransomware incidents.
    - Update procedures based on lessons learned from the incident.
2. **Training and Drills:**
    - Conduct a simulation drill for L1 analysts to practice the updated playbook.
    - Ensure that all team members understand their roles and responsibilities during an incident.

3. Use Case Creation

- **Skill Development:** Learn how to develop and implement effective use cases within a SIEM system to detect and respond to various security incidents.

Example:

Scenario: Use Case Creation for Detecting Suspicious Outbound Traffic

Background: A corporate network has recently experienced several incidents of data exfiltration where sensitive information was being sent to external, unauthorised locations. To improve detection capabilities and prevent similar incidents in the future, the SOC team needs to create a use case that monitors for suspicious outbound traffic patterns.

Objective: To develop a use case in the SIEM system that identifies unusual outbound traffic, which may indicate data exfiltration or other malicious activities. This involves defining the conditions, thresholds, and actions for the use case.

Step 1: Define the Use Case

- **Task:** Identify the specific conditions and patterns of outbound traffic that may indicate potential data exfiltration or malicious behaviour.
- **Use Case Components:**
    - **Event/Condition:** Large amounts of outbound traffic to external IP addresses or domains.
    - **Threshold:** More than 5GB of outbound traffic from a single host within a 30-minute window.
    - **Alert/Action:** Generate an alert in the SIEM and initiate further investigation or automated response actions.
- **Use Case Description:**
    - **Name:** Detection of Unusual Outbound Traffic
    - **Objective:** Identify and alert on unusually high outbound traffic that could indicate data exfiltration.

Step 2: Create and Implement the Use Case in SIEM

- **Task:** Develop the rules and configure the SIEM system to detect the conditions defined in the use case.
- **Example Implementation Steps:**
    1. **Define the Query:**
        - **Query:** Create a query to sum outbound traffic volume from each host and compare it against the defined threshold.
        - **Example Query (for a tool like Splunk):**

```
index=network_logs sourcetype=firewall_logs action=allowed
| stats sum(bytes) as total_bytes by src_ip
| where total_bytes > 5000000000  // 5GB in bytes
| stats count by src_ip
```

2. **Set Up the Alert:**
    - **Alert Configuration:** Configure the SIEM to generate an alert if the query results exceed the threshold.
    - **Alert Action:** Define the response actions, such as notifying the SOC team or triggering automated responses.
3. **Test the Use Case:**
    - **Simulated Traffic:** Generate simulated outbound traffic that meets and exceeds the threshold to test the use case.
    - **Verify Alerts:** Ensure that alerts are generated as expected and that legitimate traffic is not mistakenly flagged.

Step 3: Monitor and Refine the Use Case

- **Task:** Continuously monitor the effectiveness of the use case and make adjustments as needed to improve accuracy and relevance.
- **Monitoring Process:**
    - **Review Alerts:** Regularly review the alerts generated by the use case to ensure they are valid and actionable.
    - **Adjust Thresholds:** Fine-tune thresholds or conditions if the use case generates too many false positives or misses real incidents.
    - **Update Use Case:** Modify the use case based on evolving threats, changes in network patterns, or feedback from SOC analysts.

Step 4: Document and Report on the Use Case

- **Task:** Document the use case details, including the logic, configuration, and results.
- **Documentation:**
    - **Use Case Details:** Include the name, description, conditions, thresholds, and actions of the use case.
    - **Configuration Steps:** Provide detailed instructions on how to set up the use case in the SIEM system.
    - **Testing Results:** Summarize the results of testing, including any adjustments made.
- **Reporting:**
    - **Effectiveness Report:** Report on the performance of the use case, including the number of alerts generated, any missed incidents, and overall impact on incident detection.
    - **Recommendations:** Provide recommendations for further improvements or additional use cases based on the findings.

Step 5: Continuous Improvement

- **Task:** Implement a process for ongoing review and enhancement of use cases.
- **Process:**

- **Regular Reviews:** Schedule regular reviews of use cases to ensure they remain effective and relevant.
- **Incorporate Feedback:** Use feedback from SOC analysts and incident response teams to refine use cases and address any issues.
- **Stay Updated:** Keep up with new threats and changes in the network environment to update or create new use cases as needed.

4. **Whitelisting**

- **Skill Development:** Learn how to effectively implement and manage whitelisting in a SIEM system to reduce false positives and improve alert accuracy.

Example:

Scenario: Whitelisting Legitimate Internal Network Traffic

Background: A corporate network generates a large volume of security alerts due to regular internal activities, such as IT maintenance tasks, software updates, and routine internal communication between trusted servers. These benign activities frequently trigger false positives in the SIEM, overwhelming the SOC team and diverting attention from actual security threats.

Objective: To implement and test whitelisting in the SIEM system to reduce false positives from legitimate internal network traffic while ensuring that genuine threats are still detected.

