MASTERING XDR WITH SIEM INTEGRATION, EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

Table of Contents

XDR WITH SIEM *3*

MASTERING XDR 3

COMBINING XDR AND SIEM 5

EXAMPLES AND SIMULATIONS *7*

SCENARIO 1: MULTIPLE FAILED LOGIN ATTEMPTS 7

SCENARIO 2: ATTEMPTED DATA EXFILTRATION 13

SCENARIO 3: PRIVILEGE ESCALATION ATTEMPT 19

SCENARIO 4: C2 CONNECTION ATTEMPT 25

SCENARIO 5: UNTRUSTED SSL CERTIFICATE 31

XDR WITH SIEM

MASTERING XDR

1. **Understand XDR Fundamentals**
    - Understand how it extends beyond traditional EDR by integrating multiple security solutions (endpoint, network, email, identity, cloud, etc.) for unified detection and response.
    - Study the differences between XDR, EDR and SIEM. Understand where XDR fits in a SOC environment and how it complements other tools.
    - Explore common XDR features like telemetry aggregation, automated response actions, threat intelligence integration and AI/ML-based threat detection.
2. **Familiarise Yourself With XDR Platforms**
    - Get hands-on with leading XDR platforms like Palo Alto Cortex XDR, Microsoft 365 Defender, CrowdStrike Falcon, SentinelOne, Trend Micro Vision One and others.
    - Understand the specific capabilities and limitations of each platform.
    - Practice setting up, configuring and fine-tuning these platforms to get comfortable with their dashboards, data collection, detection rules and response mechanisms.
3. **Learn Threat Detection And Response Techniques**
    - **Detection**
      Study how XDR leverages machine learning and behavioural analytics to detect threats. Learn how to create and fine-tune detection rules.
    - **Response**
      Understand the automated and manual response capabilities, such as isolating infected systems, terminating malicious processes and blocking IOCs (Indicators of Compromise).
    - Study common attack tactics, techniques and procedures (TTPs) based on MITRE ATT&CK framework and how XDR solutions map and detect them.
4. **Integrate And Correlate Telemetry**
    - Master the skill of integrating various data sources (endpoint, network, email, cloud) within the XDR platform.
    - Learn how to correlate data across these sources to detect advanced and hidden threats.

- Understand how to leverage APIs and connectors to bring in telemetry from third-party tools for better visibility and comprehensive detection.

5. **Develop Advanced Analytical Skills**
    - Practice analysing logs, alerts and telemetry data from multiple sources to identify threats and perform root cause analysis.
    - Learn to create custom detection logic based on specific use cases or threats relevant to your environment.
    - Engage in exercises such as threat hunting, creating attack scenarios and running simulations in a lab environment.
6. **Focus On Automation And Orchestration**
    - Study how XDR leverages Security Orchestration, Automation and Response (SOAR) capabilities to automate repetitive tasks and streamline incident response.
    - Understand the process of building playbooks for automated incident response and alert triage.
    - Get familiar with scripting languages like Python or PowerShell, which are often used to automate tasks within the XDR platform.
7. **Stay Updated On Threat Intelligence And Threat Hunting**
    - Learn how to integrate and leverage threat intelligence feeds within the XDR platform for proactive defence.
    - Regularly practice threat hunting exercises, using XDR's advanced search and query capabilities to find potential threats that have evaded automated detection.
8. **Practice In A Lab Environment**
    - Set up a lab environment using tools like VMware or VirtualBox and install an XDR platform (some vendors provide trial versions).
    - Simulate various attacks (e.g., malware, lateral movement, data exfiltration) to practice detection, response and investigation.
    - Continuously create new attack scenarios to enhance your detection and response capabilities.
9. **Participate In Training and Community**
    - Attend official training and webinars provided by XDR vendors to gain insights and tips on leveraging their platforms.

- Engage with the cybersecurity community, such as attending XDR-focused conferences or participating in forums, to stay updated with the latest trends and best practices.

10. Engage In Continuous Learning

- Keep up with the latest developments in the XDR field, such as new capabilities, updates and emerging threats.
- Follow cybersecurity news, blogs and whitepapers focusing on XDR solutions and evolving detection and response strategies.
- Practice regularly with real-world threat scenarios to build expertise and confidence in handling complex incidents.

COMBINING XDR AND SIEM

1. XDR Vs SIEM

- **SIEM**
  A SIEM platform collects, aggregates, normalises and analyses logs and events from a wide range of sources across an organisation's IT infrastructure. It provides centralised log management, correlation rules, dashboards, compliance reporting and alerting for security incidents. However, SIEMs can generate a high volume of alerts, often leading to "alert fatigue."
- **XDR**
  XDR takes a more integrated approach by consolidating multiple security solutions (endpoint, network, email, cloud, identity, etc.) into a single platform. It offers deeper visibility, detection and response capabilities across these domains using advanced analytics, machine learning and automation. XDR aims to reduce complexity, provide context-rich insights and enable faster response times.

2. Enhanced Visibility and Threat Detection

- SIEM provides a wide view of the organisation's environment by aggregating logs from various sources like firewalls, servers, applications and network devices. XDR enhances this by providing deep visibility into specific domains (e.g., endpoint, network, email).
- While SIEMs use correlation rules to detect threats, XDR employs advanced analytics, machine learning and behavioural analysis to detect sophisticated threats. Integrating the two allows you to leverage both methods for comprehensive threat detection.

