UNDERSTANDING SIEM RULES: HOW THEY WORK AND DETECT THREATS

BY IZZMIER IZZUDDIN

TABLE OF CONTENTS

HOW SIEM RULES WORK

IN GENERAL

1. **Data Collection:**
   - A SIEM collects and aggregates logs from various sources such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), endpoint devices, servers, applications, databases and more.
   - Example: Logs from a web server showing login attempts.
2. **Rule Application:**
   - SIEM rules analyse these logs for specific patterns or conditions. These rules look for behavior that matches known attack methods or anomalies.
   - Example: A rule might check if a user has attempted to log in five times within one minute with incorrect credentials.
3. **Trigger and Alert:**
   - If the conditions of the rule are met, the rule triggers an alert, which is sent to the SOC team.
   - Example: An alert is generated for a potential brute-force attack when multiple failed login attempts are detected.
4. **Response:**
   - The L1 analyst investigates the alert to determine if it is a true positive (a real incident) or a false positive (not an actual threat).

COMPONENTS OF A SIEM RULE

1. **Conditions:**
   - Define what to look for in the logs.
   - Example: Failed login attempts from the same IP address within a 5-minute window.
2. **Thresholds:**
   - Specify the limits that must be exceeded to trigger an alert.
   - Example: More than 10 failed login attempts within 5 minutes.
3. **Correlation Logic:**
   - Combine multiple log events from different sources to detect complex patterns.
   - Example: Correlating a malware download from a suspicious domain with abnormal outbound traffic.
4. **Actions:**
   - Define what happens when a rule is triggered.
   - Example: Sending an email notification to the SOC team or isolating the endpoint automatically.

MAPPING SIEM RULES TO CYBER ATTACKS

1. **Brute Force Attack Detection**

- **Rule Example:**
  - Detect multiple failed login attempts from a single IP address within a short time.
- **Mapped to Attack:**
  - A brute-force attack occurs when an attacker tries multiple username-password combinations to gain unauthorised access.
- **Logic:**
  - If failed logins > 5 within 1 minute from the same IP → Trigger alert.
- **Real-World Scenario:**
  - The SIEM detects 50 failed login attempts on a web application server from the same IP, generating an alert. The analyst investigates and blocks the IP.

2. **Privilege Escalation Detection**

- **Rule Example:**
  - Detect unusual privilege changes for a user account.
- **Mapped to Attack:**
  - Privilege escalation is when an attacker elevates their access level to perform unauthorised actions.
- **Logic:**
  - If a low-privilege user suddenly gains admin rights without a corresponding change request → Trigger alert.
- **Real-World Scenario:**
  - A junior employee account suddenly gains access to the HR database. An alert is triggered and the analyst confirms malicious activity.

3. **Command and Control (C2) Communication Detection**

- **Rule Example:**
  - Detect outbound connections to known malicious domains or IPs.
- **Mapped to Attack:**
  - Attackers use C2 servers to control infected devices in a network.
- **Logic:**
  - If outbound traffic matches a threat intelligence feed of known C2 IPs → Trigger alert.
- **Real-World Scenario:**
  - A compromised workstation connects to a blacklisted IP. The analyst uses tools like Wireshark to analyse the connection and blocks it.

4. **Data Exfiltration Detection**

   - **Rule Example:**
     - Monitor large data transfers to external IPs during non-business hours.
   - **Mapped to Attack:**
     - Data exfiltration occurs when sensitive information is stolen from an organisation.
   - **Logic:**
     - If data transfer > 1GB to external IPs between 10 PM and 6 AM → Trigger alert.
   - **Real-World Scenario:**
     - A compromised employee account uploads sensitive files to a file-sharing service. The analyst investigates and terminates the session.

5. **Malware Execution Detection**

   - **Rule Example:**
     - Detect the execution of unusual scripts or processes.
   - **Mapped to Attack:**
     - Malware often uses custom scripts or executables to compromise systems.
   - **Logic:**
     - If a rarely used script runs on a critical server → Trigger alert.
   - **Real-World Scenario:**
     - The SIEM detects PowerShell executing a script that downloads files from an unknown URL. The analyst isolates the server.

HOW RULES MAP TO THE ATTACK LIFECYCLE

1. **Reconnaissance:**
   - Rules to detect port scans or enumeration activities.
   - Example: Excessive failed attempts to connect to closed ports.
2. **Initial Access:**
   - Rules to detect phishing emails or malicious downloads.
   - Example: A file download followed by antivirus disabling.
3. **Execution:**
   - Rules to detect suspicious script execution.
   - Example: Command-line tools running scripts to disable defenses.
4. **Persistence:**
   - Rules to detect unauthorised creation of scheduled tasks or services.

    - Example: New tasks that run scripts during off-hours.
5. **Lateral Movement:**
    - Rules to detect simultaneous logins across multiple systems by the same account.
    - Example: An admin account logs into 10 different servers in 1 minute.
6. **Exfiltration:**
    - Rules to monitor data leaving the organisation.
    - Example: Unusual large file uploads to external servers.

BENEFITS OF MAPPING RULES TO ATTACKS

- **Improved Threat Detection:** SIEM rules pinpoint specific attack tactics, techniques and procedures (TTPs).
- **Proactive Defense:** Early detection prevents further escalation.
- **Reduced False Positives:** Proper mapping ensures meaningful alerts.
- **Compliance:** Many compliance frameworks require monitoring for certain attack types.

FOR NEW CYBERSECURITY ANALYSTS (L1)

- **Understand the Context:** Learn how rules are designed and what specific threats they detect.
- **Learn the MITRE ATT&CK Framework:** Familiarise yourself with TTPs and how rules correspond to them.
- **Investigate Alerts Properly:** Use the context provided by alerts (source IP, event type, timestamps) to determine if it’s a true positive.
- **Practice Using SIEM Tools:** Use platforms like Splunk, QRadar or ELK Stack to practice creating and testing rules.

SIEM RULE DETECTION SCENARIO WITH SIMULATED LOG DATA

SCENARIO 1: BRUTE FORCE ATTACK ON A WEB SERVER

An attacker is attempting to perform a brute force attack on a web application server to gain unauthorised access to an account.

SIEM Rule for Detection

- **Rule Name:** Brute Force Detection
- **Conditions:**
  - Detect 10 or more failed login attempts from the same IP within 5 minutes.
- **Threshold:**
  - Failed login attempts >= 10.
- **Action:** Generate an alert.