Step 1: Identify Whitelisting Candidates

- **Task:** Review SIEM logs to identify recurring, benign activities that generate false positives. Examples include routine internal communication, known maintenance activities, and traffic from trusted IP ranges.
- **Whitelisting Candidates:**
    - **Internal IP Ranges:** Traffic between internal servers on IP ranges 10.0.0.0/24 and 192.168.1.0/24.
    - **IT Maintenance Activities:** Weekly system scans performed by IT from IP 192.168.1.10.
    - **Trusted Domains:** DNS queries to internal domains such as intranet.company.com.

Step 2: Create Whitelist Rules in SIEM

- **Task:** Develop rules within the SIEM to suppress alerts for the identified whitelisted activities.
- **Whitelist Rules:**
    1. **Whitelist Internal IP Communication:**
        - **Condition:** Traffic between IP ranges 10.0.0.0/24 and 192.168.1.0/24.
        - **Action:** Suppress alerts for these IP ranges unless external communication is detected.
    2. **Whitelist IT Maintenance Scans:**
        - **Condition:** Network scans originating from 192.168.1.10 during specified maintenance windows.
        - **Action:** Suppress alerts for these activities during the maintenance period.
    3. **Whitelist Trusted Domain Queries:**

        - **Condition:** DNS queries to intranet.company.com.
        - **Action:** Suppress alerts unless there is an abnormal spike in queries.

Step 3: Test Whitelist Implementation

- **Task:** Simulate network activity that includes both whitelisted and non-whitelisted events. Monitor the SIEM to verify that whitelisted activities no longer trigger alerts while ensuring that non-whitelisted suspicious activities still generate alerts.
- **Testing Scenario:**
    - Simulate internal server communication within the whitelisted IP ranges.
    - Run IT maintenance scans from the designated IP.
    - Generate DNS queries to the whitelisted domain.
    - Inject a simulated attack that is not part of the whitelist, such as an unauthorised login attempt from an external IP.
- **Outcome:**
    - The SIEM should not generate alerts for the whitelisted activities.
    - Alerts should be generated for the non-whitelisted simulated attack.

Step 4: Monitor and Adjust Whitelisting Rules

- **Task:** Continuously monitor the SIEM alerts after implementing whitelisting to ensure that false positives are reduced without missing genuine threats.
- **Adjustment Process:**
    - **Review:** Regularly review the effectiveness of the whitelist rules, especially after detecting any missed threats.
    - **Refine:** Adjust thresholds, conditions, or add/remove entities from the whitelist based on ongoing monitoring and feedback from SOC analysts.

Step 5: Documentation and Reporting

- **Task:** Document the whitelisting rules implemented, the rationale behind them, and their impact on reducing false positives.
- **Reporting:**
    - Summarise the reduction in false positives post-whitelisting.
    - Include any incidents where whitelisting needed adjustments.
    - Provide recommendations for ongoing whitelist management and periodic review.

5. **Advance OSINT Tools**

- **Skill Development:** Master the use of advanced OSINT tools to gather intelligence on potential threats, vulnerabilities and threat actors. Learn to effectively use tools like Maltego, Shodan, SpiderFoot and theHarvester to collect, analyse and correlate information from various sources.

Example:

Scenario: Investigating a Potential Threat Actor Involved in a Phishing Campaign

Background: A cybersecurity analyst is tasked with investigating a potential threat actor who has been involved in a recent phishing campaign targeting a financial institution.

Objective: To gather intelligence on the threat actor, identify their infrastructure and uncover any associated vulnerabilities using advanced OSINT tools like Maltego, Shodan, SpiderFoot and theHarvester.

Step 1: Initial Reconnaissance with Maltego

1. **Objective:**
    - Use Maltego to map out the digital footprint of the suspected phishing domain, email addresses and other associated entities.
2. **Steps:**
    - **Create a New Graph in Maltego:**
        - Start by entering the phishing domain (e.g., example-phishing.com) as a seed entity.
    - **Run Transforms:**
        - Run transforms to discover related domains, email addresses, IP addresses and other connected entities.
    - **Entities Discovered:**
        - **Domains:** example-phishing.com, example-threat.com
        - **IP Addresses:** 203.0.113.45, 198.51.100.23
        - **Email Addresses:** attacker@example-phishing.com
3. **Visualisation:**
    - The graph will visually represent the relationships between domains, IP addresses and email addresses, providing a clear overview of the threat actor's infrastructure.

Step 2: Network Infrastructure Analysis with Shodan

1. **Objective:**
    - Use Shodan to identify vulnerabilities and exposed services on the IP addresses associated with the phishing campaign.
2. **Steps:**
    - **Search Query in Shodan:**

203.0.113.45

- **Information Gathered:**
  - **Open Ports:** 80 (HTTP), 443 (HTTPS), 22 (SSH)
  - **Vulnerabilities:** CVE-2022-12345 (Critical)
  - **Services:** Apache 2.4.18, OpenSSH 7.2p2

3. **Analysis:**
   - The Shodan search reveals that the IP address 203.0.113.45 has several open ports and is running an outdated version of Apache with a critical vulnerability. This information suggests that the threat actor's infrastructure could be exploited.

