TECHNICAL QUESTIONS SCENARIO FOR A CYBERSECURITY

Scenario 1 (Brute-Force):

You are a Security Operations Centre (SOC) analyst working with a SIEM solution (either QRadar or Splunk). You notice an alert for multiple failed login attempts from a single IP address within a short time frame, which could indicate a potential brute-force attack.

Questions and Expected Responses:

1. **Initial Response:**
   - **Question:** What is your immediate action upon receiving an alert for multiple failed login attempts?
   - **Expected Response:** My immediate action would be to acknowledge the alert and begin an initial investigation. I would verify the alert details, such as the source IP address, the affected user accounts, and the time frame of the failed attempts. This helps in understanding the scope and potential impact of the incident.
2. **Log Analysis:**
   - **Question:** How would you analyse the logs to gather more information about the suspicious activity?
   - **Expected Response:** Using the SIEM tool, I would search for all authentication logs related to the source IP address. I would filter the logs to display both failed and successful login attempts, if any, to determine the pattern of the attack. I would also correlate these events with other log sources to see if there are any related suspicious activities.
3. **Correlation and Context:**
   - **Question:** How would you use the SIEM's correlation capabilities to identify if this is part of a larger attack?
   - **Expected Response:** I would use the SIEM's correlation rules to identify any additional indicators of compromise (IoCs) related to the source IP or targeted accounts. This includes looking for other anomalies such as unusual login locations, simultaneous logins from different locations, or access attempts to critical systems. QRadar's offense correlation and Splunk's event correlation and visualization tools can be particularly useful for this purpose.
4. **Threat Intelligence:**
   - **Question:** How can threat intelligence be integrated into your analysis of this alert?
   - **Expected Response:** I would check the source IP address against threat intelligence feeds integrated with our SIEM to see if it has been associated with known malicious activity. This can provide additional context and help assess the risk level. In QRadar, I would look at the threat intelligence section within the offense, and in Splunk, I would use threat intelligence apps or lookups.
5. **Mitigation and Response:**
   - **Question:** What mitigation steps would you take to address this potential brute-force attack?
   - **Expected Response:** First, I would block the suspicious IP address at the firewall to prevent further attempts. Then, I would notify the IT team to review and reset the passwords of the affected accounts. I would also suggest implementing account lockout policies after a certain number of failed attempts to prevent brute-force attacks in the future.

6. **Post-Incident Actions:**
   - **Question:** After addressing the immediate threat, what steps would you take to prevent similar incidents in the future?
   - **Expected Response:** I would conduct a thorough review of the incident to understand how it occurred and why it wasn't prevented initially. Based on the findings, I would update our SIEM rules and correlation logic to better detect similar patterns. Additionally, I would recommend enhancing our security controls, such as multi-factor authentication (MFA), to make it more difficult for attackers to succeed.
7. **Documentation and Reporting:**
   - **Question:** How would you document and report this incident?
   - **Expected Response:** I would document all findings, actions taken, and the outcome of the incident in an incident report. This report would include timelines, affected systems and accounts, steps taken to mitigate the threat, and recommendations for future prevention. I would also ensure that this report is shared with relevant stakeholders and included in our incident response documentation for future reference.

Detailed Example Answer for Splunk:

1. **Immediate Action:**
   - Open the alert in Splunk and review the alert details.
   - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
   - Use SPL to search for authentication logs related to the source IP:

     ```
     SPL

     index=authentication_logs sourcetype=auth_logs
     src_ip="suspicious_ip"
     ```

   - Review both failed and successful login attempts.
3. **Correlation and Context:**
   - Use Splunk's correlation capabilities to look for related events:

     ```
     SPL

     index=* src_ip="suspicious_ip"
     | transaction user maxspan=30m
     | search eventcount>5
     ```

   - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
   - Check the source IP against threat intelligence feeds:

     ```
     SPL

     | inputlookup threat_intel_lookup
     | search ip="suspicious_ip"
     ```

5. **Mitigation and Response:**
   - Block the IP address and notify the IT team.

   - Implement account lockout policies and reset affected passwords.
6. **Post-Incident Actions:**
   - Review and update SIEM rules to detect similar patterns.
   - Recommend MFA and other security enhancements.
7. **Documentation and Reporting:**
   - Document all findings and actions in an incident report.
   - Share the report with stakeholders and update incident response documentation.

