# UNDERSTANDING ANOMALIES IN CYBERSECURITY WITH EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

# TABLE OF CONTENTS

## BREAKDOWN OF ANOMALIES IN CYBERSECURITY

1. **Network Anomalies**
    - **Unusual Traffic Patterns:** Sudden spikes in traffic, unexpected communication between devices or data transfers to unknown external IPs.
    - **Abnormal Protocol Usage:** Use of non-standard protocols or ports, especially for critical systems.
    - **Geographical Anomalies:** Access or traffic originating from unexpected or unusual locations, such as foreign countries where the organisation doesn't operate.
2. **User Behaviour Anomalies**
    - **Unusual Login Times:** Users logging in at odd hours outside their normal working patterns.
    - **Multiple Failed Login Attempts:** A significant number of failed login attempts, which may indicate a brute-force attack.
    - **Unusual Access Patterns:** A user accessing files or systems they don’t typically interact with or downloading large amounts of data.
3. **Application Anomalies**
    - **Unexpected Process Execution:** New or unknown processes running on critical servers or endpoints, possibly indicating malware.
    - **Abnormal API Calls:** Applications making API requests that deviate from their usual behaviour or volume.
    - **Sudden Configuration Changes:** Unauthorised changes in application settings or configurations, which could indicate tampering.
4. **Data Anomalies**
    - **Data Exfiltration:** Unusually large volumes of data being transferred out of the network, especially to external locations.
    - **Data Integrity Issues:** Unexpected changes in data that may suggest tampering or corruption.
    - **Unusual Encryption Activity:** Sudden encryption of files, which could indicate a ransomware attack.

5. **System Anomalies**
    - **Unexpected System Reboots or Shutdowns:** Systems restarting or shutting down without a clear reason, potentially indicating a compromise or hardware failure.
    - **Unusual Resource Utilisation:** Unexplained spikes in CPU, memory or disk usage, possibly due to malicious processes.
    - **Anomalous Logs:** Log entries that are inconsistent with normal system behaviour, such as missing logs, unusual error messages or suspicious logins.
6. **Endpoint Anomalies**
    - **Unauthorised Device Connections:** Unknown devices connecting to the network, especially on endpoints with sensitive data.
    - **Malicious File Execution:** Execution of files that are flagged as suspicious or malicious by endpoint protection tools.
    - **Suspicious Software Installations:** Installation of software not typically used or required for business operations, which could be malware.
7. **Email Anomalies**
    - **Phishing Indicators:** Emails that contain suspicious links, attachments or requests for sensitive information.
    - **Unusual Email Volume:** A user sending an unusually high number of emails in a short time, especially with attachments or to external recipients.
    - **Unauthorised Forwarding Rules:** Forwarding rules created in email accounts that redirect incoming messages to external addresses.
8. **Cloud Anomalies**
    - **Unusual Cloud Access:** Access to cloud resources from unexpected IP addresses or geolocations.
    - **Abnormal Cloud Usage:** Sudden spikes in resource usage, such as excessive storage consumption or computing power.
    - **Anomalous API Requests:** Unusual API calls that deviate from the normal operations, potentially indicating a cloud compromise.

## EXAMPLES

1. **Network Traffic Anomaly**
    - **Scenario:** A company typically sees a steady amount of outbound traffic during business hours. Suddenly, at 2:00 AM, there's an unusual spike in data being transferred to an external server in a foreign country.
    - **Explanation:** This could be an indication of data exfiltration, where sensitive information is being stolen and sent to an unauthorised location.
2. **User Behaviour Anomaly**
    - **Scenario:** An employee who usually logs in from Kuala Lumpur between 9:00 AM and 6:00 PM suddenly logs in from a different city at 3:00 AM and accesses sensitive financial records they've never touched before.
    - **Explanation:** This could be a sign of a compromised account where an attacker has gained access and is attempting to steal or manipulate data.
3. **System Performance Anomaly**
    - **Scenario:** A server that usually operates with 30% CPU usage suddenly spikes to 90% usage without any scheduled task or significant increase in legitimate activity.
    - **Explanation:** This might indicate a distributed denial-of-service (DDoS) attack, a cryptocurrency mining malware infection or other forms of malicious activity that exploit system resources.
4. **Application Anomaly**
    - **Scenario:** A web application suddenly starts producing error messages when users attempt to log in and the application begins sending data to an unknown IP address.
    - **Explanation:** This could indicate that the application has been compromised, possibly through a web-based attack like SQL injection or cross-site scripting (XSS), leading to unauthorised access and data theft.
5. **File Access Anomaly**
    - **Scenario:** A user who typically works with marketing documents starts accessing engineering design files stored on the company's network share.
    - **Explanation:** This could be a sign of insider threat activity or a compromised account being used to gather sensitive information from different departments.