Step 3: Detailed Threat Actor Profiling with SpiderFoot

1. **Objective:**
   - Use SpiderFoot to automate the collection of OSINT data related to the threat actor's domain, IP addresses and associated email addresses.
2. **Steps:**
   - **SpiderFoot Scan:**
     - Input the domain example-phishing.com into SpiderFoot and run a full scan.
   - **Results:**
     - **DNS Information:** Detailed DNS records, including subdomains.
     - **Email Addresses:** Confirmed attacker@example-phishing.com.
     - **Social Media Profiles:** Linked to the email address.
     - **Associated IPs:** Additional IPs linked to the domain, such as 198.51.100.23.
3. **Correlated Findings:**
   - The scan reveals more associated domains, emails and social media profiles, helping to build a comprehensive profile of the threat actor.

Step 4: Email Harvesting with theHarvester

1. **Objective:**
   - Use theHarvester to gather email addresses and subdomains related to the threat actor's domains.
2. **Steps:**
   - **Command:**

     ```
     theharvester -d example-phishing.com -l 500 -b google
     ```

   - **Output:**

     ```
     Email Addresses: attacker@example-phishing.com, admin@example-phishing.com
     Subdomains: mail.example-phishing.com, www.example-phishing.com
     ```

3. **Analysis:**

   - TheHarvester collects additional email addresses and subdomains, providing further insight into the phishing infrastructure and potential attack vectors.

Step 5: Correlating and Validating Information

1. **Objective:**
   - Correlate data from all OSINT tools to validate findings and ensure accuracy.
2. **Steps:**
   - **Cross-Check Data:**
     - Compare IP addresses, domains and email addresses found across Maltego, Shodan, SpiderFoot and theHarvester.
   - **Validation:**
     - The IP 203.0.113.45 appears in both Maltego and Shodan, confirming its relevance.
     - The email attacker@example-phishing.com is found in both SpiderFoot and theHarvester, validating its connection to the threat actor.
3. **Best Practices:**
   - Validate the information by cross-referencing with multiple sources.
   - Ensure that any identified vulnerabilities are confirmed by checking public databases like the National Vulnerability Database (NVD).

Step 6: Reporting and Actionable Intelligence

1. **Objective:**
   - Compile a report with all findings, including actionable intelligence on the threat actor's infrastructure, vulnerabilities and associated entities.
2. **Content of the Report:**
   - **Threat Actor Profile:** Summarise the threat actor's digital footprint, including domains, IPs and email addresses.
   - **Vulnerabilities:** Highlight critical vulnerabilities found in their infrastructure.
   - **Recommendations:** Provide actionable steps, such as blocking the identified IP addresses, monitoring the email addresses and updating vulnerable systems.
3. **Report Excerpt:**

   The phishing domain example-phishing.com is associated with IP 203.0.113.45, which has open ports (80, 443) and a critical vulnerability (CVE-2022-12345). The email attacker@example-phishing.com is linked to social media profiles that may offer further insights into the threat actor's identity. It is recommended to monitor and block this IP and domain across all network layers.

6. **Log Analysis and Correlation**

   - **Skill Development:** Improve your ability to analyse logs from various sources to identify patterns, anomalies and potential security incidents. Regularly participate in log analysis challenges and simulations.

Example:

Scenario: Suspicious Activities

Background:

A corporate network has experienced a series of suspicious activities that could indicate potential security threats. Logs from firewalls, web servers and antivirus software must be analysed to identify patterns, anomalies and potential security incidents. The focus of this training is to enhance log analysis and correlation skills.

Objective:

To improve the ability to analyse logs from various sources, identify patterns and anomalies and correlate events to detect and understand potential security incidents. The exercise includes hands-on analysis using simulated real data, followed by a detailed correlation of findings.

Step 1: Understanding the Log Sources

Log Sources:

1. **Firewall Logs:**
   - Capture information about network traffic, including source and destination IP addresses, ports, protocols and actions taken (allow/deny).
2. **Web Server Logs:**
   - Record HTTP requests, including client IP addresses, request methods, URLs, response codes, user agents and referrers.
3. **Antivirus Logs:**
   - Provide alerts on detected malware, including file paths, actions taken (e.g., quarantine or deletion) and timestamps.