Log

Timestamp	Source IP	Event Type	Username	Status	Details
2024-11-25 10:00:01	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:05	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:10	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:15	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:20	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:25	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:30	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:35	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:40	192.168.1.15	Login Attempt	admin	Failed	Incorrect password
2024-11-25 10:00:45	192.168.1.15	Login Attempt	admin	Failed	Incorrect password

How the Rule Detects the Attack

1. **Log Analysis:**
   - The SIEM system continuously monitors and ingests login attempt logs.
   - The rule checks for multiple failed logins from the same IP address within a short time frame.
2. **Pattern Match:**
   - The system observes that 192.168.1.15 has attempted to log in 10 times unsuccessfully within 45 seconds.
3. **Threshold Met:**
   - Since the threshold of 10 failed login attempts is met, the rule triggers an alert.

SIEM Alert Details

- **Alert Name:** Brute Force Attack Detected
- **Severity Level:** High
- **Triggered By:** Rule: Brute Force Detection
- **Time:** 2024-11-25 10:00:45
- **Source IP:** 192.168.1.15
- **Details:** 10 failed login attempts detected within 1 minute.

Steps for L1 Analyst

1. **Review the Alert:**
   - Open the alert in the SIEM system.
   - Verify the log data and ensure the alert is not a false positive.
2. **Investigate the Source IP:**
   - Check if 192.168.1.15 belongs to an internal system or an external IP.
   - Use tools like WHOIS or Shodan to gather more information about the IP.
3. **Check for Related Activity:**
   - Look for successful logins or other suspicious activities from the same IP in the logs.
   - Correlate with other rules, such as file access or data exfiltration.
4. **Take Action:**
   - If confirmed as a brute force attack:
     - Block the IP using a firewall.
     - Notify the incident response team for further investigation.
     - Update the affected user to reset their credentials if necessary.
5. **Document Findings:**
   - Create an incident report summarising:

- The triggered rule.
- Details of the investigation.
- Actions taken to mitigate the threat.

SCENARIO 2: DATA EXFILTRATION DETECTED

An attacker has gained unauthorised access to an endpoint and is attempting to exfiltrate sensitive data to an external IP address over an unusual protocol (FTP on a non-standard port).

SIEM Rule for Detection

- **Rule Name:** Unusual Data Transfer Detection
- **Conditions:**
    - Outbound network traffic with:
        - **Unusual file size**: >100 MB.
        - **Destination IP**: Outside of the organisation's network range.
        - **Protocol**: FTP over a non-standard port (4455).
- **Threshold:** 1 event matching all criteria.
- **Action:** Generate an alert.

Logs

Firewall

Timestamp	Source IP	Destination IP	Protocol	Port	Bytes Transferred	Action
2024-11-25 12:15:01	10.0.0.25	198.51.100.45	FTP	4455	120 MB	Allowed
2024-11-25 12:16:05	10.0.0.25	198.51.100.45	FTP	4455	130 MB	Allowed

Endpoint

Timestamp	Host IP	Event Type	File Accessed	Action
2024-11-25 12:14:50	10.0.0.25	Sensitive File Access	HR_Salaries.csv	Read
2024-11-25 12:14:55	10.0.0.25	Compression Detected	HR_Salaries.zip	Compressed
2024-11-25 12:15:00	10.0.0.25	File Transfer	HR_Salaries.zip	Initiated Transfer

How the Rule Detects the Attack

1. **Log Analysis:**
    - The SIEM monitors traffic logs, endpoint activity logs and access logs.
    - The rule is configured to correlate multiple conditions:
        - A large file transfer (>100 MB).
        - A sensitive file being accessed and compressed.
        - Data sent over FTP using a non-standard port.
2. **Pattern Match:**
    - The SIEM detects that 10.0.0.25 accessed and compressed a sensitive file (HR_Salaries.csv), then transferred it via FTP to an external IP (198.51.100.45) on port 4455.
3. **Threshold Met:**
    - The single event of transferring 120 MB matches the configured rule, triggering the alert.

SIEM Alert Details

- **Alert Name:** Unusual Data Transfer Detected
- **Severity Level:** Critical
- **Triggered By:** Rule: Unusual Data Transfer Detection
- **Time:** 2024-11-25 12:15:01
- **Source IP:** 10.0.0.25
- **Destination IP:** 198.51.100.45
- **Details:** Data exfiltration attempt detected. Sensitive file transferred over FTP to external IP using non-standard port 4455.

Steps for L1 Analyst

1. **Review the Alert:**
    - Verify the alert details and log data in the SIEM system.
    - Confirm if the event matches the rule conditions (sensitive file transfer, external IP, non-standard port).
2. **Investigate the Destination IP:**
    - Use WHOIS, Shodan or threat intelligence feeds to check the reputation of 198.51.100.45.
    - Determine if this IP is known for malicious activity.
3. **Investigate the Endpoint:**
    - Check for unusual activities on 10.0.0.25:
        - File access logs.
        - Signs of malware or unauthorised access.
        - User actions (Was the user authorised?).

4. **Correlate Logs:**
    - Search for other events related to this endpoint or user (login attempts, abnormal processes).
5. **Take Action:**
    - Isolate the Endpoint: Disconnect 10.0.0.25 from the network to prevent further data transfer.
    - Block the IP: Block 198.51.100.45 in the firewall.
    - Notify the incident response team to perform a deeper investigation.
6. **Document Findings:**
    - Prepare an incident report including:
        - Alert details.
        - Actions taken (IP blocked, endpoint isolated).
        - Recommendations for preventing recurrence (disabling FTP on non-standard ports).

SCENARIO 3: MALWARE DETECTED ON AN ENDPOINT

A user unknowingly downloads a malicious executable from a phishing email. The malware tries to execute, communicate with a Command and Control (C2) server and spread laterally within the network.

SIEM Rule for Detection

- **Rule Name:** Malware Execution and C2 Communication Detection
- **Conditions:**
  - Detect a process execution with a known malicious hash.
  - Detect outbound network traffic to a suspicious or newly registered domain.
  - Correlate unusual traffic or processes on multiple endpoints.