3. Advanced Correlation and Contextual Insights

- XDR integrates natively with specific security solutions, while SIEM correlates data from any source. Together, they enable advanced correlation by using SIEM's broad data sources and XDR's contextual insights to detect complex, multi-stage attacks.
- XDR provides enriched and contextualised alerts, reducing the noise and providing actionable information. When integrated with SIEM, these alerts are supplemented with additional context from other data sources, enabling better investigation and triage.

4. **Streamlined Incident Investigation and Response**
    - Combining XDR and SIEM provides a centralised platform for analysts to investigate incidents. SIEM helps in building the initial narrative by correlating various logs, while XDR provides deeper forensic data and root cause analysis.
    - XDR platforms often have built-in automated response capabilities (like isolating hosts, killing processes, blocking IPs). When integrated with SIEM, automated playbooks can trigger orchestrated responses across both SIEM-managed and XDR-managed environments, streamlining the incident response process.
5. **Improved Operational Efficiency and Reduced Alert Fatigue**
    - XDR's ability to provide high-fidelity alerts and reduce false positives helps in reducing alert fatigue for SOC analysts. When integrated with SIEM, it can filter out unnecessary alerts, focusing only on high-priority incidents.
    - Combining XDR's response automation capabilities with SIEM's orchestration capabilities through Security Orchestration, Automation and Response (SOAR) can automate repetitive tasks and streamline workflows.
6. **Enhanced Threat Hunting and Proactive Defence**
    - SIEM provides a broad data lake for threat hunting across various data sources, while XDR offers advanced search and hunting capabilities specific to endpoint, network and other domains. Together, they provide a more comprehensive threat-hunting capability.
    - Both SIEM and XDR can consume threat intelligence feeds. Combining them allows for proactive defence measures, such as automated blocking of IOCs (Indicators of Compromise) across all integrated security controls.

EXAMPLES AND SIMULATIONS

SCENARIO 1: MULTIPLE FAILED LOGIN ATTEMPTS

A series of suspicious activities have been detected by the XDR platform and forwarded to the SIEM. These activities include anomalous login attempts, privilege escalation and data exfiltration. The SIEM correlates these activities and raises multiple alerts.

Alerts in SIEM from XDR

1. **Alert 1: Suspicious Anomalous Login Detected**
2. **Alert 2: Privilege Escalation Detected on Critical Server**
3. **Alert 3: Potential Data Exfiltration Detected via Suspicious Network Activity**

1. Alert 1: Suspicious Anomalous Login Detected

Description:
The XDR detected multiple failed login attempts followed by a successful login from an unusual location. This behaviour suggests potential credential stuffing or brute force attack.

SIEM Alert Details:

- **Source:** XDR Platform (Palo Alto Cortex XDR)
- **Severity:** High
- **Event Count:** 150 failed attempts followed by 1 successful login
- **User:** Izzmier
- **Source IP:** 203.0.113.45 (Unusual location - Russia)
- **Target System:** VPN Gateway (vpn.acme.com)
- **Timestamp:** 2024-08-30 10:30:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:30:00Z",

"source": "XDR",

"event_type": "anomalous_login",

"severity": "high",

"user": "Izzmier",

"source_ip": "203.0.113.45",

"location": "Russia",

"target_system": "vpn.acme.com",

"failed_attempts": 150,

"successful_attempt": true,

"message": "Multiple failed login attempts followed by a successful login from an unusual location."

}

2. Alert 2: Privilege Escalation Detected on Critical Server

Description:
The XDR detected a suspicious privilege escalation event on a critical database server after an unusual login. This may indicate a compromised account attempting to gain higher privileges.

SIEM Alert Details:

- **Source:** XDR Platform (Palo Alto Cortex XDR)
- **Severity:** Critical
- **Event Count:** 1
- **User:** Izzmier
- **Source IP:** 203.0.113.45
- **Target System:** DBServer01 (database.acme.com)
- **Action:** Privilege Escalation (to Domain Admin)
- **Timestamp:** 2024-08-30 10:35:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:35:00Z",

"source": "XDR",

"event_type": "privilege_escalation",

"severity": "critical",

"user": "Izzmier",

"source_ip": "203.0.113.45",

"target_system": "DBServer01",

"privilege_granted": "Domain Admin",

"message": "Privilege escalation detected on DBServer01 for user Izzmier from IP 203.0.113.45."

}

3. Alert 3: Potential Data Exfiltration Detected via Suspicious Network Activity

Description:
Following the privilege escalation, the XDR detected a large volume of data being transferred from the critical server to an external IP address. This indicates potential data exfiltration.

SIEM Alert Details:

- **Source:** XDR Platform (Palo Alto Cortex XDR)
- **Severity:** Critical
- **Event Count:** 1
- **User:** Izzmier
- **Source IP:** 203.0.113.45
- **Target System:** DBServer01 (database.acme.com)
- **External IP:** 192.0.2.50
- **Data Transferred:** 5 GB
- **Protocol:** FTP
- **Timestamp:** 2024-08-30 10:45:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:45:00Z",

"source": "XDR",

"event_type": "data_exfiltration",

"severity": "critical",

"user": "Izzmier",

"source_ip": "203.0.113.45",

"target_system": "DBServer01",

"external_ip": "192.0.2.50",

"data_transferred": "5GB",

"protocol": "FTP",

"message": "Potential data exfiltration detected from DBServer01 to external IP 192.0.2.50 using FTP."