## SIMULATIONS

### Scenario 1: Anomalous Network Traffic Detected in a Financial Institution

**Background:** A financial institution's Security Operations Centre (SOC) monitors all network traffic to detect potential security incidents. The SOC uses a SIEM (Security Information and Event Management) system integrated with network traffic monitoring tools to alert analysts of any unusual activities.

- **Date:** 17 August 2024
- **Time:** 2:30 AM
- **Location:** Headquarters in Kuala Lumpur, Malaysia
- **Typical Network Traffic:** 50 GB of data transferred daily, mostly during business hours (8:00 AM - 6:00 PM)
- **Anomaly:** 20 GB of data transferred to an external IP address during off-hours (2:00 AM - 3:00 AM)

**Detailed Analysis:**

1. **Event Detection:**
    - **Alert:** At 2:45 AM, the SIEM system triggered an alert for an unusual spike in outbound network traffic. The traffic volume reached 20 GB, directed towards an external IP address (203.0.113.55) located in a different country.
    - **Normal Pattern:** The typical outbound traffic during off-hours is minimal, averaging less than 1 GB per hour.
2. **Investigation:**
    - **Initial Review:** The SOC analyst reviewed the network logs and noticed the anomaly in data transfer volume. The external IP address (203.0.113.55) is not recognised as a regular business partner or vendor.
    - **Source of Traffic:** The traffic originated from a server within the internal network (IP: 192.168.10.45) that hosts sensitive financial data and is normally accessed only by the finance department during business hours.
    - **Unusual Activity:** The data transfer occurred outside regular business hours and the server involved had no scheduled tasks or authorised data transfers at this time.
3. **Contextual Analysis:**

   - **User Access:** The server was accessed using credentials of an employee (Izzmier, username: izzmier), who typically works 9:00 AM - 6:00 PM and had no business reason to be accessing the server at 2:00 AM.
   - **VPN Logs:** The VPN logs indicated that Izzmier's account was used to log in from a foreign IP address (198.51.100.23), which had never been associated with this user before. This raised further suspicion of credential compromise.
   - **Historical Data:** A review of the past 30 days showed no similar data transfer events or patterns, confirming this activity was highly irregular.

4. **Threat Hypothesis:**
   - **Potential Data Exfiltration:** The unusual volume of data transferred to an unknown external IP during off-hours, combined with the use of potentially compromised credentials, strongly suggests a data exfiltration attempt.
5. **Mitigation Actions:**
   - **Immediate Containment:** The SOC immediately blocked all outgoing traffic from the affected server and disconnected it from the network to prevent further data loss.
   - **User Account Suspension:** Izzmier's account was suspended pending further investigation to prevent unauthorised access.
   - **External IP Blacklisting:** The external IP address (203.0.113.55) was blacklisted across the firewall to prevent any further communication.
   - **Incident Response Team Activation:** The incident response team was alerted to investigate the potential breach and assess the scope of the data exfiltration.
6. **Root Cause Analysis:**
   - **Credential Compromise:** Further investigation revealed that Izzmier's credentials were likely compromised through a phishing email received two days prior. The email contained a malicious link that led to a fake login page mimicking the company’s VPN portal.
   - **Lack of Multi-Factor Authentication (MFA):** The absence of MFA allowed the attacker to access the network using just the stolen credentials, highlighting a gap in the organisation’s security posture.
7. **Post-Incident Actions:**