Logs

Endpoint

Timestamp	Host IP	Event Type	Process Name	Hash	Action
2024-11-25 08:45:01	10.0.0.10	File Download	invoice.exe	N/A	Completed
2024-11-25 08:45:05	10.0.0.10	Process Execution	invoice.exe	12AB34CD56EF78GH90IJ	Started
2024-11-25 08:45:08	10.0.0.10	Malware Detected	invoice.exe	12AB34CD56EF78GH90IJ	Quarantined

Firewall

Timestamp	Source IP	Destination IP/Domain	Protocol	Port	Action
2024-11-25 08:46:00	10.0.0.10	badactor[.]xyz	HTTPS	443	Allowed
2024-11-25 08:46:05	10.0.0.10	badactor[.]xyz	HTTPS	443	Allowed

Network Monitoring

Timestamp	Source IP	Event Type	Details
2024-11-25 08:46:10	10.0.0.10	Suspicious Network Traffic	C2 Communication

How the Rule Detects the Attack

1. **Log Analysis:**
   - The SIEM collects logs from the endpoint and network monitoring tools.
   - The rule is triggered by detecting:
     - A process with a hash matching a malicious file signature database.
     - Network communication to a suspicious domain (newly registered, flagged in threat intelligence feeds).
2. **Pattern Match:**
   - The process execution of invoice.exe has a hash (12AB34CD56EF78GH90IJ) flagged as malicious.
   - Network logs show communication with badactor[.]xyz, which is a known malicious domain.
   - The correlation of logs raises a high-confidence alert.
3. **Threshold Met:**
   - The combined activities (malware execution and C2 communication) exceed the detection threshold, triggering the SIEM rule.

SIEM Alert Details

- **Alert Name:** Malware and C2 Communication Detected
- **Severity Level:** Critical
- **Triggered By:** Rule: Malware Execution and C2 Communication Detection
- **Time:** 2024-11-25 08:46:10
- **Source IP:** 10.0.0.10
- **Details:** Malicious executable detected with outbound traffic to a C2 domain.

Steps for L1 Analyst

1. **Review the Alert:**
   - Open the alert in the SIEM system to examine related logs.
   - Confirm that the hash matches a known malware signature.
2. **Investigate the Domain:**
   - Use OSINT tools (WHOIS, VirusTotal) to check the reputation of badactor[.]xyz.
   - Analyse the domain's age and registration details for signs of malicious intent.
3. **Investigate the Endpoint:**
   - Check logs for additional suspicious activity on 10.0.0.10:
     - Files downloaded or executed recently.

        - Lateral movement attempts (connections to other internal IPs).

4. **Take Action:**
    - Isolate the Endpoint: Disconnect 10.0.0.10 from the network.
    - Block the Domain: Add badactor[.]xyz to the firewall blacklist.
    - Scan for Persistence: Run antivirus or forensic tools (Sysinternals) on the infected endpoint.
5. **Correlate Logs:**
    - Look for similar behavior on other endpoints.
    - Search for traffic patterns that match C2 communication across the network.
6. **Document Findings:**
    - Include details of:
        - The malicious process and its hash.
        - The external domain involved in C2 communication.
        - Actions taken to contain and mitigate the threat.

SCENARIO 4: BRUTE-FORCE ATTACK ON A WEB SERVER

An attacker is attempting to gain unauthorised access to a corporate web application by performing a brute-force attack on the login page. The attacker uses a script to try multiple username-password combinations within a short period.

SIEM Rule for Detection

- **Rule Name:** Brute-Force Login Attempt Detection
- **Conditions:**
  - More than 10 failed login attempts within a 5-minute window from the same IP address.
  - **Thresholds:**
    - 10 unique username attempts.
    - A single successful login after multiple failed attempts.

Logs

Web Server Access

Timestamp	Client IP	Username	Event Type	Status
2024-11-25 14:01:01	192.0.2.10	admin	Login Attempt	Failed
2024-11-25 14:01:03	192.0.2.10	user1	Login Attempt	Failed
2024-11-25 14:01:05	192.0.2.10	user2	Login Attempt	Failed
2024-11-25 14:01:08	192.0.2.10	test_user	Login Attempt	Failed
2024-11-25 14:01:10	192.0.2.10	admin	Login Attempt	Failed
2024-11-25 14:01:15	192.0.2.10	admin	Login Attempt	Success

Firewall

Timestamp	Source IP	Destination IP	Port	Action
2024-11-25 14:00:58	192.0.2.10	10.0.0.25	443	Allowed

SIEM Correlation Results

- **Number of Failed Logins from 192.0.2.10:** 11.
- **Successful Login After Failed Attempts:** True.
- **Severity Level:** High.

How the Rule Detects the Attack

1. **Log Analysis:**
   - SIEM collects access logs from the web server and firewall logs.
   - It identifies multiple failed login attempts originating from a single source IP (192.0.2.10) within a short time frame.
2. **Pattern Match:**
   - The attacker makes 11 login attempts within 15 seconds.
   - The SIEM correlates the failed attempts with a subsequent successful login by the same source IP.
3. **Threshold Met:**
   - The brute-force rule threshold is exceeded (10+ failed attempts and 1 success within a short window), triggering an alert.

SIEM Alert Details

- **Alert Name:** Brute-Force Login Detected
- **Severity Level:** Critical
- **Triggered By:** Rule: Brute-Force Login Attempt Detection
- **Time:** 2024-11-25 14:01:15
- **Source IP:** 192.0.2.10
- **Destination IP:** 10.0.0.25
- **Details:** Brute-force attack detected on a web server login page, with eventual success.

Steps for L1 Analyst

1. **Review the Alert:**
   - Open the alert in the SIEM.
   - Verify the logs associated with the alert to confirm the brute-force activity (multiple failed logins from the same IP followed by a success).
2. **Investigate the Source IP:**
   - Use OSINT tools like VirusTotal, GreyNoise and Shodan to analyse the reputation of 192.0.2.10.
   - Check if the IP is associated with known malicious activities or botnets.
3. **Investigate the Web Server:**
   - Check for suspicious activity in the compromised account after the successful login.
   - Look for actions like:
     - Changes to user permissions.

        - Attempts to upload files or modify critical configurations.

4. **Take Action:**
    - Block the Source IP: Use the firewall to block traffic from 192.0.2.10.
    - Lock the Compromised Account: Temporarily disable the affected user account until further investigation.
    - Force Password Reset: Notify the account owner and enforce a password change.
5. **Correlate Logs for Other Accounts:**
    - Search for similar brute-force patterns targeting other usernames or endpoints.
6. **Document Findings:**
    - Include:
        - Details of failed attempts and the compromised account.
        - Actions taken to contain the attack.
        - Recommendations for strengthening defenses (enforcing MFA).