}

Analysis

Step 1: Review Alerts and Correlate Events

- Start by reviewing the three alerts generated in the SIEM from the XDR platform.
- Correlate the events to identify a pattern:
    - **Alert 1** indicates a possible credential compromise due to unusual login behaviour.
    - **Alert 2** shows that the compromised user account, Izzmier, gained elevated privileges.
    - **Alert 3** suggests potential data exfiltration from a critical server, likely using the elevated privileges.

Step 2: Investigate the Anomalous Login (Alert 1)

- **Analysis of Logs:** The logs indicate 150 failed login attempts followed by a successful one from a location (Russia) that is not associated with Izzmier's usual login locations.
- **Action Required:**
    - Confirm with Izzmier whether they were attempting to access the VPN at the time.
    - If not, assume the credentials have been compromised.
    - Check for other users or IPs exhibiting similar patterns.

Step 3: Analyse the Privilege Escalation Event (Alert 2)

- **Analysis of Logs:** The logs show that shortly after the unusual login, the account escalated privileges to a Domain Admin on DBServer01.
- **Action Required:**

- Check the server logs to determine what commands or actions were performed after the privilege escalation.
- Verify the legitimacy of the escalation by contacting relevant personnel or by checking Active Directory logs.
- Look for additional signs of lateral movement or reconnaissance.

Step 4: Examine Potential Data Exfiltration (Alert 3)

- **Analysis of Logs:** The logs show that after escalating privileges, a large amount of data (5 GB) was transferred to an external IP (192.0.2.50) via FTP.
- **Action Required:**
  - Analyse the network traffic logs and firewall logs to confirm the data transfer details.
  - Check if the external IP is associated with any known threat actors or if it is part of a blacklisted network.
  - Quarantine the affected system DBServer01 to prevent further data loss.

Step 5: Conduct a Root Cause Analysis

- Determine how Izzmier's credentials were compromised in the first place. This could involve checking for phishing emails, malware infections or other attack vectors.
- Investigate if there were any vulnerabilities or misconfigurations in the VPN, Active Directory or other systems that allowed for the successful escalation of privileges.

Step 6: Remediation Steps

1. **Containment:**
   - Isolate the affected user account and systems (e.g., DBServer01).
   - Revoke the escalated privileges granted to Izzmier.
   - Block the suspicious external IP (192.0.2.50) at the firewall.
2. **Eradication:**
   - Reset Izzmier's credentials and enforce MFA (Multi-Factor Authentication) for all accounts.
   - Patch any vulnerabilities or misconfigurations that may have contributed to the incident.

3. **Recovery:**
    - Restore the affected server (DBServer01) from a known good backup.
    - Monitor the environment closely for any signs of recurring or related threats.
4. **Lessons Learned:**
    - Conduct a post-incident review to analyse gaps in detection and response.
    - Update detection rules in both XDR and SIEM to better detect similar activities in the future.
    - Consider user behaviour analytics (UBA) to better detect unusual login patterns.

Step 7: Report Findings

- Document the incident details, analysis steps, actions taken and lessons learned.
- Prepare a report for management that includes an executive summary, impact analysis and recommendations for improving security posture.

SCENARIO 2: ATTEMPTED DATA EXFILTRATION

The XDR system has identified a series of suspicious activities indicating a possible malware infection spreading laterally within the network. The SIEM correlates these events, raising multiple alerts.

Alerts in SIEM from XDR

1. **Alert 1: Malware Execution Detected on Multiple Endpoints**
2. **Alert 2: Lateral Movement Detected via SMB Protocol**
3. **Alert 3: Attempted Data Exfiltration to an Unknown Cloud Service**

1. Alert 1: Malware Execution Detected on Multiple Endpoints

Description:
The XDR detected malicious files executed on multiple endpoints. The malware exhibits ransomware-like behaviour, including encrypting files and generating ransom notes.

SIEM Alert Details:

- **Source:** XDR Platform (Microsoft Defender for Endpoint)
- **Severity:** Critical
- **Event Count:** 3 (Multiple endpoints affected)
- **Hostnames Affected:** WS01, WS05, WS07
- **Malware Name:** Ransomware.Sample.Gen
- **File Path:** C:\Users\Public\malicious.exe
- **Action Taken:** Quarantine initiated
- **Timestamp:** 2024-08-30 09:15:00

Log Entry in SIEM:


```
{
 "timestamp": "30-08-2024T09:15:00Z",
 "source": "XDR",
 "event_type": "malware_execution",
 "severity": "critical",
 "hosts_affected": ["WS01", "WS05", "WS07"],
 "malware_name": "Ransomware.Sample.Gen",
```

"file_path": "C:\\Users\\Public\\malicious.exe",

"action_taken": "quarantine",

"message": "Malware execution detected on multiple endpoints. Ransomware-like behaviour identified."

}

2. Alert 2: Lateral Movement Detected via SMB Protocol

Description:
The XDR detected lateral movement attempts using SMB protocol, where the compromised endpoints tried to access administrative shares on other machines.

