THREAT HUNTING PLAYBOOKS FOR MITRE TACTICS

Starting your first threat hunting

ABSTRACT

This document will help and guide you to start your first threat hunting based on MITRE ATT&CK Tactics.

PRASANNAKUMAR B MUNDAS

Reconnaissance

Objective:

Identify potential reconnaissance activity on the network

Description:

Reconnaissance is an important phase of an attack, where the attacker gathers information about the target system and network. This playbook aims to identify potential reconnaissance activity by analyzing Windows logs.

Assumptions:

The organization has a centralized logging system in place that captures Windows logs.

Playbook Steps:

1. Gather and Review Windows Logs
    - Identify the relevant log sources to be analyzed for reconnaissance activity (e.g., event logs, sysmon logs, etc.).
    - Collect and review the logs for the past 30 days or more, depending on the organization's retention policy.

2. Identify Potential Indicators of Reconnaissance Activity
    - Look for unusual activity such as spikes in network traffic, failed login attempts, and unusual access patterns.
    - Use the following Windows log sources and events to identify potential indicators of reconnaissance activity:
        - Security Event Log: - Event ID 4624: Successful logon events - Event ID 4625: Failed logon events - Event ID 4634: Successful logoff events - Event ID 4647: User initiated logoff events
        - Sysmon: - Event ID 1: Process creation events - Event ID 3: Network connection events - Event ID 7: Image load events - Event ID 8: CreateRemoteThread events

3. Analyze the Indicators of Reconnaissance Activity
    - Review the logs for each indicator of reconnaissance activity.
    - Identify any patterns or anomalies that could indicate potential reconnaissance activity.
    - Use additional tools and techniques, such as network traffic analysis, to further investigate any suspicious activity.

4. Determine the Scope and Impact of the Activity
    - Identify the scope and impact of the reconnaissance activity by analyzing the logs and any other available information.

- Determine whether the activity is a legitimate or malicious activity.
- Identify any affected systems, users, or data.

5. Remediate and Mitigate
    - Take appropriate remediation and mitigation actions based on the scope and impact of the reconnaissance activity.
    - Develop and implement a plan to prevent similar reconnaissance activity from occurring in the future.

6. Document and Report
    - Document the findings, actions taken, and any recommendations for future improvements.
    - Report the findings and recommendations to the appropriate stakeholders, such as the incident response team and management.

The Reconnaissance Threat Hunting playbook aims to identify potential reconnaissance activity on the network by analyzing Windows logs. By following this playbook, organizations can detect and respond to reconnaissance activity in a timely manner, preventing further malicious activity on the network.

Developing Resources

Hypothesis:

Attackers are developing resources for the next stage of the attack.

Objective:

To identify suspicious activity related to the development of resources in the network.

> Note: This playbook assumes that the organization has a baseline of normal network behavior and activity.

1. Data Sources
    - Endpoint logs (e.g. Sysmon, Windows Event Logs)
    - Network logs (e.g. NetFlow, Firewall logs)

2. Initial Triage
    - Identify all hosts that have been communicating with known malicious IPs or domains.
    - Look for any unusual or suspicious domain name requests.
    - Check for any unusual or suspicious HTTP requests.
    - Look for any unusual or suspicious DNS requests.

3. Threat Hunting Techniques
    - Look for any unusual process or service creations.
    - Look for any unusual or suspicious registry key modifications.
    - Look for any unusual or suspicious file creations, modifications, or deletions.
    - Look for any unusual or suspicious network connections or traffic.
    - Look for any unusual or suspicious command-line arguments.

4. Indicators of Compromise (IOCs)
    - Malicious IP addresses or domains.
    - Unusual or suspicious process names.
    - Unusual or suspicious registry key names or values.
    - Unusual or suspicious file names, paths, or extensions.
    - Unusual or suspicious network ports or protocols.

5. Recommended Actions
    - Isolate any infected hosts from the network.
    - Collect any relevant forensic evidence.
    - Analyze any suspicious files, processes, or network traffic.
    - Block or blackhole any malicious IPs or domains.
    - Patch or update any vulnerable software or systems.

- Increase monitoring and detection capabilities for future attacks.

Note: This playbook is intended as a general guide and should be customized based on the specific needs and environment of the organization. It is important to have a well-defined incident response plan in place and to involve all relevant stakeholders in the threat hunting and response process.