SCENARIO 5: DATA EXFILTRATION DETECTED VIA UNUSUAL NETWORK ACTIVITY

An insider with legitimate access to sensitive data attempts to exfiltrate large volumes of information to an unauthorised external server by using an uncommon protocol or port.

SIEM Rule for Detection

- **Rule Name:** Unusual Data Transfer Volume to External Destination
- **Conditions:**
  - Data transfer size exceeds 1 GB within 15 minutes.
  - Destination is an unapproved external IP or domain.
  - Data is sent using uncommon protocols or ports (FTP on port 21 or custom high-numbered ports).

Logs

Firewall

Timestamp	Source IP	Destination IP	Protocol	Port	Data Transferred (MB)	Action
2024-11-25 10:00:01	10.0.0.15	203.0.113.50	FTP	21	250	Allowed
2024-11-25 10:02:05	10.0.0.15	203.0.113.50	FTP	21	300	Allowed
2024-11-25 10:04:15	10.0.0.15	203.0.113.50	FTP	21	500	Allowed

Endpoint

Timestamp	Host IP	Event Type	File Name	Action
2024-11-25 09:59:50	10.0.0.15	File Access	confidential_docs.zip	Read
2024-11-25 10:00:00	10.0.0.15	File Upload	confidential_docs.zip	Started

SIEM Correlation Results

- **Total Data Transferred:** 1.05 GB within 5 minutes.
- **Protocol Used:** FTP (commonly used for data transfer but restricted in this organisation).
- **Destination:** 203.0.113.50 (not listed in approved external IPs).

- **Severity Level:** Critical.

How the Rule Detects the Attack

1. **Log Analysis:**
    - SIEM collects firewall and endpoint logs, noting:
        - Large volume of data sent over an uncommon protocol (FTP).
        - Destination IP not matching the organisation's approved external servers.
2. **Pattern Match:**
    - Correlates the large data upload (exceeding 1 GB) with the endpoint log showing sensitive file access.
3. **Threshold Met:**
    - The volume of data and the unapproved external IP trigger the SIEM rule.

SIEM Alert Details

- **Alert Name:** Data Exfiltration via Unusual Protocol Detected
- **Severity Level:** Critical
- **Triggered By:** Rule: Unusual Data Transfer Volume to External Destination
- **Time:** 2024-11-25 10:04:15
- **Source IP:** 10.0.0.15
- **Destination IP:** 203.0.113.50
- **Details:** Large data transfer to unapproved external IP using FTP protocol.

Steps for L1 Analyst

1. **Review the Alert:**
    - Open the alert in the SIEM system.
    - Analyse logs for the source endpoint (10.0.0.15) and the external IP (203.0.113.50).
2. **Investigate the Source Endpoint:**
    - Check the file that was accessed and uploaded (confidential_docs.zip).
    - Validate whether the user had legitimate reasons to access the file.
3. **Investigate the Destination:**
    - Use OSINT tools (Shodan, VirusTotal) to verify the reputation of 203.0.113.50.
    - Determine if this IP is associated with known malicious activity or belongs to an external party.
4. **Check Protocol and Policy:**

   - Confirm that FTP is not commonly used or allowed for external data transfers in your organisation.
   - Cross-reference organisational policies regarding file transfers.
5. **Take Immediate Action:**
   - Block Further Transfers: Add 203.0.113.50 to the firewall’s blocklist.
   - Quarantine the Endpoint: Disconnect 10.0.0.15 from the network to prevent further exfiltration.
   - Engage User: Reach out to the user for clarification and escalate if suspicious.
6. **Correlate Logs for Wider Threat Analysis:**
   - Check if other endpoints or users have communicated with 203.0.113.50.
   - Identify if the same FTP protocol or similar behavior has been used recently by other users.
7. **Document Findings:**
   - Include:
     - Data size, file name and destination details.
     - Results from OSINT and internal investigation.
     - Actions taken to mitigate the risk and recommendations for preventing recurrence.

SCENARIO 6: SUSPICIOUS FILE DOWNLOAD DETECTED FROM UNAPPROVED SOURCE

An employee inadvertently downloads a malicious file from an unapproved external website while browsing the internet. The file contains malware that can exfiltrate data or provide a foothold for attackers in the corporate network.

SIEM Rule for Detection

- **Rule Name:** Malicious or Suspicious File Download
- **Conditions:**
  - File downloaded from a domain not included in the organisation's approved URL whitelist.
  - File has a hash that matches known malicious files in a threat intelligence database or sandbox analysis.
  - Event detected by the endpoint protection system or DNS logs.

Logs

Proxy/Web Gateway

Timestamp	Source IP	Destination URL	File Name	File Hash	Action
2024-11-25 11:20:10	10.0.0.50	hxxp://malicious-site[.]com/evil	malicious.exe	e99a18c428cb38d5f260853678922e03	Allowed

Endpoint

Timestamp	Host IP	Event Type	File Name	Status
2024-11-25 11:20:12	10.0.0.50	File Execution Attempt	malicious.exe	Blocked

Threat Intelligence Database Query

- **File Hash:** e99a18c428cb38d5f260853678922e03
- **Threat Level:** Critical
- **Associated Malware:** Remote Access Trojan (RAT)

How the Rule Detects the Attack

1. **Log Analysis:**
   - SIEM collects logs from the proxy server, endpoint protection solution and threat intelligence feeds.
   - A file download event from an unapproved domain (hxxp://malicious-site[.]com) is flagged.
2. **Threat Intelligence Match:**
   - The file hash (e99a18c428cb38d5f260853678922e03) is compared against a database of known malicious hashes.
   - A match confirms the file as a known Remote Access Trojan (RAT).
3. **Action Taken:**
   - Endpoint protection blocks the file execution attempt.
   - SIEM generates a critical alert for further investigation.