SIEM Alert Details:

- **Source:** XDR Platform (Microsoft Defender for Endpoint)
- **Severity:** High
- **Event Count:** 10 (Across multiple hosts)
- **Source Host:** WS01
- **Target Hosts:** WS02, WS03, WS06
- **Protocol:** SMB (Server Message Block)
- **Action:** Blocked
- **Timestamp:** 2024-08-30 09:30:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T09:30:00Z",

"source": "XDR",

"event_type": "lateral_movement",

"severity": "high",

"source_host": "WS01",

"target_hosts": ["WS02", "WS03", "WS06"],

"protocol": "SMB",

"action": "blocked",

"message": "Lateral movement detected via SMB protocol from WS01 to WS02, WS03 and WS06."

}

3. Alert 3: Attempted Data Exfiltration to an Unknown Cloud Service

Description:
The XDR detected a large amount of data being uploaded to an unknown cloud service provider from one of the compromised machines. This indicates a potential data exfiltration attempt.

SIEM Alert Details:

- **Source:** XDR Platform (Microsoft Defender for Endpoint)
- **Severity:** Critical
- **Event Count:** 1
- **Host:** WS05
- **Destination IP:** 198.51.100.25 (Unknown Cloud Service)
- **Data Transferred:** 4.2 GB
- **Protocol:** HTTPS
- **Action:** Blocked
- **Timestamp:** 2024-08-30 09:45:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T09:45:00Z",

"source": "XDR",

"event_type": "data_exfiltration_attempt",

"severity": "critical",

"host": "WS05",

"destination_ip": "198.51.100.25",

"data_transferred": "4.2GB",

"protocol": "HTTPS",

"action": "blocked",

"message": "Attempted data exfiltration to an unknown cloud service from WS05 using HTTPS protocol."

}

Analysis

Step 1: Review Alerts and Correlate Events

- Begin by reviewing the alerts generated in the SIEM from the XDR platform.
- Correlate the alerts to understand the full scope of the attack:
    - **Alert 1** indicates that a malware, likely ransomware, has been executed on multiple endpoints.
    - **Alert 2** shows that the ransomware is attempting to spread laterally across the network using SMB protocol.
    - **Alert 3** suggests an attempted data exfiltration to an unknown cloud service, possibly to monetise stolen data.

Step 2: Investigate Malware Execution (Alert 1)

- **Analysis of Logs:** The logs indicate that a ransomware sample was executed on three endpoints (WS01, WS05, WS07), leading to the encryption of files.
- **Action Required:**
    - Isolate the affected endpoints to prevent further spread.
    - Review the XDR telemetry to determine how the malware was delivered (e.g., email attachment, malicious link).
    - Check endpoint logs for processes spawned by malicious.exe to see if there are any additional indicators of compromise (IOCs).

Step 3: Analyse Lateral Movement Attempts (Alert 2)

- **Analysis of Logs:** The compromised endpoint WS01 attempted to move laterally to WS02, WS03 and WS06 using the SMB protocol.
- **Action Required:**
    - Review network traffic logs and endpoint logs for these lateral movement attempts.
    - Verify whether the attempts were successful or blocked.
    - Identify any further attempts or suspicious behaviour from WS02, WS03 and WS06.

- Apply network segmentation and update firewall rules to restrict SMB traffic.

Step 4: Examine Data Exfiltration Attempt (Alert 3)

- **Analysis of Logs:** The compromised machine WS05 attempted to upload a large amount of data (4.2 GB) to an unknown cloud service.
- **Action Required:**
  - Identify the content of the data that was attempted to be exfiltrated by checking WS05 logs and memory dumps.
  - Verify if there were any DNS queries or HTTPS sessions related to 198.51.100.25 before the exfiltration attempt.
  - Block the IP 198.51.100.25 at the firewall and monitor for any further connections to unknown cloud services.

Step 5: Conduct a Root Cause Analysis

- Investigate how the malware initially entered the network. Was it through phishing, a drive-by download or another vector?
- Identify any vulnerable software or misconfigurations that could have facilitated the lateral movement.

Step 6: Remediation Steps

1. **Containment:**
   - Isolate affected endpoints (WS01, WS05, WS07).
   - Block external connections to unknown or suspicious IPs like 198.51.100.25.
   - Apply segmentation and restrict SMB traffic between different segments.
2. **Eradication:**
   - Remove malware from infected machines and restore from known good backups.
   - Apply patches to fix any exploited vulnerabilities and update anti-malware definitions.
3. **Recovery:**
   - Monitor the environment closely for signs of re-infection or residual malware.

- Gradually bring isolated systems back online with heightened monitoring.

4. **Lessons Learned:**
    - Conduct a post-incident review to understand what went well and what needs improvement.
    - Strengthen email filtering and user awareness training to prevent malware delivery.
    - Improve detection rules for ransomware-like behaviour and lateral movement attempts.

Step 7: Report Findings

- Document the entire incident, from initial detection to remediation, in a detailed report.
- Provide an executive summary for management with key takeaways and recommendations to prevent similar incidents in the future.

SCENARIO 3: PRIVILEGE ESCALATION ATTEMPT

A user account has been compromised and the attacker is attempting to move laterally within the network using Remote Desktop Protocol (RDP) and escalate privileges to gain control over critical systems.

