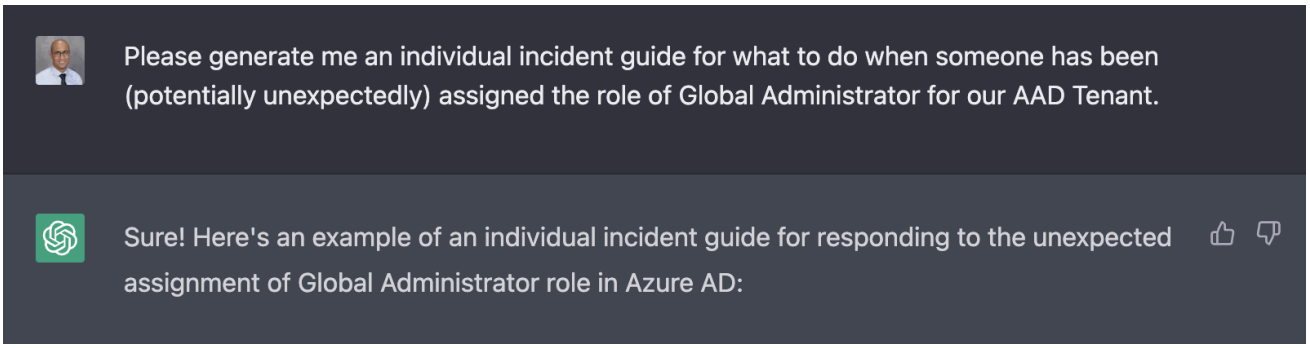
IR Playbook Table of Contents

Containment and Recovery Steps for Organization Defined Alerts

FYI: Playbook response outlines created with the following ChatGPT prompt:
Please generate me an individual incident guide for what to do when someone has been (potentially unexpectedly) assigned the role of Global Administrator for our AAD Tenant.



Incident: CUSTOM: Possible Privilege Escalation (Global Admin Role Assignment)

Incident Description

- This incident involves the unexpected assignment of the Global Administrator role to a user account in Azure AD.

Initial Response Actions

- Verify the authenticity of the alert or report.
- Identify the user account that was assigned the Global Administrator role.
- Determine how and when the role assignment occurred.
- Assess the potential impact of the incident.

Containment and Recovery

- Revoke the Global Administrator role from the affected user account immediately if unintended, otherwise skip to the documentation phase.
- Check for any other unauthorized role assignments made by the attacker and revoke them if necessary.
- Identify the root cause of the incident and take corrective actions to prevent similar incidents from occurring in the future.
- Restore any data or system configurations that may have been affected by the incident. This may involve resetting the Global Administrator password for the affected account and updating the secret in Key Vault

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Possible Privilege Escalation (Azure Key Vault Critical Credential Retrieval or Update)

Incident Description

- This incident involves the unexpected reading of a critical secret from the organization's Key Vault.

Initial Response Actions

- Verify the authenticity of the alert or report.
- Identify the secret that was read and the user or application that read it.
- Determine how and when the secret was read.
- Assess the potential impact of the incident.

Containment and Recovery

- Revoke access to the secret from the affected user or application immediately if unintended, otherwise skip to the documentation phase.
- Check for any other unauthorized access to the secret and revoke it if necessary.
- Monitor the affected systems for any suspicious activity related to the incident.
- Identify the root cause of the incident and take corrective actions to prevent similar incidents from occurring in the future.
- Change the secret if it was compromised.

Document Findings and Close out Incident

[Back to Top]

CUSTOM: CUSTOM: Malware Detected

Incident Description

- This incident involves malware being detected on a workstation, potentially compromising the confidentiality, integrity, or availability of the system and data.

Initial Response Actions

- Verify the authenticity of the alert or report.
- Identify the primary user account of the system if applicable
- Notify any affected stakeholders, such as users or customers, as appropriate, and provide them with guidance on how to protect themselves from potential harm.
- Run a full system scan using an up-to-date antivirus software to identify and remove the malware.
- If the malware cannot be removed or is suspected to have caused significant damage, shut down the workstation and disconnect it from the network.

Containment and Recovery

- Quarantine the infected workstation and any other systems that may have been impacted by the malware.
- Restore the infected workstation to a known clean state, such as a system image or a clean installation of the operating system and applications.

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force SUCCESS - Windows and Linux

Incident Description

- This incident involves observation of potential brute force attempts against a Windows VM.

Initial Response Actions

- Verify the authenticity of the alert or report.
- Immediately isolate the machine and change the password of the affected user
- Identify the origin of the attacks and determine if they are attacking or involved with anything else
- Determine how and when the attack occurred
    - Are the NSGs not being locked down? If so, check other NSGs
- Assess the potential impact of the incident.
    - What type of account was it? Permissions?

Containment and Recovery

- Lock down the NSG assigned to that VM/Subnet, either entirely, or to allow only necessary traffic
- Reset the affected user's password
- Enable MFA

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force SUCCESS - Azure Active Directory

Incident Description

- This incident involves observation of potential brute force success against Azure Active Directory

Initial Response Actions

- Verify the authenticity of the alert or report.
- Immediately identify and Revoke Sessions/Access for affected user
- Identify the origin of the attacker and determine if they are attacking or involved with anything else
- Assess the potential impact of the incident.
    - What type of account was it?
    - What Roles did it have?
    - How long has it been since the breach went unattended?

Containment and Recovery

- Reset the affected user's password and Roles if applicable
- Enable MFA
- Consider preventing any logins from outside the US with Conditional Access

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Possible Lateral Movement (Excessive Password Resets)

Incident Description

- This incident involves observation of potential lateral movement based on excessive password resets

Initial Response Actions

- Verify the authenticity of the alert or report.
- Immediately identify and Revoke Sessions/Access for any affected users
- Identify the attacker and determine if they are attacking or involved with anything else
- Observe the target accounts which had their passwords reset.
    - Have any of them immediately logged in or done anything else?
- Assess the potential impact of the incident.
    - What type of accounts are involved?
    - What Roles did it have?
    - How long has it been since the breach went unattended?

Containment and Recovery

- Reset the affected users' password and Roles if applicable
- Enable MFA

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force ATTEMPT - Windows

Incident Description

- ———————— Remaining are Blanke for you to Fill Out if You Like 🙂 ————————

Initial Response Actions

-

Containment and Recovery

-

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force ATTEMPT - MS SQL Server

Incident Description

-

Initial Response Actions

-

Containment and Recovery

-

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force ATTEMPT - Linux Syslog

Incident Description

-

Initial Response Actions

-

Containment and Recovery

-

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force ATTEMPT - Azure SQL Server

Incident Description

-

Initial Response Actions

-

Containment and Recovery

-

Document Findings and Close out Incident

[Back to Top]

CUSTOM: Brute Force ATTEMPT - Azure Active Directory

Incident Description

-

Initial Response Actions

-

Containment and Recovery

-

Document Findings and Close out Incident

[Back to Top]