SIEM Alert Details

- **Alert Name:** Malicious File Download Attempt Detected
- **Severity Level:** High
- **Triggered By:** Rule: Malicious or Suspicious File Download
- **Time:** 2024-11-25 11:20:12
- **Source IP:** 10.0.0.50
- **Destination URL:** hxxp://malicious-site[.]com/evil
- **File Hash:** e99a18c428cb38d5f260853678922e03

Steps for L1 Analyst

1. **Review the Alert:**
   - Open the alert in the SIEM system.
   - Validate the download event by reviewing proxy and endpoint logs.
2. **Investigate the File:**
   - Use tools like VirusTotal to verify the malicious hash.
   - Check sandbox results for e99a18c428cb38d5f260853678922e03 (Cuckoo Sandbox or Hybrid Analysis).
3. **Investigate the Source URL:**
   - Use OSINT tools such as URLScan, AlienVault OTX or Shodan to gather information about hxxp://malicious-site[.]com.
   - Determine if the domain is known for distributing malware.
4. **Investigate the Host:**

   - Run an endpoint scan on 10.0.0.50 to ensure no residual malicious activity exists.
   - Check for other suspicious activities or downloads on the host.
5. **Take Immediate Action:**
   - Block the Domain: Add hxxp://malicious-site[.]com to the proxy blocklist.
   - Quarantine the Host: Isolate 10.0.0.50 from the network if the investigation reveals further compromise.
   - Alert the User: Notify the employee about the suspicious activity and provide training on safe browsing practices.
6. **Correlate Logs for Similar Behavior:**
   - Search SIEM for other hosts that accessed the same domain or downloaded files with the same hash.
7. **Document Findings:**
   - Include:
     - The malicious file hash and associated malware.
     - URL details and threat intelligence findings.
     - Actions taken to block the threat and recommendations to strengthen security.

SCENARIO 7: BRUTE-FORCE ATTACK DETECTED ON A WEB SERVER

An attacker attempts to gain unauthorised access to a web application by repeatedly trying different username-password combinations on the login page.

SIEM Rule for Detection

- **Rule Name:** Excessive Login Failures
- **Conditions:**
    - More than 10 failed login attempts from the same IP address within 5 minutes.
    - Login attempts targeting sensitive applications, such as a web server or admin portal.

Log

Web Server Access

Timestamp	Source IP	Username	Event	User-Agent	Status Code
2024-11-25 14:00:01	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:00:10	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:00:20	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:00:30	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:00:40	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:00:50	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:01:00	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:01:10	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:01:20	192.168.1.15	admin	Login Failed	Mozilla/5.0	401
2024-11-25 14:01:30	192.168.1.15	admin	Login Successful	Mozilla/5.0	200

SIEM Correlation Results

- **Source IP:** 192.168.1.15
- **Total Failed Login Attempts:** 10 within 90 seconds.
- **Target:** Web server login portal.
- **Event Severity:** Critical (successful login after multiple failures).

How the Rule Detects the Attack

1. **Log Analysis:**
   - SIEM analyses web server logs and detects multiple failed login attempts from the same IP (192.168.1.15) targeting the admin account.
2. **Threshold Met:**
   - More than 10 failed attempts within the configured 5-minute window trigger the alert.
3. **Critical Escalation:**
   - A successful login from the same IP following repeated failures increases the alert severity.

SIEM Alert Details

- **Alert Name:** Brute-Force Login Attack Detected
- **Severity Level:** High
- **Triggered By:** Rule: Excessive Login Failures
- **Time:** 2024-11-25 14:01:30
- **Source IP:** 192.168.1.15
- **Target Account:** admin
- **Details:** Multiple failed login attempts followed by a successful login.

Steps for L1 Analyst

1. **Review the Alert:**
   - Analyse the alert in the SIEM system and review associated logs.
   - Validate the number of failed login attempts and confirm the IP address involved.
2. **Investigate the Source IP:**
   - Use OSINT tools like Shodan or IPVoid to gather information about the source IP (192.168.1.15).

   - Check if the IP is linked to previous malicious activities or known attackers.
3. **Investigate the Target Account:**
   - Verify the admin account activity after the successful login.
   - Check for unusual actions such as privilege escalations, changes to system configurations or data access.
4. **Validate the User:**
   - Reach out to the account owner (if internal) to confirm if they were the ones accessing the account.
   - If unverified, treat the account as compromised.
5. **Take Immediate Action:**
   - **Block the IP:** Temporarily block 192.168.1.15 at the firewall level.
   - **Reset Credentials:** Reset the password for the compromised admin account.
   - **Enable Multi-Factor Authentication (MFA):** If not already implemented, recommend enabling MFA for the account.
6. **Correlate Logs for Broader Analysis:**
   - Search SIEM for similar brute-force attempts targeting other accounts or systems.
   - Check if the attacker attempted other entry points into the environment.
7. **Document Findings:**
   - Include:
     - Source IP, account details and timeline of events.
     - Results from OSINT investigations.
     - Mitigation steps taken to prevent further exploitation.

SCENARIO 8: DATA EXFILTRATION VIA SUSPICIOUS FILE TRANSFER

An attacker who has gained unauthorised access to a corporate system attempts to exfiltrate sensitive data by uploading files to an external FTP server.

SIEM Rule for Detection

- **Rule Name:** Large File Transfer to External IP
- **Conditions:**
    - File transfer over 50MB to an external IP address.
    - Use of uncommon ports or protocols (FTP, SCP).
    - Destination IP not in the list of approved external IPs.

Logs

Network Firewall

Timestamp	Source IP	Destination IP	Port	Protocol	Bytes Transferred	Action
2024-11-25 10:05:30	10.0.0.12	203.0.113.45	21	FTP	5MB	Allowed
2024-11-25 10:06:15	10.0.0.12	203.0.113.45	21	FTP	15MB	Allowed
2024-11-25 10:07:45	10.0.0.12	203.0.113.45	21	FTP	35MB	Allowed
2024-11-25 10:09:00	10.0.0.12	203.0.113.45	21	FTP	60MB	Allowed

Host

Timestamp	Source Host	Process	Action
2024-11-25 10:05:00	HR-Desktop	FTP.exe	Started
2024-11-25 10:09:05	HR-Desktop	SensitiveFile.docx	Uploaded via FTP

SIEM Correlation Results

- **Source IP:** 10.0.0.12
- **Destination IP:** 203.0.113.45
- **Total Data Transferred:** 115MB.
- **Port/Protocol:** FTP (Port 21).
- **Event Severity:** Critical.

How the Rule Detects the Attack

1. **Network Monitoring:**
   - The SIEM detects large outbound file transfers using FTP.
   - The destination IP (203.0.113.45) is not part of the allowed external IP list.
2. **Threshold Met:**
   - File size exceeds the defined threshold of 50MB.
3. **Uncommon Activity:**
   - FTP is rarely used within the organisation, raising suspicion about the protocol usage.

SIEM Alert Details

- **Alert Name:** Suspicious Large File Transfer
- **Severity Level:** Critical
- **Triggered By:** Rule: Large File Transfer to External IP
- **Time:** 2024-11-25 10:09:00
- **Source Host:** HR-Desktop (10.0.0.12)
- **Destination:** 203.0.113.45
- **Details:** Multiple file uploads via FTP, exceeding 100MB total data transfer.