Alerts in SIEM from XDR

1. **Alert 1: Suspicious PowerShell Command Execution Detected**
2. **Alert 2: Unauthorised Remote Desktop Protocol (RDP) Access Attempt**
3. **Alert 3: Privilege Escalation Attempt Detected on Domain Controller**

1. Alert 1: Suspicious PowerShell Command Execution Detected

Description:
The XDR detected suspicious PowerShell commands executed on a user's workstation, indicating a possible credential harvesting attempt.

SIEM Alert Details:

- **Source:** XDR Platform (Palo Alto Cortex XDR)
- **Severity:** High
- **Event Count:** 5 (Multiple commands executed)
- **Host:** WS03
- **User Account:** user.izzmier
- **Command Executed:** Invoke-Mimikatz.ps1
- **Action Taken:** Blocked
- **Timestamp:** 2024-08-30 10:15:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:15:00Z",

"source": "XDR",

"event_type": "suspicious_powershell_execution",

"severity": "high",

"host": "WS03",

"user_account": "user.izzmier",

"command_executed": "Invoke-Mimikatz.ps1",

"action_taken": "blocked",

"message": "Suspicious PowerShell command execution detected on WS03 by user.izzmier. Possible credential harvesting attempt using Mimikatz."

}

2. Alert 2: Unauthorised Remote Desktop Protocol (RDP) Access Attempt

Description:
The XDR detected unauthorised RDP access attempts to several systems within the network. These attempts were traced back to a compromised user account.

SIEM Alert Details:

- **Source:** XDR Platform (Palo Alto Cortex XDR)
- **Severity:** Critical
- **Event Count:** 3
- **Source Host:** WS03
- **Target Hosts:** SRV01, SRV02, SRV03
- **Protocol:** RDP (Remote Desktop Protocol)
- **User Account:** user.izzmier
- **Action:** Blocked
- **Timestamp:** 2024-08-30 10:30:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:30:00Z",

"source": "XDR",

"event_type": "unauthorised_rdp_access_attempt",

"severity": "critical",

"source_host": "WS03",

"target_hosts": ["SRV01", "SRV02", "SRV03"],

"protocol": "RDP",

"user_account": "user.izzmier",

"action": "blocked",

"message": "Unauthorised RDP access attempts detected from WS03 to SRV01, SRV02 and SRV03 using compromised account user.izzmier."

}

3. Alert 3: Privilege Escalation Attempt Detected on Domain Controller

Description:
The XDR identified an attempted privilege escalation on a domain controller (DC01). The attacker used a compromised user account to try to add a user to the "Domain Admins" group.

SIEM Alert Details:

- **Source:** XDR Platform (Palo Alto Cortex XDR)
- **Severity:** Critical
- **Event Count:** 1
- **Host:** DC01
- **User Account:** user.izzmier
- **Attempted Action:** Add user attacker.account to "Domain Admins"
- **Action Taken:** Blocked
- **Timestamp:** 2024-08-30 10:45:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:45:00Z",

"source": "XDR",

"event_type": "privilege_escalation_attempt",

"severity": "critical",

"host": "DC01",

"user_account": "user.izzmier",

"attempted_action": "Add user attacker.account to Domain Admins",

"action_taken": "blocked",

"message": "Privilege escalation attempt detected on DC01 by user.izzmier trying to add attacker.account to Domain Admins."

}

Analysis

Step 1: Review Alerts and Correlate Events

- Start by reviewing the alerts generated in the SIEM from the XDR platform.
- Correlate these alerts to determine the full scope of the attack:
    - **Alert 1** shows a suspicious PowerShell command execution, indicating potential credential theft using Mimikatz.
    - **Alert 2** indicates lateral movement attempts using RDP with the compromised account.
    - **Alert 3** reveals a privilege escalation attempt on a domain controller using the same compromised account.

Step 2: Investigate Suspicious PowerShell Execution (Alert 1)

- **Analysis of Logs:** The user account user.izzmier executed Invoke-Mimikatz.ps1 on WS03, suggesting credential harvesting.
- **Action Required:**
    - Confirm the legitimacy of the user user.izzmier and check for any unauthorised logins or access attempts.
    - Investigate how Invoke-Mimikatz.ps1 was executed. Was it through a script file, email attachment or a download from the internet?
    - Isolate WS03 and inspect the memory and system logs for evidence of credential dumping or other malware activity.

Step 3: Analyse Unauthorised RDP Access Attempts (Alert 2)

- **Analysis of Logs:** The attacker, using the compromised account user.izzmier, attempted to access multiple servers (SRV01, SRV02, SRV03) via RDP.
- **Action Required:**
    - Review network traffic and endpoint logs for these RDP access attempts.
    - Verify if any of these attempts were successful or if additional suspicious activity was noticed from the target servers.

- Disable RDP access for non-administrative accounts and implement multi-factor authentication (MFA) for administrative access.

Step 4: Examine Privilege Escalation Attempt on Domain Controller (Alert 3)

- **Analysis of Logs:** An attempted privilege escalation on DC01 was detected, where user.izzmier tried to add attacker.account to the "Domain Admins" group.
- **Action Required:**
  - Investigate the Domain Controller logs for further details on the privilege escalation attempt.
  - Ensure that attacker.account has been blocked or deleted and confirm the integrity of the domain controllers.
  - Conduct a review of the "Domain Admins" group and reset credentials for all accounts to avoid any unauthorised access.