- **Enhanced Monitoring:** The SOC increased monitoring on all sensitive servers, particularly during off-hours, to detect any further anomalies.
- **Security Awareness Training:** The company initiated a mandatory security awareness training program focusing on phishing attacks and the importance of MFA.
- **MFA Implementation:** Multi-Factor Authentication was quickly rolled out across all remote access systems to prevent similar incidents in the future.
- **Forensic Analysis:** A forensic analysis of the affected server was conducted to identify any other malicious activities and ensure no backdoors were left by the attacker.

8. **Reporting:**
    - **Executive Summary:** A report was prepared for the executive team, summarising the incident, the potential impact, the steps taken to contain and mitigate the threat and recommendations for strengthening the organisation's security posture.
    - **Regulatory Reporting:** Given the financial institution's compliance requirements, the incident was reported to the relevant regulatory bodies, detailing the nature of the breach and the response actions taken.

**Scenario 2: Anomalous User Behaviour in a Healthcare Organisation**

**Background:** A healthcare organisation's SOC monitors user activity to ensure that access to sensitive patient data complies with HIPAA (Health Insurance Portability and Accountability Act) regulations. The SOC uses user behaviour analytics (UBA) integrated with their SIEM to identify potential insider threats or compromised accounts.

- **Date:** 17 August 2024
- **Time:** 11:30 PM
- **Location:** Hospital in Kuala Lumpur, Malaysia
- **Typical User Behaviour:** Healthcare staff access patient records primarily during business hours (7:00 AM - 7:00 PM). Access to records is restricted to medical staff directly involved in patient care.
- **Anomaly:** A nurse, typically assigned to general wards, accessed a large volume of oncology patient records late at night.

**Detailed Analysis:**

1. **Event Detection:**
    - **Alert:** At 11:45 PM, the UBA system triggered an alert for unusual access patterns. The nurse, Iffah (username: iffah), accessed 50 oncology patient records between 11:00 PM and 11:30 PM.
    - **Normal Pattern:** Iffah usually works day shifts in the general wards and rarely accesses oncology patient records. Her typical access is limited to around 5-10 records per shift, all related to her ward.
2. **Investigation:**
    - **Initial Review:** The SOC analyst reviewed the access logs and noted the discrepancy. Iffah's access to a high volume of records from a different department (Oncology) was unusual, especially late at night.
    - **User Role:** Iffah’s role as a nurse in the general wards does not require her to access oncology patient data, raising concerns about the legitimacy of this access.
    - **Access Source:** The access was made from a workstation in the Oncology department, which Iffah is not typically assigned to.
3. **Contextual Analysis:**

- **Shift Timing:** Iffah's shift ended at 7:00 PM, making her presence in the hospital after hours without a valid reason unusual. There was no scheduled overtime or night shift for her on this date.
- **Previous Activity:** A review of her access patterns over the past three months showed no previous instances of accessing oncology patient records, reinforcing the abnormality of this event.
- **Workstation Logs:** The workstation in Oncology, from which the access was made, had no other unusual activities logged. However, it was noted that another employee from Oncology had recently reported suspicious emails.

4. **Threat Hypothesis:**
    - **Potential Insider Threat:** The anomalous access suggests that Iffah might be involved in unauthorised data collection, possibly for malicious purposes. Alternatively, her credentials might have been compromised, leading to unauthorised access by another party.
5. **Mitigation Actions:**
    - **Immediate Lockdown:** Access to the electronic medical records (EMR) system was immediately suspended for Iffah pending further investigation.
    - **Physical Security Check:** Hospital security was notified to verify Iffah's presence in the building after hours. She was found to have left the premises earlier, contradicting the late-night access logs.
    - **Workstation Quarantine:** The workstation in Oncology was quarantined for forensic analysis to determine if any malware or unauthorised access tools had been installed.
6. **Root Cause Analysis:**
    - **Credential Compromise:** Further investigation revealed that Iffah's credentials had been compromised. A phishing email, which she opened earlier in the week, had installed keylogging malware on her work computer, capturing her login details.
    - **Malicious Access:** The compromised credentials were used by an external attacker to gain unauthorised access to the EMR system late at night, using the Oncology workstation.
7. **Post-Incident Actions:**