Steps for L1 Analyst

1. **Review the Alert:**
   - Examine the SIEM alert and logs to confirm the file transfer details (size, destination IP and protocol).
2. **Investigate the Source Host:**
   - Use endpoint detection tools to check for:
     - Suspicious processes (FTP.exe) running on HR-Desktop.
     - Recently accessed or modified sensitive files on the host.
3. **Investigate the Destination IP:**
   - Perform an OSINT investigation using tools like VirusTotal or GreyNoise on 203.0.113.45:
     - Determine if the IP is associated with malicious activity or is part of known attacker infrastructure.
4. **Correlate User Activity:**
   - Identify the user logged into HR-Desktop at the time of the event.
   - Check for unusual behaviors, such as excessive access to sensitive files.

5. **Take Immediate Action:**
    - **Block the IP:** Block 203.0.113.45 at the network firewall.
    - **Kill Suspicious Process:** Terminate FTP.exe on HR-Desktop.
    - **Isolate the Host:** Quarantine HR-Desktop to prevent further data exfiltration.
6. **Escalate for Forensic Analysis:**
    - Escalate to the L2/L3 team to conduct a forensic analysis of HR-Desktop:
        - Examine memory dumps for malicious artifacts.
        - Analyse network traffic for additional indicators of compromise (IOCs).
7. **Mitigation and Recommendations:**
    - **Restrict FTP Usage:** Disable FTP protocol in the network unless explicitly needed.
    - **Implement DLP Solutions:** Deploy data loss prevention tools to monitor and prevent unauthorised data transfers.
8. **Document and Report:**
    - Provide a comprehensive report detailing:
        - Event timeline, source and destination details.
        - Steps taken to mitigate the threat.
        - Additional recommendations to prevent similar incidents.

SCENARIO 9: PRIVILEGE ESCALATION FOLLOWED BY UNAUTHORISED ACCESS

An attacker exploits a vulnerability on an employee's workstation to escalate privileges and gain administrative access. They then access a file server containing sensitive documents outside of the employee's typical working hours.

SIEM Rule for Detection

- **Rule Name:** Unusual Administrative Privilege Escalation and Access to Restricted Files
- **Conditions:**
  - User account transitions to administrative privileges unexpectedly.
  - Access to critical file servers occurs outside typical working hours.
  - Correlation with known privilege escalation events (suspicious processes or tools like PowerShell).

Logs

Windows Security (Privilege Escalation)

Timestamp	Source Host	User	Event ID	Description
2024-11-25 02:13:15	HR-Laptop	employee1	4673	User attempted special privilege assignment
2024-11-25 02:13:20	HR-Laptop	employee1	4672	Administrative privileges assigned to user
2024-11-25 02:14:00	HR-Laptop	SYSTEM	4688	Process started: PowerShell.exe with encoded commands

File Server (Unauthorised File Access)

Timestamp	File Server	User	Action	File Name
2024-11-25 02:15:30	FileServer01	employee1	Accessed	SensitiveDocs/Financials.xlsx
2024-11-25 02:16:45	FileServer01	employee1	Copied to Local Drive	SensitiveDocs/ClientsList.docx

SIEM Correlation Results

- **Source Host:** HR-Laptop
- **Affected System:** FileServer01

- **Event Details:** Privilege escalation followed by unauthorised access to sensitive files outside standard working hours.

How the Rule Detects the Attack

1. **Privilege Escalation Detection:**
    - The user account (employee1) escalates privileges to administrative rights, flagged by Event ID 4672.
    - A suspicious PowerShell process executes soon after, suggesting potential exploitation.
2. **File Access Outside Business Hours:**
    - **Access Time:** 2:15 AM (outside standard working hours).
    - Access to sensitive files like Financials.xlsx is unusual for the user's role.
3. **Correlation of Events:**
    - Privilege escalation from HR-Laptop correlates with unauthorised access to FileServer01.

SIEM Alert Details

- **Alert Name:** Unauthorised Privilege Escalation and File Access
- **Severity Level:** Critical
- **Triggered By:** Rule: Unusual Admin Privilege and File Access
- **Time:** 2024-11-25 02:15:30
- **Source Host:** HR-Laptop (10.0.0.45)
- **Affected Host:** FileServer01 (10.0.1.20)
- **Details:** Privilege escalation detected on HR-Laptop, followed by unauthorised access to sensitive files on FileServer01.

Steps for L1 Analyst

Step 1: Investigate Privilege Escalation

- **Check the Logs:**
    - Verify Event ID 4672 for administrative rights assignment.
    - Examine Event ID 4688 to confirm suspicious PowerShell execution.
- **Inspect Process Details:**
    - Look into the PowerShell.exe command used:
        - Encoded commands might indicate malicious scripts for exploitation.

    - Use tools like Sysmon to trace any dropped files or connections initiated.

Step 2: Investigate File Server Activity

- **Review File Server Logs:**
    - Confirm unauthorised file access and copying actions by employee1.
    - Validate the accessed files against sensitive or restricted lists.
- **Check User Behavior:**
    - Investigate if the user had legitimate reasons to access the files at the time.
    - Determine if the user account was compromised.

Step 3: Perform OSINT Analysis

- **Threat Intelligence Lookup:**
    - Search for known PowerShell exploitation patterns or IOCs associated with privilege escalation.
    - Use tools like AlienVault OTX or ThreatMiner for matching malicious commands.

Step 4: Take Immediate Action

- **Disable the User Account:** Disable employee1 to prevent further misuse.
- **Contain the Host:** Isolate HR-Laptop from the network to prevent further activity.
- **Block PowerShell Execution:** Apply Group Policy to restrict unauthorised PowerShell scripts.

Step 5: Escalate to L2/L3 Teams

- **Forensic Analysis:**
    - Capture a memory dump of HR-Laptop for analysis.
    - Investigate if malicious scripts were downloaded or if persistence mechanisms were established.
- **Review File Server Integrity:**
    - Verify that no files were modified or exfiltrated further.

Step 6: Remediation

- **Patch Management:** Ensure the exploited vulnerability on HR-Laptop is patched.
- **Least Privilege Policy:** Review and enforce policies to minimise administrative rights.
- **File Access Monitoring:** Implement alerts for access to sensitive files outside working hours.

SCENARIO 10: BRUTE-FORCE ATTACK FOLLOWED BY SUCCESSFUL UNAUTHORISED LOGIN

A brute-force attack targets a public-facing web application login portal. The attacker attempts multiple username-password combinations, ultimately succeeding in accessing an admin account. The compromised account is then used to execute unauthorised administrative actions.