Step 5: Conduct a Root Cause Analysis

- Investigate how the initial compromise occurred. Was it through phishing, an infected attachment or malicious websites?
- Identify if there were any vulnerabilities or misconfigurations that allowed for the credential theft and attempted lateral movement.

Step 6: Remediation Steps

1. **Containment:**
   - Isolate affected endpoints (WS03, SRV01, SRV02, SRV03) and the domain controller (DC01).
   - Block RDP access for non-authorised accounts across the network.
   - Change credentials for all users, especially user.izzmier and enforce stronger password policies.
2. **Eradication:**
   - Remove any malicious scripts or tools like Mimikatz found on affected systems.
   - Review and patch any known vulnerabilities or misconfigurations that allowed the attack vector.
3. **Recovery:**
   - Monitor the environment for re-infection or further signs of compromise.

- Re-enable RDP access only for authorised and trusted users and services with enhanced monitoring.

4. **Lessons Learned:**
    - Conduct a thorough incident review to determine improvements in detection, response and prevention capabilities.
    - Implement endpoint detection and response (EDR) policies that trigger alerts for unusual PowerShell and RDP activities.
    - Increase user awareness training on phishing and credential protection.

Step 7: Report Findings

- Document the incident, analysis, actions taken and recommendations in a detailed report.
- Provide a summary to management highlighting key points, such as the detection of credential theft, lateral movement and privilege escalation attempts.

SCENARIO 4: C2 CONNECTION ATTEMPT

A compromised third-party software application has been used to deploy a malicious payload within the organisation's network, resulting in data exfiltration attempts and attempts to establish a Command and Control (C2) connection.

Alerts in SIEM from XDR

1. **Alert 1: Suspicious Application Behaviour Detected**
2. **Alert 2: Outbound DNS Requests to Malicious Domains**
3. **Alert 3: Command and Control (C2) Connection Attempt Detected**

1. Alert 1: Suspicious Application Behaviour Detected

Description:
The XDR platform detected unusual behaviour from a trusted third-party software application (trusted_app.exe) installed on several workstations. The software attempted to execute scripts and make unexpected network connections.

SIEM Alert Details:

- **Source:** XDR Platform (Microsoft Defender for Endpoint)
- **Severity:** High
- **Event Count:** 12
- **Affected Hosts:** WS05, WS06, WS07
- **User Account:** Various users
- **Process Name:** trusted_app.exe
- **Unusual Behaviour:** Attempt to execute PowerShell script malicious_script.ps1
- **Action Taken:** Quarantined
- **Timestamp:** 2024-08-30 09:45:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T09:45:00Z",

"source": "XDR",

"event_type": "suspicious_application_behaviour",

"severity": "high",

"affected_hosts": ["WS05", "WS06", "WS07"],

"user_account": "various_users",

"process_name": "trusted_app.exe",

"unusual_behaviour": "Attempt to execute PowerShell script malicious_script.ps1",

"action_taken": "quarantined",

"message": "Suspicious behaviour detected from trusted third-party application 'trusted_app.exe' attempting to execute PowerShell script 'malicious_script.ps1' on multiple hosts."

}

2. Alert 2: Outbound DNS Requests to Malicious Domains

Description:
Following the suspicious behaviour alert, the XDR detected multiple outbound DNS requests to domains known for hosting malicious content. These requests originated from the same endpoints where trusted_app.exe was running.

SIEM Alert Details:

- **Source:** XDR Platform (Microsoft Defender for Endpoint)
- **Severity:** High
- **Event Count:** 8
- **Affected Hosts:** WS05, WS06, WS07
- **DNS Queries:** malicious-domain[.]com, c2-malware[.]net
- **Action Taken:** Blocked
- **Timestamp:** 2024-08-30 10:00:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:00:00Z",

"source": "XDR",

"event_type": "outbound_dns_request_to_malicious_domain",

"severity": "high",

"affected_hosts": ["WS05", "WS06", "WS07"],

"dns_queries": ["malicious-domain.com", "c2-malware.net"],

"action_taken": "blocked",

"message": "Multiple outbound DNS requests detected to known malicious domains 'malicious-domain.com' and 'c2-malware.net' from WS05, WS06 and WS07."

}

3. Alert 3: Command and Control (C2) Connection Attempt Detected

Description:
The XDR identified a C2 connection attempt from one of the affected workstations (WS07) to a known C2 server. The connection attempt was blocked, but this indicates that malware on the host attempted to communicate with an external threat actor.

SIEM Alert Details:

- **Source:** XDR Platform (Microsoft Defender for Endpoint)
- **Severity:** Critical
- **Event Count:** 1
- **Source Host:** WS07
- **Destination IP:** 192.168.10.101 (known C2 server)
- **Protocol:** HTTPS
- **Action Taken:** Blocked
- **Timestamp:** 2024-08-30 10:15:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T10:15:00Z",

"source": "XDR",

"event_type": "c2_connection_attempt_detected",

"severity": "critical",

"source_host": "WS07",

"destination_ip": "192.168.10.101",

"protocol": "HTTPS",

"action_taken": "blocked",

"message": "C2 connection attempt detected from WS07 to known C2 server IP 192.168.10.101 via HTTPS protocol."