Step 2: Log Sources

1. **Firewall Log:**

```
2024-08-12 10:15:34 Allow 192.168.1.100 10.0.0.5 TCP 80
2024-08-12 10:15:35 Deny 192.168.1.101 10.0.0.5 TCP 80
2024-08-12 10:15:36 Allow 192.168.1.102 10.0.0.5 TCP 443
2024-08-12 10:15:37 Deny 192.168.1.103 10.0.0.5 TCP 23
```

2. **Web Server Log:**

```
192.168.1.100 - - [12/Aug/2024:10:15:34 +0000] "GET /index.html HTTP/1.1" 200 512 "-" "Mozilla/5.0"
192.168.1.101 - - [12/Aug/2024:10:15:35 +0000] "POST /login.php HTTP/1.1" 403 324 "-" "Mozilla/5.0"
192.168.1.102 - - [12/Aug/2024:10:15:36 +0000] "GET /admin/ HTTP/1.1" 401 289 "-" "Mozilla/5.0"
192.168.1.103 - - [12/Aug/2024:10:15:37 +0000] "GET /telnet HTTP/1.1" 404 512 "-" "Mozilla/5.0"
```

3. **Antivirus Log:**

```
2024-08-12 10:15:36 [INFO] Malware detected: Troj/FakeAV-AX [Detected] on C:\Users\admin\downloads\malicious.exe [Quarantined]
2024-08-12 10:15:37 [INFO] Malware detected: W32/Sality [Deleted] on C:\Program Files\app\infected.dll [Deleted]
```

Step 3: Analysing the Logs

1. **Firewall Logs Analysis:**
   - **Observation:** The firewall log shows denied traffic from IP 192.168.1.101 trying to access port 80 and 192.168.1.103 trying to access port 23. Port 23 is typically associated with Telnet, which is often disabled due to security risks.
   - **Analysis:** The denial of access to port 23 suggests that there might be an attempt to exploit the Telnet service, potentially as part of a reconnaissance effort. The denied access to port 80 could indicate an unauthorised attempt to interact with a web server.
   - **Next Steps:** Investigate the source of these IPs and determine whether they are internal or external. If external, assess whether these could be part of a broader attack.
2. **Web Server Logs Analysis:**
   - **Observation:** The web server logs show a failed POST request to /login.php from 192.168.1.101, which returned a 403 Forbidden status, indicating that the access was blocked. Additionally, a request to /telnet from 192.168.1.103 returned a 404 Not Found status.
   - **Analysis:** The failed login attempt and the 403 error could indicate a brute-force attack or an attempt to exploit vulnerabilities in the login page. The request for /telnet, which does not exist on the server, aligns with the denied access attempt in the firewall log, indicating a probing attempt.
   - **Next Steps:** Investigate further to determine if these are isolated incidents or part of a more significant attack attempt. Check for any related logs that might provide additional context.
3. **Antivirus Logs Analysis:**

    - **Observation:** The antivirus log shows the detection and quarantine of malicious.exe on 192.168.1.102, coinciding with a failed access attempt to /admin/ on the web server. Another detection of W32/Sality on the same machine led to the deletion of the infected file.
    - **Analysis:** The presence of malicious.exe and the failed access to /admin/ suggest that the machine might have been compromised. The correlation between the time of malware detection and the failed admin access indicates a potential breach attempt using the compromised machine.
    - **Next Steps:** Conduct a full forensic analysis of 192.168.1.102 to determine the extent of the compromise. Correlate this event with network traffic to identify if the malware was attempting to propagate or communicate with an external command and control server.

Step 4: Correlation and Reporting

1. **Event Correlation:**
    - **Correlation:** The analysis suggests a coordinated attack involving multiple stages: initial probing from 192.168.1.103, a potential brute-force attack from 192.168.1.101 and a possible compromise of 192.168.1.102, which was detected by the antivirus software.
    - **Detailed Findings:**
        - **192.168.1.101:** Attempted unauthorised access to the web server, potentially a brute-force attack.
        - **192.168.1.103:** Engaged in reconnaissance activities, attempting to probe Telnet.
        - **192.168.1.102:** Likely compromised, with malware detected and possible unauthorised access attempts to admin areas of the web server.
    - **Conclusion:** The logs indicate a multi-stage attack with reconnaissance, brute-force attempts and potential compromise. The compromised system (192.168.1.102) poses a significant risk and should be isolated for further investigation.
2. **Reporting:**
    - **Summary:** Generate a report summarising the findings, including timelines, IP addresses involved, types of suspicious activities and the potential impact on the network.
    - **Recommendations:** Provide actionable recommendations, such as isolating compromised systems, blocking suspicious IP addresses and reviewing firewall and web server configurations to prevent similar attacks.

7. **Network Security Monitoring**

- **Skill Development:** Deepen your understanding of network protocols, traffic analysis and network-based attacks.

Example:

Scenario: Network Based Attack

Background:

A corporate network has been experiencing unusual traffic patterns and there are concerns about potential network-based attacks. The objective is to monitor the network in real-time, analyse traffic and identify any malicious activities. The focus of this training is to deepen the understanding of network protocols, traffic analysis and detecting network-based attacks using tools like Wireshark, Zeek (Bro) and Snort.