By demonstrating a thorough understanding of the steps involved in analysing multiple login failures, you can effectively showcase your ability to handle such incidents in a cybersecurity role.

Scenario 2 (Port Scanning):

You are a Security Operations Centre (SOC) analyst monitoring network traffic using a SIEM solution (either QRadar or Splunk). An alert is generated indicating a potential port scanning activity originating from an external IP address.

Questions and Expected Responses:

1. **Initial Response:**
    - **Question:** What steps would you take immediately upon receiving a port scanning alert?
    - **Expected Response:** I would first acknowledge the alert to ensure it is being tracked. Then, I would review the details of the alert, including the source IP address, the targeted network segments, and the specific ports being scanned. This helps in understanding the scope and potential intent of the scan.
2. **Log Analysis:**
    - **Question:** How would you analyse the logs to gather more information about the suspicious port scanning activity?
    - **Expected Response:** Using the SIEM tool, I would search for network traffic logs related to the source IP address. I would filter the logs to display all connection attempts, noting the frequency and sequence of port scans. Additionally, I would check for any corresponding firewall or IDS/IPS logs to see if any other defences detected and potentially blocked the scans.
3. **Correlation and Context:**
    - **Question:** How would you use the SIEM’s correlation capabilities to identify if this port scan is part of a larger attack?
    - **Expected Response:** I would use the SIEM's correlation engine to identify if there are any related alerts or suspicious activities from the same source IP or targeting the same network segment. This includes checking for follow-up activities like login attempts or exploit attempts on open ports. Correlating this information helps determine if the port scan is part of a reconnaissance phase of a larger attack.
4. **Threat Intelligence:**
    - **Question:** How can threat intelligence be integrated into your analysis of this port scanning alert?
    - **Expected Response:** I would check the source IP address against threat intelligence feeds integrated with our SIEM to see if it has been associated with known malicious actors or previous attacks. This can provide additional context and help assess the risk level of the port scan.
5. **Mitigation and Response:**
    - **Question:** What mitigation steps would you take to address this potential port scanning activity?
    - **Expected Response:** First, I would block the source IP address at the perimeter firewall to prevent further reconnaissance activities. Then, I would review the firewall and IDS/IPS configurations to ensure they are properly tuned to detect and block such activities in the future. Additionally, I would notify the network team and potentially affected asset owners about the incident.
6. **Post-Incident Actions:**

- **Question:** After addressing the immediate threat, what steps would you take to prevent similar incidents in the future?
- **Expected Response:** I would conduct a post-incident review to understand how the port scan was detected and why it was not blocked sooner. Based on the findings, I would update our SIEM rules and correlation logic to better detect similar patterns. I would also recommend implementing or refining network segmentation and access control measures to limit the exposure of critical assets.

7. **Documentation and Reporting:**
   - **Question:** How would you document and report this incident?
   - **Expected Response:** I would document all findings, actions taken, and the outcome of the incident in an incident report. This report would include timelines, affected systems, and accounts, steps taken to mitigate the threat, and recommendations for future prevention. I would also ensure that this report is shared with relevant stakeholders and included in our incident response documentation for future reference.

Detailed Example Answer for Splunk:

1. **Immediate Action:**
   - Open the alert in Splunk and review the alert details.
   - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
   - Use SPL to search for network traffic logs related to the source IP:

     ```
     SPL

     index=network_traffic sourcetype=firewall_logs
     src_ip="suspicious_ip"
     ```

   - Review the sequence and frequency of port scans.
3. **Correlation and Context:**
   - Use Splunk's correlation capabilities to look for related events:

     ```
     SPL

     index=* src_ip="suspicious_ip"
     | transaction dest_ip maxspan=30m
     | search eventcount>5
     ```

   - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
   - Check the source IP against threat intelligence feeds:

     ```
     SPL

     | inputlookup threat_intel_lookup
     | search ip="suspicious_ip"
     ```

5. **Mitigation and Response:**
   - Block the IP address at the firewall and notify the IT team.

   - Ensure firewall and IDS/IPS configurations are tuned to detect and block port scanning.
6. **Post-Incident Actions:**
   - Review and update SIEM rules to detect similar patterns.
   - Recommend network segmentation and access control measures.
7. **Documentation and Reporting:**
   - Document all findings and actions in an incident report.
   - Share the report with stakeholders and update incident response documentation.