Initial Access

Hypothesis:

Adversaries are using phishing emails to gain initial access to the network.

Objective:

To detect any suspicious or malicious activity related to phishing emails and to prevent any unauthorized access.

Playbook:

1. Identify relevant logs:
    - Email logs: Microsoft Exchange, Office 365, G Suite, etc.
    - Web proxy logs: Microsoft Forefront, Palo Alto Networks, etc.
    - Network traffic logs: Wireshark, Bro/Zeek, etc.
    - Endpoint logs: Windows event logs, Sysmon logs, etc.

2. Look for indicators of phishing emails:
    - Check for emails sent from suspicious or unknown domains.
    - Look for emails with unusual or suspicious subject lines and body content.
    - Check for emails sent from external sources, especially those not typically associated with business communication.
    - Look for emails with attachments that are uncommon or unexpected, such as .zip, .exe, or .dll files.
    - Check for emails with hyperlinks that lead to unknown or suspicious websites.

3. Check for suspicious activity on endpoints:
    - Look for signs of credential harvesting, such as keylogging or password stealing.
    - Check for unusual or unauthorized logins, such as logins from unknown or suspicious IP addresses.

- Check for the presence of suspicious files or applications, such as those related to remote access or command and control (C2) activity.

4. Analyze network traffic:
    - Look for signs of network reconnaissance, such as port scanning or ping sweeps.
    - Check for unusual or unauthorized network connections, such as connections to known C2 servers.
    - Look for signs of lateral movement, such as connections between internal systems that are not typically seen.

5. Remediate any threats found:
    - Quarantine or delete suspicious emails, attachments, or files.
    - Block or restrict access to known malicious IP addresses and domains.
    - Disable or remove any suspicious or unauthorized user accounts.
    - Ensure that all endpoints and systems are fully patched and updated.

6. Review and refine:
    - Document all findings and actions taken.
    - Review the playbook regularly to ensure it is up-to-date and effective.
    - Continuously monitor logs and network activity to detect and respond to new threats.

By following this Threat Hunting playbook for the Initial Access hypothesis, you can proactively detect and respond to phishing attacks before they can do significant harm to your organization.

Execution

Objective:

To proactively search for and identify potential malicious executions or attempted executions on endpoints, servers, and network devices.

Hypothesis:

Adversaries have gained access to the network and are attempting to execute malicious code on endpoints or servers.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.
    - Gather data: Collect and analyze the following data sources to identify potential malicious executions:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Anti-virus logs and reports

2. Develop queries: Develop and run queries across the collected data sources to identify any suspicious executions. Queries may include:
    - Any attempts to execute files from suspicious locations
    - Any unauthorized executions of specific file types (e.g., .exe, .bat)
    - Any executions with suspicious command-line arguments or parameters
    - Any executions of known malicious files or hashes

3. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Unusual file paths or locations
    - Suspicious file names or extensions
    - Known malware file hashes
    - Any anomalous command-line parameters or arguments

4. Take action: Once potential IOCs have been identified, take the following actions:
    - Quarantine any suspicious files or systems
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

5. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential malicious executions and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Persistence

Objective:

To proactively search for and identify potential persistence mechanisms that adversaries may use to maintain access to endpoints, servers, and network devices.

Hypothesis:

Adversaries have established persistence mechanisms on endpoints, servers, or network devices to maintain access and control over the environment.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential persistence mechanisms:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Anti-virus logs and reports

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to persistence. Queries may include:
    - Any new scheduled tasks or services created
    - Any registry changes related to persistence
    - Any changes to autorun entries or startup folders
    - Any changes to system files or directories that are commonly used for persistence

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:

- New scheduled tasks or services that are not associated with known applications or services
- Suspicious registry keys or values
- Changes to autorun entries or startup folders that are not authorized or expected
- Any modifications to system files or directories that could indicate tampering

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Remove any suspicious persistence mechanisms
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential persistence mechanisms and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Privilege escalation

Objective:

To proactively search for and identify potential privilege escalation attempts by adversaries on endpoints, servers, and network devices.