Objective:

To enhance the ability to monitor network traffic, understand network protocols and detect potential network-based attacks. The exercise includes hands-on practice using simulated real data and analysing the results with network monitoring tools.

Step 1: Understanding Network Monitoring Tools

Tools:

1. **Wireshark:**
   - A network protocol analyser that captures and displays network traffic in real-time. It allows detailed inspection of individual packets and is used for troubleshooting and analysing network issues.
2. **Zeek (Bro):**
   - A powerful network analysis framework that provides real-time monitoring of network traffic and logs detailed information about network events, such as HTTP requests, DNS queries and SSL handshakes.
3. **Snort:**
   - An open-source network intrusion detection system (NIDS) that analyses network traffic against a set of predefined rules to detect and alert on malicious activities.

Step 2: Data

1. **Network Traffic Capture (PCAP):**
   - The following simulated data represents a capture file of network traffic containing various protocols like HTTP, DNS and TCP.
2. **Traffic Patterns:**
   - **Normal Traffic:** Routine web browsing, DNS queries and secure HTTPS connections.

- **Suspicious Traffic:** Unusual TCP connections, repeated DNS queries to an unknown domain and an HTTP request containing a suspicious payload.

Step 3: Analysing the Network Traffic with Wireshark

1. **Capture Traffic:**
   - Use Wireshark to open the provided PCAP file and begin analysing the network traffic. Focus on identifying protocols, inspecting packet details and filtering for specific activities.
2. **Analysis:**
   - **TCP Connections:**
     - Identify a large number of connections originating from a single IP address (192.168.1.105) to various external IPs. These connections are made over non-standard ports.
     - **Action:** Investigate the source IP and examine the payloads for any signs of malicious intent. A detailed inspection of the data reveals the presence of a possible port-scanning activity.
   - **DNS Queries:**
     - Detect repeated DNS queries to an unknown domain (suspicious-domain.com). The queries are coming from multiple internal IP addresses within a short period.
     - **Action:** Examine the DNS responses to determine whether the domain is associated with known malicious activity. Correlate this with other traffic patterns to assess if it's part of a broader attack.
   - **HTTP Request:**
     - Identify an HTTP POST request containing a suspicious payload. The payload appears to be base64 encoded and the destination server is an external IP address not typically accessed by the network.
     - **Action:** Decode the base64 payload to reveal potential malicious content. Further analysis may indicate an attempted data exfiltration.

Step 4: Real-Time Monitoring with Zeek (Bro)

1. **Zeek Configuration:**
   - Set up Zeek to monitor live traffic and generate logs for various network protocols, including HTTP, DNS and SSL. Ensure that the logging configuration is set to capture detailed information about each event.
2. **Monitoring and Analysis:**
   - **HTTP Logs:**
     - Review the logs generated by Zeek for HTTP traffic. Focus on identifying unusual requests, such as those containing suspicious user agents, long URLs, or uncommon methods (e.g., PUT, DELETE).

        - **Analysis:** Identify an HTTP request with an abnormal user agent string (Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)) that doesn't match the usual pattern of traffic. The request includes a query parameter with what appears to be an SQL injection attempt.
    - **DNS Logs:**
        - Analyse DNS logs to detect repeated queries for the same domain or queries to known malicious domains.
        - **Analysis:** Zeek logs show consistent DNS requests to suspicious-domain.com, correlating with the Wireshark findings. This could indicate domain generation algorithm (DGA) activity commonly associated with botnets.
    - **SSL Logs:**
        - Inspect SSL/TLS connections, focusing on expired certificates, self-signed certificates, or connections to suspicious domains.
        - **Analysis:** An SSL connection to an IP address associated with known command-and-control servers is identified. The certificate is self-signed and does not match any trusted root authorities.

Step 5: Intrusion Detection with Snort

1. **Rule Configuration:**
    - Set up Snort with a set of predefined rules, including those designed to detect port scanning, SQL injection and suspicious DNS queries. Customize the rules to match the specific patterns identified in the previous analyses.
2. **Real-Time Detection:**
    - **Port Scanning:**
        - Snort triggers an alert for a potential port scan originating from 192.168.1.105, matching the pattern observed in the Wireshark analysis.
        - **Action:** Review the alert details and correlate with other logs to confirm the activity. This could be a precursor to more targeted attacks.
    - **SQL Injection:**
        - An alert is generated for a potential SQL injection attempt in the HTTP request. The rule detects the presence of typical SQL keywords in the request parameters.
        - **Action:** Immediately block the offending IP address and log the incident for further investigation. Verify if the injection attempt was successful or blocked by the application's security measures.
    - **Malicious DNS Query:**
        - Snort detects repeated DNS queries to suspicious-domain.com and raises an alert for potential DGA activity.
        - **Action:** Investigate the source of these queries and isolate any potentially compromised machines. Further inspection may reveal a broader infection within the network.