Detailed Example Answer for QRadar:

1. **Immediate Action:**
   - Open the alert in QRadar and review the alert details.
   - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
   - Use QRadar to search for network traffic logs related to the source IP:

     ```
     bash

     source address = "suspicious_ip"
     ```

   - Review the sequence and frequency of port scans.
3. **Correlation and Context:**
   - Use QRadar's correlation capabilities to look for related events:

     ```
     java

     same source IP = "suspicious_ip"
     and destination address = "targeted_network"
     ```

   - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
   - Check the source IP against threat intelligence feeds in QRadar:

     ```
     bash

     Reference set lookup: "threat_intel_feed"
     where IP = "suspicious_ip"
     ```

5. **Mitigation and Response:**
   - Block the IP address at the firewall and notify the IT team.
   - Ensure firewall and IDS/IPS configurations are tuned to detect and block port scanning.
6. **Post-Incident Actions:**
   - Review and update SIEM rules to detect similar patterns.
   - Recommend network segmentation and access control measures.
7. **Documentation and Reporting:**
   - Document all findings and actions in an incident report.
   - Share the report with stakeholders and update incident response documentation.

By demonstrating a comprehensive understanding of the steps involved in analysing and responding to a port scanning alert, you can effectively showcase your ability to handle such incidents in a cybersecurity role.

Scenario 3 (Malware):

You are a Security Operations Centre (SOC) analyst monitoring endpoint security using a SIEM solution (either QRadar or Splunk). An alert is generated indicating a potential malware infection on one of the corporate workstations. The malware was detected by the endpoint protection system.

Questions and Expected Responses:

1. **Initial Response:**
   - **Question:** What steps would you take immediately upon receiving a malware detection alert?
   - **Expected Response:** My immediate action would be to acknowledge the alert to ensure it is being tracked. I would then review the alert details, such as the affected machine's IP address, the type of malware detected, the time of detection, and any associated user information. This helps in understanding the severity and potential impact of the malware infection.
2. **Log Analysis:**
   - **Question:** How would you analyse the logs to gather more information about the malware infection?
   - **Expected Response:** Using the SIEM tool, I would search for logs from the endpoint protection system related to the infected machine. I would look for details such as the malware signature, file paths, and actions taken by the endpoint protection system (e.g., quarantine, delete). Additionally, I would review other related logs, such as network traffic and user activity logs, to identify any unusual behaviour or signs of lateral movement.
3. **Correlation and Context:**
   - **Question:** How would you use the SIEM’s correlation capabilities to identify if this malware infection is part of a larger attack?
   - **Expected Response:** I would use the SIEM's correlation engine to look for other related alerts or suspicious activities from the same machine or user account. This includes checking for unusual network traffic patterns, access to critical systems, or similar alerts on other machines. Correlating this information helps determine if the malware infection is isolated or part of a coordinated attack.
4. **Threat Intelligence:**
   - **Question:** How can threat intelligence be integrated into your analysis of this malware alert?
   - **Expected Response:** I would check the malware signature and associated indicators of compromise (IoCs) against threat intelligence feeds integrated with our SIEM. This can provide additional context about the malware, such as its behaviour, known command-and-control (C2) servers, and if it has been associated with known threat actors. This information helps assess the risk level and potential impact of the malware infection.
5. **Mitigation and Response:**
   - **Question:** What mitigation steps would you take to address this malware infection?
   - **Expected Response:** First, I would isolate the infected machine from the network to prevent further spread. Then, I would coordinate with the IT team to perform a thorough scan and removal of the malware. If necessary, I would

reimage the machine. I would also review and reset any compromised user credentials and notify affected users. Finally, I would ensure all systems are up-to-date with the latest security patches and endpoint protection signatures.

6. **Post-Incident Actions:**
   - **Question:** After addressing the immediate threat, what steps would you take to prevent similar incidents in the future?
   - **Expected Response:** I would conduct a post-incident review to understand how the malware infection occurred and why it was not prevented initially. Based on the findings, I would update our endpoint protection policies, improve our SIEM detection rules, and implement additional security controls if necessary. I would also provide security awareness training to users to prevent similar incidents.
7. **Documentation and Reporting:**
   - **Question:** How would you document and report this incident?
   - **Expected Response:** I would document all findings, actions taken, and the outcome of the incident in an incident report. This report would include timelines, affected systems, and accounts, steps taken to mitigate the threat, and recommendations for future prevention. I would also ensure that this report is shared with relevant stakeholders and included in our incident response documentation for future reference.