- **Credential Reset:** Iffah's credentials were reset and she was advised on stronger password practices. Additional MFA (Multi-Factor Authentication) was enforced for all users accessing sensitive patient records.
- **Employee Training:** A hospital-wide security awareness training was launched, focusing on identifying phishing emails and protecting login credentials.
- **Forensic Analysis:** A detailed forensic investigation of the compromised workstation was conducted to identify any backdoors or other malware that could have been used to facilitate the attack.
- **Incident Documentation:** A thorough incident report was compiled, documenting the event, the investigation findings and the steps taken to resolve the issue.

8. **Reporting:**
   - **Regulatory Reporting:** Given the breach of patient data, the incident was reported to the Ministry of Health Malaysia, along with details on the compromised records and the mitigation steps taken.
   - **Executive Summary:** An executive summary was prepared for the hospital's board of directors, outlining the incident, the potential impact on patient confidentiality and recommendations for preventing future occurrences.

**Scenario 3: Anomalous System Performance in a Retail Company's Payment Processing Server**

**Background:** A large retail company uses a dedicated server to process online payments. The server is monitored by the SOC for any unusual activity, given its critical role in handling financial transactions. The company uses an Intrusion Detection System (IDS) and a SIEM to monitor system performance and network traffic.

- **Date:** 17 August 2024
- **Time:** 4:00 AM
- **Location:** Data Centre in Cyberjaya, Malaysia
- **Typical System Performance:** The payment processing server (IP: 10.0.0.5) usually operates at 30% CPU usage during peak hours and less than 10% during off-hours.
- **Anomaly:** CPU usage spikes to 95% at 4:00 AM, along with unusual outbound network traffic to an unknown IP address.

**Detailed Analysis:**

1. **Event Detection:**
    - **Alert:** At 4:05 AM, the SIEM system triggered an alert for an abnormal spike in CPU usage on the payment processing server, which had reached 95% and sustained this level for over 30 minutes.
    - **Normal Pattern:** During off-hours (12:00 AM - 6:00 AM), the CPU usage typically remains below 10%. No scheduled tasks or maintenance were planned at this time.
2. **Investigation:**
    - **Initial Review:** The SOC analyst reviewed the server logs and noted that the spike in CPU usage coincided with an unusual amount of outbound network traffic directed towards an unknown external IP address (192.0.2.25).
    - **Process Analysis:** A process running under the name svchost.exe was consuming an unusually high amount of CPU resources. This process is typically legitimate but can be exploited by malware to disguise malicious activities.
    - **Network Traffic:** The outbound traffic was encrypted and being sent to the external IP over a non-standard port (TCP 8081), which is not typically used for legitimate transactions or communications.

3. **Contextual Analysis:**
    - **Unusual Timing:** The anomaly occurred during off-hours when the system should be idle, raising concerns about unauthorised activity.
    - **Historical Data:** A review of the past month's logs showed no similar spikes in CPU usage or unusual network traffic at this time, confirming the anomaly's uniqueness.
    - **External IP Reputation:** A quick lookup of the external IP address (192.0.2.25) revealed it to be associated with known Command and Control (C2) servers used by botnets to communicate with compromised systems.
4. **Threat Hypothesis:**
    - **Potential Malware Infection:** The combination of high CPU usage, unusual network traffic to a suspicious external IP and the use of svchost.exe suggests that the server might be infected with malware, potentially part of a botnet operation.
5. **Mitigation Actions:**
    - **Immediate Isolation:** The payment processing server was immediately isolated from the network to prevent further data exfiltration and communication with the suspected C2 server.
    - **Malware Scan:** A full antivirus and malware scan was conducted on the server, which identified and quarantined a Trojan that had infiltrated the system via a compromised RDP (Remote Desktop Protocol) session.
    - **Outbound Traffic Block:** The firewall was updated to block all outbound traffic to the suspicious IP (192.0.2.25) and any similar IPs associated with known C2 servers.
6. **Root Cause Analysis:**
    - **RDP Compromise:** Further investigation revealed that an RDP session had been compromised through brute-force attacks. The attacker gained access to the server and deployed the malware, which then established communication with the C2 server.
    - **Inadequate RDP Security:** The RDP service was found to be running without strong authentication measures or IP whitelisting, making it vulnerable to such attacks.
7. **Post-Incident Actions:**