Step 6: Correlation and Reporting

1. **Event Correlation:**
   - **Combined Analysis:** The unusual traffic patterns observed in Wireshark, the detailed logging in Zeek and the alerts generated by Snort indicate a coordinated attempt to compromise the network. The patterns suggest reconnaissance followed by targeted attacks, including SQL injection and possible malware communication with external servers.
   - **Conclusion:** The network has likely been the target of an advanced persistent threat (APT), involving multiple stages such as reconnaissance, exploitation and potential data exfiltration.
2. **Reporting:**
   - **Summary:** Generate a report that summaries the identified suspicious activities, correlated events and potential security incidents. Include details on the tools used, the specific findings and the impact on the network.
   - **Recommendations:** Provide actionable recommendations, such as tightening firewall rules, blocking suspicious domains and conducting a full security audit to identify and mitigate any vulnerabilities.

8. Reporting

- **Skill Development:** Learn how to produce executive monthly and quarterly reports by transforming auto-generated SIEM reports into insightful executive summaries with analysis.

Example:

Scenario: Quarterly Security Operations Report for a Financial Institution

Background:

A financial institution requires a comprehensive Quarterly Security Operations Report to present to its executive team. The report should summarise security incidents, trends and overall security posture. The raw data will be sourced from auto-generated reports within the SIEM platform, which will then be analysed and presented in a format suitable for executive-level stakeholders.

Objective:

To enhance skills in producing executive monthly and quarterly reports by transforming auto-generated SIEM reports into insightful executive summaries with analysis.

Step 1: Download Auto-Generated Reports from SIEM

1. **Log in to SIEM:**
    - Access the SIEM platform (e.g., QRadar).
    - Navigate to the reporting section where standard reports are available.
2. **Select Relevant Reports:**
    - Identify and download reports that cover incident summaries, threat detection statistics and compliance metrics.
    - Common reports might include:
        - **Incident Summary Report:** Provides details on security incidents detected and handled.
        - **Threat Detection Report:** Shows trends in detected threats, categorised by type, severity and impacted assets.
        - **Compliance Report:** Evaluates adherence to security policies and regulatory requirements.
3. **Export Data:**
    - Export these reports in a format suitable for analysis (e.g., CSV, PDF).

Step 2: Analyse and Summarise Key Insights

1. **Data Review:**
    - Open the exported reports and review the data.
    - Focus on identifying trends, patterns and anomalies in the incident and threat data.

    - Note any recurring issues, significant incidents, or improvements in security posture.
2. **Trend Analysis:**
    - Compare data across the months to identify significant trends.
    - Highlight key areas such as:
        - Increase or decrease in phishing attempts.
        - Changes in the number of detected malware variants.
        - New types of attacks or vulnerabilities identified.
    - Use Excel to create graphs and charts that visually represent these trends.
3. **Key Metrics and KPIs:**
    - Extract key performance indicators (KPIs) relevant to executive stakeholders, such as:
        - Mean time to detect (MTTD) and mean time to respond (MTTR).
        - Percentage of incidents resolved within SLA.
        - Number of critical incidents vs. total incidents.
    - Summarise the most impactful metrics in the report.

Step 3: Prepare the Executive Report

1. **Structure the Report:**
    - **Executive Summary:** Provide a high-level overview of the security posture and key findings.
    - **Incident Overview:** Summarise the number and types of incidents detected, with comparisons to previous periods.
    - **Threat Landscape:** Discuss emerging threats and how they were mitigated.
    - **Compliance Status:** Report on the organisation's compliance with relevant standards and regulations.
    - **Recommendations:** Offer actionable recommendations for improving security posture.
2. **Visual Presentation:**
    - Use PowerPoint to create a polished executive report.
    - Include graphs, charts and infographics to make the data easily digestible.
    - Ensure that the visual elements align with the company's branding and are easy to understand for non-technical executives.
3. **Review and Refine:**
    - Review the report for accuracy and clarity.
    - Ensure that the language is clear and concise, avoiding technical jargon.
    - Consider peer reviews to get feedback and make necessary adjustments.

Step 4: Report Example

Executive Quarterly Security Operations Report

Client: De Ligt Financial Institution
Period: Q2 2024
Prepared by: Izzmier Izzuddin
Date: July 15, 2024

a) Executive Summary

In Q2 2024, De Ligt Financial Institution experienced a moderate increase in security incidents, driven primarily by a rise in phishing attempts and malware detections. Despite the increase, the average response time (MTTR) improved by 15%, reflecting the effectiveness of recent incident response process optimisations. The overall security posture remains strong, with all critical incidents resolved within SLA targets.

b) Incident Overview

Total Incidents Detected: 475
Total Critical Incidents: 15
Resolved within SLA: 100%

Incident Type	Q1 2024	Q2 2024	% Change
Phishing Attempts	120	185	+54%
Malware Detections	98	130	+33%
Unauthorised Access	45	50	+11%
DDoS Attacks	5	3	-40%

Analysis:

- **Phishing Attempts:** The significant increase in phishing attempts (54%) suggests that attackers are increasingly targeting employee credentials. This necessitates additional user training and improved email filtering.
- **Malware Detections:** A 33% rise in malware detections indicates a growing threat landscape. Enhanced endpoint protection and regular updates to threat intelligence feeds are recommended.

c) Threat Landscape

Emerging Threats:

- **Ransomware Variant (Xcrypt):** Detected in 10 instances, leveraging spear-phishing as an initial attack vector.
- **New Phishing Techniques:** Attackers are using more sophisticated social engineering tactics, leading to a higher click-through rate on malicious links.