SIEM Rule for Detection

- **Rule Name:** Brute-Force Login Attempts and Suspicious Admin Actions
- **Conditions:**
  - Repeated failed login attempts on the same account within a short period (10 attempts in 1 minute).
  - Successful login after numerous failed attempts.
  - Subsequent actions inconsistent with the user's typical behavior, such as admin-level changes or new user creation.

Logs

Web Application Login

Timestamp	IP Address	Username	Action	Result
2024-11-25 01:30:10	192.168.1.100	admin	Login Attempt	Failed
2024-11-25 01:30:12	192.168.1.100	admin	Login Attempt	Failed
2024-11-25 01:30:15	192.168.1.100	admin	Login Attempt	Failed
2024-11-25 01:30:20	192.168.1.100	admin	Login Attempt	Success

Admin Actions

Timestamp	User	Action	Details
2024-11-25 01:35:00	admin	Created New Admin User	Username: temp_admin
2024-11-25 01:40:00	admin	Deleted Logs	Target: Application Logs
2024-11-25 01:45:00	temp_admin	Accessed Sensitive Data	Table: User_Credentials

How the Rule Detects the Attack

1. **Brute-Force Detection:**

    - Multiple failed login attempts for the admin account are flagged as suspicious activity.
    - A subsequent successful login after repeated failures suggests potential brute-force success.
2. **Anomalous Admin Actions:**
    - After login, unusual administrative actions (creating a new admin account, deleting logs) are logged.
    - The use of the newly created admin account (temp_admin) to access sensitive data further raises suspicion.
3. **Correlation of Events:**
    - The SIEM correlates the brute-force attack with the unauthorised login and subsequent admin actions, generating a high-severity alert.

SIEM Alert Details

- **Alert Name:** Brute-Force Login and Suspicious Admin Actions
- **Severity Level:** Critical
- **Triggered By:** Rule: Multiple Failed Logins Followed by Admin Actions
- **Time:** 2024-11-25 01:30:20
- **Source Host:** Public Web Server (192.168.1.100)
- **Details:** Brute-force attack detected against the admin account, followed by unauthorised login and suspicious admin activities.

Steps for L1 Analyst

Step 1: Investigate Login Attempts

- **Check Login Logs:**
    - Identify the source IP (192.168.1.100) responsible for repeated failed login attempts.
    - Verify if the successful login is consistent with typical admin behavior (login time, IP location).
- **Geo-IP Lookup:**
    - Use tools like iplocation.net or MaxMind GeoIP to determine the source IP's geographic location.
    - Confirm if the login originated from an expected or unusual region.

Step 2: Investigate Post-Login Actions

- **Review Admin Activity Logs:**
  - Check for unusual actions performed by the admin account:
    - Creation of a new admin user (temp_admin).
    - Deletion of application logs.
    - Accessing sensitive user credential tables.
- **Determine User Behavior:**
  - Verify if the admin user typically performs these actions.
  - Investigate whether the new admin account creation was authorised.

Step 3: Cross-Check Threat Intelligence

- **Check the IP Address Reputation:**
  - Use threat intelligence tools like AlienVault OTX, VirusTotal or AbuseIPDB to verify if the IP (192.168.1.100) is associated with malicious activity.
- **Inspect Brute-Force Patterns:**
  - Look for known brute-force attack indicators, such as tools used (Hydra or Burp Suite).

Step 4: Immediate Response

- **Block the Attacker's IP:**
  - Apply a firewall rule to block incoming traffic from 192.168.1.100.
- **Disable Compromised Accounts:**
  - Temporarily disable both the admin and temp_admin accounts.
- **Secure the Application:**
  - Enforce strong password policies and implement account lockout after several failed attempts.
  - Enable multi-factor authentication (MFA) for admin accounts.

Step 5: Escalate to L2/L3 Teams

- **Forensic Analysis:**
  - Capture a full log of the attacker's activity for deeper investigation.
  - Perform memory and disk analysis on the affected server to identify potential backdoors or malicious scripts.
- **Check for Data Exfiltration:**
  - Analyse network traffic logs to determine if sensitive data was exfiltrated after login.

Step 6: Long-Term Mitigation

- **Enhance Login Security:**
  - Implement rate-limiting on login attempts.
  - Introduce CAPTCHA to prevent automated brute-force attacks.
- **Log Retention and Monitoring:**
  - Prevent admin users from deleting critical logs without approval.
  - Regularly monitor login activity for suspicious patterns.
- **Threat Simulation and Testing:**
  - Conduct periodic penetration tests to ensure the web application is resilient to brute-force attacks.

SCENARIO 11: DATA EXFILTRATION VIA DNS TUNNELING

An attacker compromises an internal system and exfiltrates sensitive data using DNS tunneling. The attacker encodes the data into DNS queries, bypassing traditional detection mechanisms since DNS traffic is often permitted and unmonitored.

SIEM Rule for Detection

- **Rule Name:** Anomalous DNS Query Activity
- **Conditions:**
  - High frequency of DNS queries to uncommon or newly registered domains.
  - Large data payloads encoded in DNS query names.
  - DNS queries with unusual patterns, such as subdomains with randomised characters.

Log

DNS Query

Timestamp	Source IP	Destination Domain	Query Length	Response Size
2024-11-25 10:01:10	192.168.1.50	abcdefghij.encodeddata1.example.com	75	50
2024-11-25 10:01:15	192.168.1.50	klmnopqrst.encodeddata2.example.com	80	55
2024-11-25 10:01:20	192.168.1.50	uvwxyzabcd.encodeddata3.example.com	78	60
2024-11-25 10:01:25	192.168.1.50	efghijklmn.encodeddata4.example.com	85	50

How the Rule Detects the Attack

1. **Unusual DNS Query Patterns:**
   - DNS query logs show randomised subdomains, which is atypical for normal network traffic.
2. **High Volume of Queries:**
   - Multiple DNS queries to the same domain with incremental patterns suggest potential data transmission.
3. **Correlation with External Threat Feeds:**

   - The domain (example.com) is newly registered and flagged as suspicious by threat intelligence sources.

SIEM Alert Details

- **Alert Name:** Suspicious DNS Tunneling Activity Detected
- **Severity Level:** High
- **Triggered By:** High-frequency DNS queries with large query lengths to an unknown domain.
- **Source Host:** Internal Host (192.168.1.50).
- **Details:** Possible data exfiltration detected via DNS tunneling.