- **RDP Security Hardening:** All RDP services across the company were reviewed and secured by implementing MFA, IP whitelisting and stronger password policies.
- **Botnet Detection:** The SOC implemented additional IDS signatures to detect traffic patterns associated with botnet activity, especially on critical servers like the payment processor.
- **Server Patching:** The server was fully patched with the latest security updates to address any vulnerabilities that could have been exploited by the attackers.

8. **Reporting:**
    - **Executive Summary:** A report was prepared for the executive team, summarising the incident, the financial risks and the steps taken to secure the payment processing system.
    - **Customer Notification:** As the server handled payment processing, customers were notified of the potential breach, with reassurances that no payment data was believed to have been compromised due to the quick isolation of the server.

**Scenario 4: Anomalous File Activity on a Government Agency's Internal Network**

**Background:** A government agency's internal network is monitored by a SOC to protect sensitive data, including classified documents. The agency uses Data Loss Prevention (DLP) tools and a SIEM to detect and respond to unauthorised file access, modifications or transfers.

- **Date:** 17 August 2024
- **Time:** 2:00 PM
- **Location:** Government Office in Putrajaya, Malaysia
- **Typical File Activity:** Access to classified files is tightly controlled and audited. Files are accessed only by authorised personnel and typically during working hours (8:00 AM - 6:00 PM). File modifications are rare and usually involve a single document.
- **Anomaly:** Multiple classified documents were accessed, modified and copied within a short time frame by a user who typically does not have access to this level of data.

**Detailed Analysis:**

1. **Event Detection:**
    - **Alert:** At 2:15 PM, the DLP system triggered an alert when an employee, Noussair (username: noussair), accessed and copied 20 classified documents from a secure file server within 10 minutes. The SIEM correlated this with unusual file modifications detected by the file integrity monitoring (FIM) system.
    - **Normal Pattern:** Noussairis an IT support technician with limited access to low-level internal documentation. His role does not require access to classified files, especially those marked as "Top Secret."
2. **Investigation:**
    - **Initial Review:** The SOC analyst reviewed the file access logs and confirmed that Noussair accessed and modified multiple classified documents, transferring copies to a removable USB drive.
    - **Access Rights:** A quick check of Noussair'suser profile showed that his account should not have permissions to access or modify classified documents. This raised immediate concerns about how these permissions were obtained.

- **File Modifications:** The FIM logs indicated that metadata within the files had been altered, suggesting a possible attempt to tamper with document integrity or cover tracks.

3. **Contextual Analysis:**
    - **User Activity:** Noussair'srecent activity showed no previous interaction with classified files, making this sudden spike in access highly suspicious.
    - **Access Source:** The logs indicated that the access occurred from Noussair'susual workstation, but the volume of data transferred and modified was inconsistent with his typical workload.
    - **Permission Escalation:** A review of the user account management logs revealed that Noussair'saccount permissions were escalated approximately one hour before the file access occurred. This escalation was performed using an administrative account that had been inactive for several months.
4. **Threat Hypothesis:**
    - **Potential Insider Threat:** The pattern of access suggests that Noussair may have escalated his own privileges or someone may have compromised his account to perform the unauthorised file operations.
    - **Possible Data Exfiltration:** The copying of classified documents to a USB drive raises concerns about data exfiltration, potentially to be shared with unauthorised parties or used for malicious purposes.
5. **Mitigation Actions:**
    - **Account Lockdown:** Noussair'saccount was immediately disabled to prevent any further unauthorised access.
    - **USB Device Seizure:** Physical security teams were notified to locate Noussair and confiscate the USB device he used for the data transfer.
    - **Administrative Account Review:** The SOC performed an audit on the compromised administrative account, identifying any other suspicious activity or unauthorised access. The account was disabled and its credentials were reset.
6. **Root Cause Analysis:**
    - **Privilege Escalation:** Forensic analysis revealed that Noussair had used a PowerShell script to exploit a vulnerability in the agency's Active