Threat Intelligence Summary:

- **High-Risk IP Addresses:** 25 new IPs identified and blacklisted.
- **Malicious Domains:** 40 domains flagged and blocked.

Response & Mitigation:

- Increased monitoring and automated blocking of identified high-risk IPs and domains.
- Strengthened endpoint detection and response (EDR) capabilities.

d) Compliance Status

Regulatory Compliance:

- **PCI-DSS:** Full compliance maintained.
- **GDPR:** No breaches reported; all data processing activities remain compliant.

Security Audits:

- **Internal Audits:** 2 audits conducted, with no major findings.
- **Third-Party Audits:** Completed, with minor recommendations for improving network segmentation.

e) Key Performance Indicators (KPIs)

KPI	Q1 2024	Q2 2024	% Change
Mean Time to Detect (MTTD)	2 hours	1.8 hours	-10%
Mean Time to Respond (MTTR)	4 hours	3.4 hours	-15%
Percentage of Incidents Resolved	92%	97%	+5%
Number of Vulnerabilities Patched	120	145	+21%

Analysis:

- **MTTD/MTTR Improvement:** The reduction in detection and response times highlights the effectiveness of process optimisations and the introduction of automated detection tools.
- **Vulnerability Management:** The increase in patched vulnerabilities demonstrates proactive efforts in reducing the attack surface.

f) Recommendations

1. **Enhanced Phishing Training:** Implement quarterly phishing simulation exercises to train employees on recognising sophisticated phishing attempts.
2. **Upgrade Email Filtering:** Invest in advanced email filtering solutions to reduce the volume of phishing emails reaching end-users.
3. **Threat Hunting:** Establish a proactive threat-hunting program to identify and mitigate potential threats before they escalate into incidents.
4. **Compliance Monitoring:** Continue monitoring compliance status, especially in light of evolving regulatory requirements.

g) Conclusion

Q2 2024 was marked by an increase in threat activity, particularly in phishing and malware incidents. However, the improvements in response times and the proactive measures implemented demonstrate XYZ Financial Institution's commitment to maintaining a robust security posture. The recommendations provided will help further enhance security operations and protect against emerging threats.

9. **Understanding Cybersecurity Frameworks**

- **Skill Development:** Familiarise yourself with key cybersecurity frameworks such as NIST, ISO/IEC 27001 and the MITRE ATT&CK framework.

Example:

Scenario: Enhancing Security Posture and Compliance

Background:

A financial institution is undergoing an audit to ensure compliance with industry-standard cybersecurity frameworks. The organisation must demonstrate adherence to the NIST Cybersecurity Framework, ISO/IEC 27001 and effectively map its security operations to the MITRE ATT&CK framework. The objective is to assess the current security posture, identify gaps and implement necessary controls to achieve compliance and improve overall security.

Objective:

To deepen the understanding of cybersecurity frameworks and their practical application, focusing on how they can be utilised to assess and improve the security posture of an organisation. The exercise will involve hands-on practice with real-world scenarios and data, applying these frameworks to analyse the current state and recommend improvements.

Step 1: NIST Cybersecurity Framework (CSF) Assessment

Task: Conduct a baseline assessment of the organisation's current cybersecurity practices using the NIST CSF.

- **Identify:** Determine the organisation's current practices in the five core functions: Identify, Protect, Detect, Respond and Recover.
- **Analyse:** Use real audit data, such as existing security policies, risk assessments and incident reports, to identify areas where the organisation is strong and where there are gaps.
- **Document:** Create a report detailing the organisation's maturity level in each function and provide recommendations for improvement.

Output: A detailed maturity assessment report with recommendations to enhance the "Detect" function by integrating more advanced threat detection tools and enhancing monitoring capabilities.

Step 2: ISO/IEC 27001 Implementation

Task: Apply the ISO/IEC 27001 framework to implement and manage a comprehensive Information Security Management System (ISMS).

- **Scope Definition:** Define the scope of the ISMS based on the organisation's objectives and risk appetite.
- **Risk Assessment:** Perform a risk assessment using real data, identifying critical assets, threats, vulnerabilities and potential impacts.
- **Controls Implementation:** Map the risks to the ISO/IEC 27001 controls (Annex A) and create an implementation plan to address identified risks.