Steps for L1 Analyst

Step 1: Investigate DNS Query Logs

- **Analyse Traffic Patterns:**
  - Review logs for DNS queries originating from the source IP (192.168.1.50).
  - Look for irregular query names (long, randomised subdomains).
- **Check Query Frequency:**
  - Identify if the queries occur in quick succession, indicating potential automated behavior.

Step 2: Correlate with Network Logs

- **Look for Matching Traffic:**
  - Use network logs to verify if large volumes of outbound traffic correspond to DNS queries.
- **Verify Domain Reputation:**
  - Query the suspicious domain (example.com) using tools like VirusTotal, AlienVault OTX or IBM X-Force Exchange for threat intelligence.

Step 3: Cross-Check with Endpoint Logs

- **Check the Host System:**
  - Analyse the system at 192.168.1.50 for signs of compromise:
    - Suspicious processes.
    - Unauthorised tools like tunneling software (iodine, dnscat2).
- **Inspect Data Movement:**
  - Look for files or processes that might be encoding data for transmission.

Immediate Response

1. **Isolate the Affected Host:**
   - Disconnect 192.168.1.50 from the network to prevent further data exfiltration.
2. **Block Malicious Domains:**
   - Add the destination domain (example.com) to the DNS blocklist.
3. **Capture Traffic:**
   - Use a network monitoring tool (Wireshark) to capture and decode live DNS traffic.

Forensic Analysis

1. **Review Full Network Traffic:**
   - Use captured PCAP files to reconstruct encoded DNS queries and verify the data being exfiltrated.
2. **Endpoint Analysis:**
   - Perform memory and disk analysis on the affected system using tools like Volatility or FTK.
3. **Identify Root Cause:**
   - Determine how the attacker gained access to the system (phishing, exploiting vulnerabilities).

Long-Term Mitigation

1. **Implement DNS Monitoring:**
   - Deploy DNS logging and monitoring tools to detect unusual query patterns.
2. **Use Data Loss Prevention (DLP):**
   - Configure DLP solutions to block sensitive data transmission over DNS channels.
3. **Threat Intelligence Integration:**
   - Continuously update SIEM with threat intelligence feeds to detect malicious domains.
4. **Regular Security Audits:**
   - Conduct periodic vulnerability scans and pen tests to identify weaknesses in DNS configurations.

SCENARIO 12: UNAUTHORISED ACCESS TO CRITICAL DATABASE

A database containing sensitive customer data experiences unauthorised access. An attacker uses stolen credentials to log into the database server outside business hours and attempts to extract records. The activity triggers SIEM rules for unusual database queries and access anomalies.

SIEM Rule for Detection

- **Rule Name:** Anomalous Database Access
- **Conditions:**
  - Database access occurring during non-business hours.
  - Queries retrieving unusually high volumes of data.
  - Source IP or device not recognised as trusted.

Logs

Authentication

Timestamp	Source IP	Username	Event	Status
2024-11-25 02:15:10	203.0.113.45	db_admin	Login Attempt	Success
2024-11-25 02:15:20	203.0.113.45	db_admin	Privilege Escalation	Granted

Database Query

Timestamp	Username	Query	Data Retrieved
2024-11-25 02:16:00	db_admin	SELECT * FROM customers;	10,000 rows
2024-11-25 02:16:10	db_admin	SELECT * FROM transactions WHERE amount > 10,000;	5,000 rows

SIEM Alert

Alert Name	Severity	Details
Unusual Database Access Detected	High	Unusual login outside business hours and large data retrieval by "db_admin" from unknown IP.

How the Rule Detects the Attack

1. **Login Outside Business Hours:**
    - Access occurred at 2:15 AM, which is outside the organisation's usual operating hours.
2. **Unfamiliar Source IP:**
    - The access originated from an IP address (203.0.113.45) not associated with regular users.
3. **Large-Scale Data Queries:**
    - Queries retrieved unusually large volumes of data, raising suspicion of potential data theft.
4. **Privilege Escalation:**
    - The user escalated privileges immediately after logging in, which is abnormal behavior.

Steps for L1 Analyst

Step 1: Verify the Authentication Event

- **Check Login Time and Source:**
    - Confirm the login occurred during an unusual time (2:15 AM) from the IP (203.0.113.45).
    - Identify whether this IP is internal, external or a VPN endpoint.
- **Investigate Credential Use:**
    - Contact the user (db_admin) to verify if they logged in at the specified time.
    - If not, this indicates possible credential theft.

Step 2: Investigate the Database Activity

- **Analyse Query Logs:**
    - Review the executed queries. The SELECT * FROM customers query suggests an attempt to retrieve all customer data.
- **Identify Abnormal Patterns:**
    - Determine if the retrieved data volume exceeds typical access limits.
    - Cross-check with past activity logs for similar queries by the same user.

Step 3: Review Network Logs

- **Check Data Transmission:**
    - Look for large outbound data transfers originating from the database server.
    - Use tools like Wireshark to analyse traffic for possible exfiltration attempts.

Immediate Response

1. **Lock the Compromised Account:**
   - Disable or lock the db_admin account to prevent further unauthorised access.
2. **Block Untrusted IP:**
   - Add 203.0.113.45 to the blocklist to deny further network access.
3. **Preserve Evidence:**
   - Collect logs from the database server, SIEM and network monitoring tools for forensic analysis.

Forensic Analysis

1. **Trace Login Source:**
   - Use DNS and geolocation services to identify the physical location of 203.0.113.45.
   - Check if the IP is associated with known threat actors or compromised devices.
2. **Analyse Stolen Data:**
   - Determine the nature of the retrieved records (PII, financial data).
   - Assess whether sensitive data was successfully exfiltrated.
3. **Inspect Database Server:**
   - Check for malware or backdoors installed during the attack.
   - Analyse privilege escalation logs to understand how it was achieved.

Long-Term Mitigation

1. **Enhance Access Policies:**
   - Enforce multi-factor authentication (MFA) for privileged accounts.
   - Restrict login access to specific IP ranges or devices.
2. **Implement Database Activity Monitoring (DAM):**
   - Deploy DAM tools to continuously monitor and alert on unusual query patterns.
3. **Regularly Update Passwords:**
   - Encourage users to change passwords frequently and avoid reusing credentials.
4. **User Behavior Analytics (UBA):**
   - Integrate UBA into SIEM to detect deviations from normal user activity.