Detailed Example Answer for Splunk:

1. **Immediate Action:**
   - Open the alert in Splunk and review the alert details.
   - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
   - Use SPL to search for endpoint protection logs related to the infected machine:

     ```
     SPL

     index=endpoint_protection sourcetype=antivirus_logs
     host="infected_machine"
     ```

   - Review details such as malware signature, file paths, and actions taken.
3. **Correlation and Context:**
   - Use Splunk's correlation capabilities to look for related events:

     ```
     SPL

     index=* host="infected_machine"
     | transaction user maxspan=30m
     | search eventcount>5
     ```

   - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
   - Check the malware signature against threat intelligence feeds:

     ```
     SPL

     | inputlookup threat_intel_lookup
     | search signature="malware_signature"
     ```

5. **Mitigation and Response:**
    - Isolate the infected machine from the network and notify the IT team.
    - Perform a thorough scan and removal of the malware.
    - Reimage the machine if necessary and reset any compromised credentials.
6. **Post-Incident Actions:**
    - Review and update endpoint protection policies and SIEM detection rules.
    - Implement additional security controls and provide security awareness training.
7. **Documentation and Reporting:**
    - Document all findings and actions in an incident report.
    - Share the report with stakeholders and update incident response documentation.

Detailed Example Answer for QRadar:

1. **Immediate Action:**
    - Open the alert in QRadar and review the alert details.
    - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
    - Use QRadar to search for endpoint protection logs related to the infected machine:

      sql

      ```
      SELECT * FROM events WHERE source address = 'infected_machine'
      ```

    - Review details such as malware signature, file paths, and actions taken.
3. **Correlation and Context:**
    - Use QRadar's correlation capabilities to look for related events:

      java

      ```
      same source IP = "infected_machine"
      and destination address = "critical_assets"
      ```

    - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
    - Check the malware signature against threat intelligence feeds in QRadar:

      bash

      ```
      Reference set lookup: "threat_intel_feed"
      where malware_signature = "malware_signature"
      ```

5. **Mitigation and Response:**
    - Isolate the infected machine from the network and notify the IT team.
    - Perform a thorough scan and removal of the malware.
    - Reimage the machine if necessary and reset any compromised credentials.
6. **Post-Incident Actions:**

  - Review and update endpoint protection policies and SIEM detection rules.
  - Implement additional security controls and provide security awareness training.

7. **Documentation and Reporting:**
   - Document all findings and actions in an incident report.
   - Share the report with stakeholders and update incident response documentation.

By demonstrating a comprehensive understanding of the steps involved in analysing and responding to a malware detection alert, you can effectively showcase your ability to handle such incidents in a cybersecurity role.

Scenario 4 (SQL Injection):

You are a Security Operations Centre (SOC) analyst working with a SIEM solution (either QRadar or Splunk). You receive an alert indicating a potential SQL injection attack targeting a web application hosted on your corporate server. The alert was triggered by a specific SIEM rule designed to detect SQL injection attempts.

Questions and Expected Responses:

1. **Initial Response:**
   - **Question:** What is your immediate action upon receiving an SQL injection alert?
   - **Expected Response:** My immediate action would be to acknowledge the alert to ensure it is tracked. I would then review the alert details, such as the source IP address, the target URL or web application, the payload of the suspicious request, and the time of the attack. This helps in understanding the scope and potential impact of the incident.
2. **Log Analysis:**
   - **Question:** How would you analyse the logs to gather more information about the suspicious activity?
   - **Expected Response:** Using the SIEM tool, I would search for web server logs related to the target application and source IP. I would look for HTTP request logs to identify the exact payloads used in the potential SQL injection attempts. Additionally, I would check for patterns that match common SQL injection signatures, such as unexpected database errors or unusual query structures.
3. **Correlation and Context:**
   - **Question:** How would you use the SIEM's correlation capabilities to identify if this SQL injection attempt is part of a larger attack?
   - **Expected Response:** I would use the SIEM's correlation rules to identify any related alerts or suspicious activities from the same source IP or targeting the same web application. This includes looking for other types of web attacks, scanning activities, or any signs of successful exploitation like unauthorized data access. Correlating these events helps determine if the SQL injection attempt is part of a broader attack campaign.
4. **Threat Intelligence:**
   - **Question:** How can threat intelligence be integrated into your analysis of this SQL injection alert?
   - **Expected Response:** I would check the source IP and any payload signatures against threat intelligence feeds integrated with our SIEM to see if they are associated with known malicious actors or previously observed attack patterns. This provides additional context and helps assess the risk level of the SQL injection attempt.
5. **Mitigation and Response:**
   - **Question:** What mitigation steps would you take to address this potential SQL injection attack?
   - **Expected Response:** First, I would block the source IP address at the web application firewall (WAF) to prevent further attempts. Then, I would review the web application's code and input validation mechanisms to identify and fix any vulnerabilities that allowed the SQL injection attempt. Additionally, I

would ensure that the database and web server configurations follow best security practices, such as using parameterized queries and proper error handling.