Hypothesis:

Adversaries have gained access to a system and are attempting to escalate their privileges to gain greater control over the environment.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential privilege escalation attempts:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Anti-virus logs and reports

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to privilege escalation. Queries may include:
    - Any changes to user accounts or group membership
    - Any attempts to run applications or commands with elevated privileges
    - Any attempts to exploit known vulnerabilities to escalate privileges

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Unusual changes to user accounts or group membership
    - Suspicious use of elevated privileges
    - Any attempts to exploit known vulnerabilities

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Remove any unauthorized user accounts or group memberships
    - Disable any elevated privileges that are not necessary or authorized
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential privilege escalation attempts and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Defense Evasion

Objective:

To proactively search for and identify potential attempts by adversaries to evade detection and remain undetected in the environment.

Hypothesis:

Adversaries have deployed various evasion techniques to bypass security controls and remain undetected in the environment.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential evasion techniques:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Anti-virus logs and reports

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to evasion techniques. Queries may include:
    - Any attempts to disable or bypass security controls (e.g., antivirus, firewalls)
    - Any attempts to use known legitimate tools for malicious purposes (e.g., PowerShell, netsh)
    - Any attempts to hide or obfuscate malicious activity (e.g., using rootkits or backdoors)

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:

- Attempts to disable or bypass security controls
- Suspicious use of legitimate tools for malicious purposes
- Any attempts to hide or obfuscate malicious activity

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Enable any disabled or bypassed security controls
    - Remove any suspicious tools or scripts used for malicious purposes
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential defense evasion techniques used by adversaries and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Credential Access

Objective:

To proactively search for and identify potential attempts by adversaries to gain unauthorized access to credentials and user accounts.

Hypothesis:

Adversaries have gained access to a system and are attempting to steal credentials to gain greater control over the environment.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential credential theft attempts:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Anti-virus logs and reports

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to credential theft. Queries may include:
    - Any attempts to brute force login credentials
    - Any attempts to use known credential harvesting techniques (e.g., phishing, keylogging)
    - Any attempts to dump passwords from memory or registry

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Multiple failed login attempts from the same source
    - Suspicious network traffic to known command and control (C2) servers
    - Unusual changes to user accounts or group membership

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Reset compromised user account passwords
    - Remove any unauthorized user accounts or group memberships
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential credential theft attempts and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Discovery

Objective:

To proactively search for and identify potential attempts by adversaries to gather information about the environment for the purpose of launching further attacks.

Hypothesis:

Adversaries have gained access to the environment and are attempting to gather information about the network, systems, and applications.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential reconnaissance activities:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Anti-virus logs and reports

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to reconnaissance. Queries may include:
    - Any attempts to scan the network or systems
    - Any attempts to gather information about the environment (e.g., domain names, system configurations)
    - Any attempts to identify vulnerable systems or applications

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:

- Multiple failed login attempts from the same source
- Suspicious network traffic to known command and control (C2) servers
- Unusual changes to user accounts or group membership

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Close any open ports or services that are not needed
    - Review and update firewall and access control lists to block known malicious traffic
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential reconnaissance activities used by adversaries and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Lateral Movement

Objective:

To proactively search for and identify potential attempts by adversaries to move laterally within the environment in order to gain access to sensitive systems or data.

Hypothesis:

Adversaries have gained access to a system and are attempting to move laterally to other systems in the network.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential lateral movement attempts:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Active Directory logs

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to lateral movement. Queries may include:
    - Any attempts to connect to other systems or devices on the network
    - Any attempts to exploit vulnerabilities to gain access to other systems
    - Any attempts to use compromised credentials to access other system

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Unusual network traffic between systems
    - Suspicious logon events or user activity
    - Changes to file or directory permissions

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Quarantine any infected systems or devices
    - Reset compromised user account passwords
    - Remove any unauthorized user accounts or group memberships
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes

- If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential lateral movement attempts used by adversaries and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Collection

Objective:

To proactively search for and identify potential attempts by adversaries to collect or exfiltrate sensitive data from the environment.

Hypothesis:

Adversaries have gained access to the environment and are attempting to collect or exfiltrate sensitive data.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential data collection or exfiltration attempts:
   - Endpoint logs (e.g., Windows event logs, system logs)
   - Network logs (e.g., firewall logs, DNS logs)
   - Application logs (e.g., web server logs, database logs)
   - Email logs and alerts

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to data collection or exfiltration. Queries may include:
   - Any attempts to access sensitive files or directories
   - Any attempts to copy or move sensitive data to external locations
   - Any attempts to compress or encrypt data before exfiltration

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:

- Unusual network traffic to external IP addresses or domains
- Suspicious email activity or attachments
- Changes to file or directory permissions

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Block any unauthorized network traffic to external IP addresses or domains
    - Quarantine any infected systems or devices
    - Review and update file or directory permissions to prevent unauthorized access
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential data collection or exfiltration attempts used by adversaries and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Command and Control

Objective:

To proactively search for and identify potential command and control (C2) activities used by adversaries to remotely control compromised systems within the environment.