}

Analysis

Step 1: Review Alerts and Correlate Events

- Review the alerts generated by the SIEM from XDR to understand the scope of the attack:
    - **Alert 1** shows that a trusted third-party application (trusted_app.exe) attempted to execute a PowerShell script (malicious_script.ps1), indicating it may have been compromised.
    - **Alert 2** reveals multiple outbound DNS requests to known malicious domains, suggesting an attempt to establish communication with external servers.
    - **Alert 3** indicates an actual C2 connection attempt from WS07 to a known C2 server, confirming that malware is attempting to communicate externally.

Step 2: Investigate Suspicious Application Behaviour (Alert 1)

- **Analysis of Logs:** Review the behaviour of the third-party software trusted_app.exe to understand how it was exploited.
    - Analyse the execution of malicious_script.ps1. Did it contain commands to download additional payloads, exfiltrate data or disable defences?
    - **Action Required:**
        - Isolate affected hosts (WS05, WS06, WS07) to prevent further spread of the potential infection.
        - Inspect the application's update logs to check if the malicious behaviour occurred after a recent update or a specific trigger.

Step 3: Analyse Outbound DNS Requests to Malicious Domains (Alert 2)

- **Analysis of Logs:** The DNS logs show that WS05, WS06 and WS07 attempted to resolve domains (malicious-domain.com and c2-malware.net) known for hosting malware.
    - Review network traffic to identify if any DNS requests were resolved or if any other malicious activities were initiated.
    - **Action Required:**

        - Block all outbound traffic to these domains at the firewall and monitor for any further attempts.
        - Use threat intelligence feeds to cross-check these domains and IPs for additional context on the attacker's infrastructure.

Step 4: Examine Command and Control (C2) Connection Attempt (Alert 3)

- **Analysis of Logs:** A C2 connection attempt was detected from WS07 to 192.168.10.101, a known malicious server.
    - Review the network logs and endpoint logs to understand the nature of the HTTPS connection attempt. Was any data exfiltrated or transferred?
    - **Action Required:**
        - Confirm that the attempted connection was blocked by reviewing firewall logs and XDR alerts.
        - Investigate the origin of the malware that attempted to initiate the C2 connection and its persistence mechanisms.

Step 5: Conduct a Root Cause Analysis

- Determine how trusted_app.exe was compromised. Was the software update server breached or was it a supply chain attack affecting the vendor?
- Assess if there are any other instances of the compromised application in the environment and inspect them for unusual behaviour.

Step 6: Remediation Steps

1. **Containment:**
    - Quarantine the affected endpoints (WS05, WS06, WS07).
    - Block the compromised third-party software's traffic and remove it from all endpoints.
    - Disable the software from auto-updating until the vendor provides a clean and verified version.
2. **Eradication:**
    - Remove all traces of the malicious_script.ps1 and any related malware components from the network.
    - Conduct a vulnerability assessment to identify potential weaknesses in third-party software usage.
3. **Recovery:**

- Reinstall or update the compromised software with a secure, validated version from the vendor.
- Monitor the network for any signs of re-infection or unusual behaviour.

4. **Lessons Learned:**
    - Conduct a post-incident review to identify how the organisation can improve its supply chain security posture.
    - Implement additional monitoring and alerting for third-party software behaviours and anomalies.

Step 7: Report Findings

- Document the entire incident, analysis, remediation steps and lessons learned.
- Provide a summary report to the management team and stakeholders, highlighting the risks of supply chain attacks and the steps taken to prevent future incidents.

SCENARIO 5: UNTRUSTED SSL CERTIFICATE

Unusual SSL/TLS certificate usage and a series of suspicious network behaviours indicate a possible MitM attack within the internal network, with evidence of an attacker intercepting traffic and using stolen credentials to access sensitive systems.

Alerts in SIEM from XDR

1. **Alert 1: Untrusted SSL Certificate Observed in Network Traffic**
2. **Alert 2: Abnormal Traffic Patterns to External IPs**
3. **Alert 3: Successful Login Using Stolen Credentials from a Suspicious IP Address**

1. Alert 1: Untrusted SSL Certificate Observed in Network Traffic

Description:
The XDR platform detects multiple instances where an untrusted SSL certificate was used to intercept HTTPS traffic between internal clients (10.10.5.20, 10.10.5.21) and an internal application server (10.10.8.5). This suggests potential MitM activity.

SIEM Alert Details:

- **Source:** XDR Platform (CrowdStrike Falcon)
- **Severity:** High
- **Event Count:** 15
- **Affected Hosts:** 10.10.5.20, 10.10.5.21
- **Destination Host:** 10.10.8.5
- **Certificate Fingerprint:** a5c9b2d5f8f7b7a1d3e9a5b7c8e6
- **Action Taken:** Detected (not blocked)
- **Timestamp:** 2024-08-30 11:30:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T11:30:00Z",

"source": "XDR",

"event_type": "untrusted_ssl_certificate_observed",

"severity": "high",

"affected_hosts": ["10.10.5.20", "10.10.5.21"],

"destination_host": "10.10.8.5",

"certificate_fingerprint": "a5c9b2d5f8f7b7a1d3e9a5b7c8e6",

"action_taken": "detected",

"message": "Untrusted SSL certificate observed in network traffic between internal clients 10.10.5.20, 10.10.5.21 and internal server 10.10.8.5. Potential MitM activity."