Output: A risk treatment plan that includes specific controls to mitigate identified risks, such as enhancing access control measures, implementing encryption for sensitive data and conducting regular security awareness training.

Step 3: MITRE ATT&CK Framework Integration

Task: Map the organisation's security operations to the MITRE ATT&CK framework to improve threat detection and response capabilities.

- **Technique Mapping:** Use real incident data (e.g., logs, alerts) to map observed attack techniques to the MITRE ATT&CK framework.
- **Detection Rules:** Develop and implement detection rules in your SIEM (e.g., QRadar) to monitor for specific MITRE ATT&CK techniques.
- **Gap Analysis:** Identify gaps in the current detection capabilities and recommend enhancements, such as adding new log sources or refining correlation rules.

Output: A threat detection improvement plan that includes the implementation of new detection rules for TTPs (Tactics, Techniques and Procedures) such as "Credential Dumping" (T1003) and "Persistence via Registry Run Keys" (T1060).

Step 4: Continuous Monitoring and Improvement

Task: Implement continuous monitoring and review processes to ensure ongoing compliance and improvement.

- **Monitoring:** Set up continuous monitoring dashboards in your SIEM to track compliance with the frameworks.
- **Reporting:** Generate monthly and quarterly compliance reports for management, highlighting key metrics, incidents and areas for improvement.

Output: An executive summary report for the board that outlines the current compliance status, recent security incidents and proposed actions for further strengthening the security posture.

10. Communication and Collaboration

- **Skill Development:** Improve your ability to communicate complex security issues to non-technical stakeholders.

Example:

Scenario: Communicating a Security Incident to Non-Technical Stakeholders

Background:

Your organisation has experienced a security incident involving unauthorised access to a sensitive internal system. The incident was detected through abnormal login activity and was contained before any significant damage was done. However, the incident must be communicated to non-technical stakeholders, including executive leadership and clients, who may not have a deep understanding of cybersecurity.

Objective:

To improve communication skills by crafting clear and concise incident reports and effectively conveying the details of the incident, its impact and the mitigation steps to non-technical stakeholders. Additionally, this exercise will involve participating in team meetings and collaborating with cross-functional teams to ensure a unified response.

Step 1: Writing a Clear and Concise Incident Report

Task: Draft an incident report that explains the security breach, its impact and the mitigation steps in a way that non-technical stakeholders can easily understand.

- **Incident Overview:** Summarise what happened, focusing on the key facts without using technical jargon.
- **Impact Analysis:** Explain the potential impact on the organisation, including any risks to data, systems, or client trust.
- **Mitigation and Next Steps:** Describe the steps taken to contain the incident, any ongoing investigations and the actions that will be taken to prevent future occurrences.

Output:

Incident Report: Unauthorised Access Incident

Date: 12 August 2024

Summary: On 11 August 2024, our security team identified unauthorised access to our internal accounting system. The incident was detected through unusual login patterns and was quickly contained. No sensitive data was accessed or exfiltrated and normal operations have been restored.

Impact: While no data loss occurred, this incident highlights the need for enhanced access controls. There is potential reputational risk and we are taking immediate steps to ensure our systems are further protected.

Mitigation and Next Steps: We have disabled the compromised accounts, initiated a full audit of our access control policies and are enhancing our multi-factor authentication (MFA) mechanisms. We are also conducting a thorough investigation to identify the root cause and will provide a detailed follow-up report with additional security measures.

Step 2: Communicating the Incident to Clients

Task: Prepare a client-facing communication, ensuring transparency while maintaining trust and confidence.

- **Client Notification:** Draft an email or letter that explains the situation to clients, assuring them that the incident has been managed and that their data remains secure.
- **Tone and Language:** Use a professional and reassuring tone, avoiding technical terms that may confuse or alarm clients.

Output:

Subject: Important Update: Security Incident and Our Commitment to Your Security

Dear Mason Mount,

We are writing to inform you about a recent security incident that occurred within our internal systems. On 11 August 2024, our security team detected unauthorised access to our internal accounting system. We acted swiftly to contain the issue and we want to assure you that no sensitive data was compromised.

We take your security very seriously and are conducting a thorough review to ensure that such incidents do not occur in the future. As part of our commitment to transparency, we will keep you informed of any further developments.

Please feel free to reach out to us if you have any questions or concerns. We appreciate your continued trust and partnership.

Sincerely,
Iffah Nadzirah
Cybersecurity Analyst
Izzmier Cybersecurity Services

Step 3: Participating in Team Meetings and Cross-Functional Collaboration

Task: Engage in a simulated team meeting where you will present the incident details and collaborate with different departments (e.g., IT, legal, public relations) to coordinate the response.

- **Internal Presentation:** Prepare a brief presentation summarising the incident, its impact and the steps taken. Focus on clear communication and the key points relevant to each department.
- **Collaboration:** Work with IT to ensure technical solutions are implemented, with legal to ensure compliance with regulations and with public relations to manage external communication.