Directory, allowing him to escalate his privileges temporarily. The script was found in his user profile, hidden among legitimate IT support tools.

- **Unauthorised Access:** Once privileges were escalated, Noussair accessed the classified file server, modified the documents and copied them to the USB drive.

7. **Post-Incident Actions:**
    - **Vulnerability Patch:** The identified Active Directory vulnerability was patched and a full review of account privileges and group policies was conducted to prevent similar attacks.
    - **Security Awareness:** All IT personnel received additional training on the risks of privilege escalation and the importance of adhering to access control policies.
    - **DLP Enhancement:** The DLP system's rules were updated to more aggressively monitor for unusual file activity, including large-volume data transfers, especially involving removable media.
    - **Legal and Disciplinary Action:** The incident was referred to the agency's internal investigation unit and legal actions were initiated against Noussair for the unauthorised access and potential breach of classified information.
8. **Reporting:**
    - **Incident Report:** A detailed incident report was prepared and shared with the agency's senior leadership, outlining the nature of the breach, the steps taken to mitigate it and recommendations for preventing future incidents.
    - **Government Compliance:** Given the sensitive nature of the data involved, the incident was reported to the relevant governmental oversight bodies, along with a compliance report detailing the measures implemented post-incident.

### Scenario 5: Anomalous Outbound Traffic from a Healthcare Company's Database Server

**Background:** A healthcare company manages a vast database containing sensitive patient records. The company’s IT infrastructure includes a database server dedicated to storing and managing these records. Given the critical nature of the data, the server is closely monitored using a combination of firewalls, IDS/IPS systems and a SIEM solution. Regular traffic to and from the server primarily involves internal communications with the company's application servers and secure backup systems.

**Fake Data Overview:**

- **Date:** 17 August 2024
- **Time:** 11:30 PM
- **Location:** Data Centre in Kuala Lumpur, Malaysia
- **Typical Network Traffic:** The database server (IP: 192.168.10.5) typically communicates internally, with minimal to no outbound traffic to external IP addresses. Off-hours traffic is usually limited to backup operations and internal data syncing.
- **Anomaly:** An unexpected spike in outbound traffic was detected, with a large volume of data being transmitted to an external IP address over a non-standard port.

**Detailed Analysis:**

1. **Event Detection:**
    - **Alert:** At 11:35 PM, the SIEM system flagged an anomaly when the database server began transmitting a significant amount of data to an external IP address (203.0.113.45) using port 4444, which is uncommon for database server communications.
    - **Normal Pattern:** The database server should not have any direct communication with external IP addresses, especially not during off-hours.
2. **Investigation:**
    - **Initial Review:** The SOC analyst reviewed the firewall and IDS logs, confirming that over 500 MB of data had been sent to the external IP in a span of 15 minutes. The traffic originated from a process named dbsync.exe, which typically handles internal data synchronisation.

- **Network Traffic Analysis:** The outbound traffic was encrypted but sent over a non-standard port (4444), which is often associated with malicious activities such as reverse shells or data exfiltration attempts.
- **Data Transmission Source:** The traffic originated from a non-critical folder on the database server, which should not have been involved in external communications. This indicated that the process might have been hijacked or spoofed.

