AGE2

MANUAL DE UNTITLED GOOSE TOOL

1. Finalidad de la herramienta

Untitled Goose Tool es una herramienta robusta y flexible para encontrar y dar respuesta a incidentes que añade métodos novedosos de autenticación y recopilación de datos para ejecutar una investigación completa contra los entornos **Azure Active Directory (AzureAD***)*, **Azure** y **Microsoft 365** de un cliente. La herramienta Untitled Goose recopila telemetría adicional de **Microsoft Defender for Endpoint (MDE)** y **Defender for Internet of Things (IoT) (D4IoT)**.

Esta herramienta fue diseñada para ayudar a los equipos de respuesta a incidentes mediante la exportación de artefactos en la nube después de un incidente para entornos que no están realizando registros en un *SIEM (Security Information and Events Management)* u otra solución a largo plazo para registros.

2. Comenzando

2.1. Pre-Requisitos

- Se requiere Python 3.7, 3.8, o 3.9 para ejecutar Untitled Goose Tool con Python.
- Se requiere Firefox para autenticarse con Untitled Goose Tool.
- También se recomienda ejecutar Untitled Goose Tool dentro de un entorno virtual.

2.1.1. Instalación de versión inferior de Python (3.7,3.8,3.9)

WINDOWS 10

https://www.python.org/ftp/python/3.8.10/python-3.8.10-amd64.exe

Lo instalamos y marcamos la opción de Agregar al PATH.

LINUX

Link de los comandos: https://pastebin.com/yP6wKYNe

sudo apt update -y && sudo apt upgrade -y

sudo su

sudo apt install build-essential zlib1g-dev libncurses5-dev libgdbm-dev libnss3-dev libssl-dev libsqlite3-dev libreadline-dev libffi-dev curl libbz2-dev -y

wget https://www.python.org/ftp/python/3.8.0/Python-3.8.0.tgz

tar -xvf Python-3.8.0.tgz

cd Python-3.8.0

sudo ./configure –enable-optimizations

make -j

make altinstall

python3.8 --version

sudo update-alternatives --install /usr/bin/python python /usr/local/bin/python3.8 1

2.1.2. Instalamos Firefox

https://www.mozilla.org/es-ES/firefox/new/

2.1.3. Instalamos Visual C++

https://aka.ms/vs/17/release/vc_redist.x64.exe

2.2. Requisitos principales

Se requieren los siguientes permisos de AzureAD/M365 para ejecutar Untitled Goose Tool y proporcionarle acceso de solo lectura al tenant.

Una cuenta de usuario con los siguientes permisos:

Centro de administración de Exchange Online:
- View-Only Audit Logs
- View-Only Configuration
- View-Only Recipients
- User Options

Una aplicación creada como servicio principall de azure con los siguientes permisos:

- **Permisos API:**

Microsoft Threat Protection:
- AdvancedHunting.Read.All (Application)

WindowsDefenderATP:
- AdvancedQuery.Read.All (Application)
- Alert.Read.All (Application)
- Library.Manage (Application)
- Machine.Read.All (Application)
- SecurityRecommendation.Read.All (Application)
- Software.Read.All (Application)

- Ti.ReadWrite (Application)
- Vulnerability.Read.All (Application)

Microsoft Graph:
- APIConnectors.Read.All (Application)
- AuditLog.Read.All (Application)
- ConsentRequest.Read.All (Application)
- Directory.Read.All (Application)
- Domain.Read.All (Application)
- IdentityProvider.Read.All (Application)
- IdentityRiskEvent.Read.All (Application)
- IdentityRiskyServicePrincipal.Read.All (Application)
- IdentityRiskyUser.Read.All (Application)
- MailboxSettings.Read (Application)
- Policy.Read.All (Application)
- Policy.Read.PermissionGrant (Application)
- Reports.Read.All (Application)
- RoleManagement.Read.All (Application)
- SecurityActions.Read.All (Application)
- SecurityAlert.Read.All (Application)
- SecurityEvents.Read.All (Application)
- UserAuthenticationMethod.Read.All (Application)

Roles de la Suscripción IAM de Azure:
- Reader
- Storage Blob Data Reader
- Storage Queue Data Reader

Aviso: Al crear el servicio principal de azure, asegúrese de guardar el valor del secret del cliente (no el ID del secret del cliente). El secret y el ID son valores distintos.