}

2. Alert 2: Abnormal Traffic Patterns to External IPs

Description:
Following the SSL certificate alert, the XDR identified unusual outbound traffic from one of the affected clients (10.10.5.21) to an external IP (185.203.125.50). The volume and pattern of the traffic resemble data exfiltration activities.

SIEM Alert Details:

- **Source:** XDR Platform (CrowdStrike Falcon)
- **Severity:** Critical
- **Event Count:** 6
- **Source Host:** 10.10.5.21
- **Destination IP:** 185.203.125.50 (unknown IP)
- **Traffic Volume:** 1.2 GB in 5 minutes
- **Protocol:** HTTPS
- **Action Taken:** Monitored (not blocked)
- **Timestamp:** 2024-08-30 11:45:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T11:45:00Z",

"source": "XDR",

"event_type": "abnormal_outbound_traffic_pattern",

"severity": "critical",

"source_host": "10.10.5.21",

"destination_ip": "185.203.125.50",

"traffic_volume": "1.2 GB",

"protocol": "HTTPS",

"action_taken": "monitored",

"message": "Abnormal outbound traffic pattern observed from 10.10.5.21 to external IP 185.203.125.50. Potential data exfiltration attempt."

}

3. Alert 3: Successful Login Using Stolen Credentials from a Suspicious IP Address

Description:
A login attempt was detected from a suspicious IP address (198.51.100.100) using credentials associated with an internal user (izzmier). The login was successful, indicating a potential compromise.

SIEM Alert Details:

- **Source:** XDR Platform (CrowdStrike Falcon)
- **Severity:** High
- **Event Count:** 1
- **User Account:** izzmier
- **Source IP:** 198.51.100.100 (unknown IP)
- **Destination System:** Cloud Management Console
- **Action Taken:** User account locked
- **Timestamp:** 2024-08-30 12:00:00

Log Entry in SIEM:

{

"timestamp": "30-08-2024T12:00:00Z",

"source": "XDR",

"event_type": "successful_login_using_stolen_credentials",

"severity": "high",

"user_account": "izzmier",

"source_ip": "198.51.100.100",

"destination_system": "Cloud Management Console",

"action_taken": "user account locked",

"message": "Successful login detected using stolen credentials from IP 198.51.100.100. User account 'izzmier' locked for security."

}

Analysis

Step 1: Review Alerts and Correlate Events

- Review the alerts generated by the SIEM from XDR to understand the potential MitM attack:
    - **Alert 1** indicates the presence of an untrusted SSL certificate between clients and an internal application server, suggesting potential MitM activity.
    - **Alert 2** reveals unusual outbound traffic to an unknown external IP, which may indicate data exfiltration.
    - **Alert 3** shows that credentials stolen through the MitM attack might have been used to access sensitive systems, confirmed by a successful login from a suspicious IP address.

Step 2: Investigate the Untrusted SSL Certificate Alert (Alert 1)

- **Analysis of Logs:** Review the SSL/TLS logs to examine the certificate details and the communication pattern.
    - Check the fingerprint (a5c9b2d5f8f7b7a1d3e9a5b7c8e6) and compare it with known certificates in the organisation's database.
    - **Action Required:**
        - Block or isolate traffic associated with this untrusted certificate.
        - Check if the internal network devices, like routers or switches, are compromised or misconfigured.

Step 3: Analyse the Abnormal Traffic Patterns to External IPs (Alert 2)

- **Analysis of Logs:** Review the network traffic logs to understand the volume and destination of the traffic.
    - Check the nature of the data being transmitted—are there patterns indicating the transfer of sensitive information?
    - **Action Required:**

        - Block the outbound connection to the external IP (185.203.125.50).
        - Capture and analyse packets to understand if sensitive data has been exfiltrated.

Step 4: Examine the Successful Login Using Stolen Credentials (Alert 3)

- **Analysis of Logs:** Analyse user activity logs for izzmier to identify unusual patterns, such as logins from unfamiliar IP addresses or outside of normal working hours.
    - **Action Required:**
        - Disable the izzmier account temporarily and initiate a password reset.
        - Review logs to determine if any unauthorised actions were performed in the Cloud Management Console.

Step 5: Conduct a Root Cause Analysis

- Determine how the attacker gained access to the network to perform the MitM attack.
- Inspect the internal network for any rogue devices or misconfigured network settings.
- Analyse any indications of phishing or social engineering used to compromise internal accounts.

Step 6: Remediation Steps

1. **Containment:**
    - Isolate affected endpoints and prevent further communication with suspicious IPs.
    - Revoke any untrusted SSL certificates used for internal communications.
2. **Eradication:**
    - Remove any unauthorised devices or rogue access points in the network.
    - Conduct a full scan of the network to detect any other compromised systems or unauthorised changes.
3. **Recovery:**
    - Reinstate user accounts with stronger authentication mechanisms, such as multi-factor authentication (MFA).

    - Monitor network traffic for any additional MitM signs or anomalies.

4. **Lessons Learned:**
    - Implement tighter controls on network traffic inspection and SSL certificate validation.
    - Conduct regular security awareness training to help employees recognise potential phishing attacks.

Step 7: Report Findings

- Document the entire incident, including the detection, analysis and remediation steps taken.
- Provide a summary report to management and stakeholders, highlighting the importance of secure network configurations and the need for robust authentication methods.