Hypothesis:

Adversaries have gained access to the environment and are attempting to establish C2 communications to remote command and control servers.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential C2 activities:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Email logs and alerts

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to C2 communications. Queries may include:
    - Any attempts to connect to known malicious IP addresses or domains
    - Any attempts to use non-standard network ports for communication
    - Any attempts to use encrypted or obfuscated communication protocols

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Unusual network traffic to known malicious IP addresses or domains
    - Suspicious DNS requests or responses
    - Changes to firewall rules or configurations

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Block any unauthorized network traffic to known malicious IP addresses or domains
    - Quarantine any infected systems or devices
    - Review and update firewall rules and configurations to prevent unauthorized access
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential C2 activities used by adversaries and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Exfiltration

Objective:

To proactively search for and identify potential attempts by adversaries to exfiltrate sensitive data from the environment.

Hypothesis:

Adversaries have gained access to the environment and are attempting to exfiltrate sensitive data out of the organization.

Playbook:

1. Define scope: Identify the network, endpoints, and servers that are in scope for this hunt. Ensure that the systems are up to date with the latest patches and have updated antivirus software.

2. Gather data: Collect and analyze the following data sources to identify potential exfiltration attempts:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Email logs and alerts

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to exfiltration. Queries may include:
    - Any attempts to access or move sensitive data to external locations
    - Any attempts to compress or encrypt data before exfiltration
    - Any attempts to transfer large amounts of data during non-business hours

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Unusual network traffic to external IP addresses or domains

- Suspicious email activity or attachments
- Changes to file or directory permissions

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Block any unauthorized network traffic to external IP addresses or domains
    - Quarantine any infected systems or devices
    - Review and update file or directory permissions to prevent unauthorized access
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes
    - If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential exfiltration attempts used by adversaries and take steps to prevent further attacks on your network. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers.

Impact

Objective:

To proactively search for and identify potential threats that could have an impact on critical assets within the organization.

Hypothesis:

Adversaries have already gained access to the environment and are attempting to carry out activities that could lead to significant impact on the organization.

Playbook:

1. Define scope: Identify the critical assets within the environment that could potentially be impacted. These assets may include servers, databases, applications, and other critical systems.

2. Gather data: Collect and analyze the following data sources to identify potential activities that could lead to impact:
    - Endpoint logs (e.g., Windows event logs, system logs)
    - Network logs (e.g., firewall logs, DNS logs)
    - Application logs (e.g., web server logs, database logs)
    - Email logs and alerts

3. Develop queries: Develop and run queries across the collected data sources to identify any suspicious activities related to impact. Queries may include:
    - Any attempts to modify or delete critical files or directories
    - Any attempts to modify or delete system settings or configurations
    - Any attempts to launch denial-of-service attacks against critical systems

4. Analyze results: Review the results of the queries to identify potential indicators of compromise (IOCs). These may include:
    - Unusual network traffic to critical systems or applications
    - Unusual login or access attempts to critical systems or applications
    - Changes to file or directory permissions or configurations

5. Take action: Once potential IOCs have been identified, take the following actions:
    - Block any unauthorized network traffic to critical systems or applications
    - Quarantine any infected systems or devices
    - Review and update file or directory permissions and configurations to prevent unauthorized access
    - Conduct further investigation to confirm the existence of malicious activity
    - Update antivirus signatures and firewalls to block known malicious files and hashes

- If necessary, escalate the incident to the incident response team for further action

6. Report: Document the findings and actions taken during the hunt. Share the findings with the appropriate stakeholders and ensure that any necessary actions are taken to prevent future attacks.

By following this playbook, you can proactively identify potential threats that could have an impact on critical assets within the organization and take steps to prevent further attacks. It is important to conduct regular threat hunting exercises to stay ahead of potential attackers and minimize the impact of any successful attacks.