3. **Contextual Analysis:**
    - **User Activity:** No scheduled tasks or backup operations were planned at this time. A review of user activity logs revealed that no legitimate users were logged in or executing commands on the database server.
    - **Historical Traffic:** A review of historical network traffic from the database server showed no previous instances of communication with the external IP address, confirming this as a unique and potentially malicious event.
    - **External IP Reputation:** The external IP address (203.0.113.45) was found to be associated with previous cyber-attacks, specifically those involving data exfiltration by sophisticated threat actors.
4. **Threat Hypothesis:**
    - **Compromised Server:** The anomalous traffic suggests that the database server may have been compromised by an attacker who managed to exfiltrate sensitive patient data to the external IP address.
    - **Potential Backdoor:** The use of port 4444 and the atypical process dbsync.exe indicates the possibility of a backdoor installed on the server, enabling the attacker to exfiltrate data stealthily.
5. **Mitigation Actions:**
    - **Immediate Network Isolation:** The database server was immediately isolated from the network to prevent further data transmission and to contain the potential breach.
    - **Process Termination:** The suspicious process dbsync.exe was terminated to halt any ongoing data exfiltration attempts.
    - **Detailed Forensic Analysis:** A forensic investigation was launched to examine the compromised server for malware, rootkits or any unauthorised access logs. The investigation revealed the presence of a backdoor trojan, which had been running on the server for the past two days.

6. **Root Cause Analysis:**
    - **Unauthorised Access:** The forensic team discovered that the attacker had gained access to the server via an unpatched vulnerability in the server's web interface. This vulnerability allowed the attacker to upload and execute the malicious dbsync.exe file, enabling unauthorised data transfer.
    - **Privilege Escalation:** The attacker used the backdoor to escalate privileges, giving them the ability to access and exfiltrate sensitive data stored in the database.
7. **Post-Incident Actions:**
    - **Patch Management:** The vulnerability in the server's web interface was patched immediately to prevent further exploitation. A comprehensive vulnerability assessment was conducted across all critical infrastructure to identify and address similar weaknesses.
    - **Enhanced Monitoring:** The SOC implemented enhanced monitoring rules in the SIEM to detect unusual outbound traffic patterns, especially those involving sensitive servers like the database.
    - **Access Control Review:** The incident prompted a review and tightening of access controls, particularly for critical servers, to limit the potential attack surface for similar breaches.
    - **Data Loss Impact Assessment:** A thorough assessment was conducted to determine the extent of the data exfiltration and to assess the potential impact on patients. Notifications were prepared for any potentially affected individuals as per regulatory requirements.
8. **Reporting:**
    - **Incident Report:** A detailed report was compiled and presented to the company's executive team and the board, explaining the breach, the data loss and the corrective actions taken.
    - **Regulatory Compliance:** The breach was reported to relevant healthcare regulatory bodies and the company worked closely with legal and compliance teams to ensure all necessary notifications and remedial actions were carried out.

## Scenario 6: Anomalous Email Activity in a Financial Institution

**Background:** A major financial institution in Malaysia, responsible for handling sensitive financial data and transactions, uses email for internal communication and customer service. The institution employs advanced email security gateways, a SIEM and DLP systems to monitor and secure email communications. Normally, email traffic involves regular communication between employees, clients and automated alerts from financial systems.

**Fake Data Overview:**

- **Date:** 17 August 2024
- **Time:** 9:00 AM
- **Location:** Kuala Lumpur, Malaysia
- **Typical Email Activity:** Employees use emails mainly for client communication, internal updates and automated notifications from financial systems. Outgoing emails with attachments are generally limited to customer service, legal and financial reporting departments. Email content is monitored for sensitive information such as financial data or personally identifiable information (PII).
- **Anomaly:** An unusually large number of outgoing emails containing encrypted ZIP file attachments were detected, sent from an employee's account that typically has low email traffic and no history of sending encrypted files.