6. **Post-Incident Actions:**
   - **Question:** After addressing the immediate threat, what steps would you take to prevent similar incidents in the future?
   - **Expected Response:** I would conduct a thorough review of the incident to understand how the SQL injection attempt occurred and why it was not blocked initially. Based on the findings, I would update our SIEM rules and correlation logic to better detect similar patterns. Additionally, I would recommend conducting regular security code reviews, performing penetration testing on web applications, and providing secure coding training to developers.
7. **Documentation and Reporting:**
   - **Question:** How would you document and report this incident?
   - **Expected Response:** I would document all findings, actions taken, and the outcome of the incident in an incident report. This report would include timelines, affected systems and applications, steps taken to mitigate the threat, and recommendations for future prevention. I would also ensure that this report is shared with relevant stakeholders and included in our incident response documentation for future reference.

Detailed Example Answer for Splunk:

1. **Immediate Action:**
   - Open the alert in Splunk and review the alert details.
   - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
   - Use SPL to search for web server logs related to the target application and source IP:

     ```
     SPL

     index=web_logs sourcetype=access_combined
     src_ip="suspicious_ip" uri_path="/target_application"
     ```

   - Review HTTP request logs for SQL injection payloads and patterns.
3. **Correlation and Context:**
   - Use Splunk’s correlation capabilities to look for related events:

     ```
     SPL

     index=* src_ip="suspicious_ip" OR
     uri_path="/target_application"
     | transaction user maxspan=30m
     | search eventcount>5
     ```

   - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
   - Check the source IP and payload signatures against threat intelligence feeds:

     ```
     SPL
     ```

```
| inputlookup threat_intel_lookup
| search ip="suspicious_ip" OR
signature="sql_injection_signature"
```

5. **Mitigation and Response:**
   - Block the source IP address at the WAF and notify the web application team.
   - Review and fix web application vulnerabilities, ensuring parameterized queries are used.
6. **Post-Incident Actions:**
   - Review and update SIEM rules to detect similar patterns.
   - Conduct regular security code reviews and penetration testing.
7. **Documentation and Reporting:**
   - Document all findings and actions in an incident report.
   - Share the report with stakeholders and update incident response documentation.

Detailed Example Answer for QRadar:

1. **Immediate Action:**
   - Open the alert in QRadar and review the alert details.
   - Acknowledge the alert to ensure it's being tracked.
2. **Log Analysis:**
   - Use QRadar to search for web server logs related to the target application and source IP:

     sql

     ```
     SELECT * FROM events WHERE source address = 'suspicious_ip' AND
     uri_path = '/target_application'
     ```

   - Review HTTP request logs for SQL injection payloads and patterns.
3. **Correlation and Context:**
   - Use QRadar's correlation capabilities to look for related events:

     java

     ```
     same source IP = "suspicious_ip" OR uri_path =
     "/target_application"
     ```

   - Identify any patterns or related suspicious activities.
4. **Threat Intelligence:**
   - Check the source IP and payload signatures against threat intelligence feeds in QRadar:

     bash

     ```
     Reference set lookup: "threat_intel_feed"
     where IP = "suspicious_ip" OR signature =
     "sql_injection_signature"
     ```

5. **Mitigation and Response:**
   - Block the source IP address at the WAF and notify the web application team.

    - Review and fix web application vulnerabilities, ensuring parameterized queries are used.
6. **Post-Incident Actions:**
    - Review and update SIEM rules to detect similar patterns.
    - Conduct regular security code reviews and penetration testing.
7. **Documentation and Reporting:**
    - Document all findings and actions in an incident report.
    - Share the report with stakeholders and update incident response documentation.

By demonstrating a comprehensive understanding of the steps involved in analysing and responding to an SQL injection attack detection alert, you can effectively showcase your ability to handle such incidents in a cybersecurity role.