**Detailed Analysis:**

1. **Event Detection:**
   - **Alert:** At 9:15 AM, the email security gateway triggered an alert when Garnacho (username: garnacho), an HR officer, sent 50 emails in rapid succession to various external email addresses. Each email contained an encrypted ZIP file as an attachment, which is uncommon for Garnacho’s role.
   - **Normal Pattern:** Garnacho’s email activity typically involves internal communication with the HR department and occasionally sending non-sensitive documents to job applicants. Her account had no history of sending encrypted files or emailing external contacts outside HR-related purposes.
2. **Investigation:**
   - **Initial Review:** The SOC analyst reviewed the email logs and discovered that the outgoing emails were sent to a mix of personal and professional

email addresses, none of which were recognised as regular recipients by the institution.

- **Attachment Analysis:** The encrypted ZIP files could not be opened directly without a password. This encryption and the volume of emails raised red flags, suggesting possible data exfiltration or phishing attempts.
- **Source of Anomaly:** The emails were sent from Garnacho's usual work laptop, connected to the corporate network. However, the timing and pattern of the emails did not match her typical working hours or habits.

3. **Contextual Analysis:**
   - **User Activity:** Logs showed that Sarah logged in at 8:50 AM, just before the emails were sent. However, she had also logged in the previous evening at 8:00 PM and remained active for several hours—a behaviour inconsistent with her normal working pattern.
   - **Phishing or Compromise:** The SOC team checked for recent phishing attempts and found that Garnacho's email account had received several suspicious emails in the past few days. One of these emails contained a malicious attachment disguised as a corporate policy update.
   - **Behavioural Anomaly:** The volume and timing of the emails, along with the use of encrypted ZIP files, were highly unusual for an HR officer. This, coupled with the earlier login activity, suggested that Garnacho's account might have been compromised.
4. **Threat Hypothesis:**
   - **Compromised Account:** It is likely that Garnacho's account was compromised by a threat actor who gained access through a phishing attack. The attacker then used her account to send out potentially malicious attachments to external targets.
   - **Data Exfiltration:** The encrypted ZIP files could contain sensitive data exfiltrated from the institution's internal systems or they might be used to deliver malware to the recipients.
5. **Mitigation Actions:**
   - **Immediate Account Lockdown:** Garnacho's account was locked and she was contacted to confirm her recent activity. It was determined that she was unaware of the suspicious emails, confirming that her account had been compromised.

- **Email Recall and Block:** The IT team initiated an email recall for the suspicious messages and configured the email gateway to block any further emails with similar attachments. The external recipients were also contacted to prevent them from opening the encrypted ZIP files.
- **Forensic Analysis:** The SOC team conducted a forensic analysis on Garnacho's laptop and email account. They discovered that the phishing email she received the previous evening contained a macro-based malware that logged her credentials and allowed remote access to her email.

6. **Root Cause Analysis:**
    - **Phishing Attack:** The investigation confirmed that Garnacho's account was compromised via a successful phishing attack. The attacker used stolen credentials to access her email and send the malicious emails.
    - **Lack of Awareness:** Sarah had not reported the suspicious email she received, highlighting a gap in employee training on phishing awareness and reporting procedures.
7. **Post-Incident Actions:**
    - **Credential Reset:** Garnacho's credentials were reset and multi-factor authentication (MFA) was enforced across all employee accounts to reduce the risk of future compromises.
    - **Employee Training:** The institution rolled out a mandatory phishing awareness training program, focusing on identifying and reporting suspicious emails and attachments.
    - **Enhanced Monitoring:** The SOC updated the SIEM rules to detect unusual login times and the sending of encrypted files by employees who do not typically engage in such activities. The email security gateway was also reconfigured to flag emails with encrypted attachments for additional review.
    - **Phishing Campaign Simulation:** The institution conducted a simulated phishing campaign to assess the effectiveness of the training and identify any remaining vulnerabilities.
8. **Reporting:**
    - **Incident Report:** A comprehensive report was prepared for the institution's cybersecurity leadership, detailing the phishing attack, the compromise of Garnacho's account and the steps taken to mitigate the incident.

- **Regulatory Compliance:** The incident was reviewed to ensure compliance with financial and data protection regulations. Given that no customer data appeared to have been exfiltrated, the breach was classified as low impact, but lessons learned were documented for future reference.