2.3. Instalación

Para instalar, clone el repositorio de la herramienta, en el github oficial de CISA y luego haga una instalación pip:

git clone https://github.com/cisagov/untitledgoosetool.git

cd untitledgoosetool

python -m pip install .

3. Uso

3.1. Configuración

Untitled Goose Tool requiere parámetros de autenticación y configuración. Para construir automáticamente el archivo de configuración, ejecute lo siguiente con el repositorio clonado:

python scripts/generate_conf.py

Después de esto, los archivos .conf y .d4iot_conf deben ser colocados en su directorio actual. Estos archivos son utilizados por Untitled Goose Tool. Debes rellenar la sección superior [auth] para que Untitled Goose Tool pueda autenticarse correctamente en los recursos apropiados.

La configuración básica es la siguiente:

Link del texto: https://pastebin.com/AvsT2hrV

[auth]
username=
password=
tenant=
us_government=
exo_us_government=
appid=
clientsecret=
subscriptionid=
m365=
msgtrace=

[filters]
date_start=
date_end=

[azure]
activity_log=False
alerts=False
all_azure_subscriptions=False
all_resources=False
assessments=False
bastion_logs=False
compliance=False
container_config=False
diagnostic_settings=False
file_shares=False
key_vault_log=False
network=False

nsg_flow_logs=False
portal_alerts=False
portal_defendersettings=False
portal_pcap=False
portal_sensors=False
security_center=False
storage_accounts=False
vm_config=False

[azuread]
applications=False
azuread_audit=False
azuread_provisioning=False
conditional_access=False
devices=False
directory_roles=False
groups=False
identity_provider=False
organization=False
policies=False
risk_detections=False
risky_objects=False
security=False
service_principals=False
signins_adfs=False
signins_msi=False
signins_rt=False
signins_sp=False
summaries=False
users=False

[m365]
exo_addins=False
exo_groups=False
exo_inboxrules=False
exo_mailbox=False
powershell_calls=False
ual=False

[mde]
advanced_hunting_query=False
alerts=False
indicators=False
investigations=False
library_files=False
machine_vulns=False
machines=False
recommendations=False

software=False

[msgtrc]
setemailaddress=
direction=
messageid=
notifyaddress=
originalclientip=
recipientaddress=
reporttitle=
reporttype=
senderaddress=

Aquí hay un archivo conf con descripciones de los campos:

[auth]
username= El nombre de usuario de tu cuenta. ej: AAD_upn@example.onmicrosoft.com

password= La contraseña de su cuenta. ej: AAD_password

tenant= El ID de tenant de tu tenant AAD.

us_government= Si tiene un tenant GCC High, establezca este valor en True; de lo contrario, establezca este valor en False. (GCC High significa "Government Community Cloud High" y es una versión de Microsoft Azure que cumple con los requisitos de seguridad y cumplimiento de la información del Departamento de Defensa de los Estados Unidos (DoD) para manejar datos no clasificados y controlados.)

exo_us_government= Si su tenant de Microsoft 365 es un tenant gubernamental, establezca este valor en True; de lo contrario, establezca este valor en False.

appid= El ID de aplicación de su servicio principal.

clientsecret= El secret de cliente de su principal de servicio (no el ID secret).

subscriptionid= Si desea comprobar todas sus suscripciones de Azure, establezca esta opción en Todas; de lo contrario, introduzca su ID de suscripción de Azure. Para varios ID, sepárelos con comas, sin espacios.

m365= Si tienes un entorno M365, establezca este valor en True; de lo contrario, establezca este valor en False.

msgtrace= Si desea ejecutar el rastreo de mensajes, establezca este valor en True; de lo contrario, establezca este valor en False.

[filters]
date_start= Sólo se aplica a las llamadas de inicio de sesión de Azure AD. El intervalo de fechas máximo es de 30 días. El formato debe ser AAAA-MM-DD.

date_end= Sólo se aplica a las llamadas de inicio de sesión de Azure AD. El intervalo de fechas máximo es la fecha de hoy. El formato debe ser AAAA-MM-DD.

[azure]
activity_log=False
alerts=False
all_azure_subscriptions=False
all_resources=False
assessments=False
bastion_logs=False
compliance=False
container_config=False
diagnostic_settings=False
file_shares=False
key_vault_log=False
network=False
nsg_flow_logs=False
portal_alerts=False
portal_defendersettings=False
portal_pcap=False
portal_sensors=False
security_center=False
storage_accounts=False
vm_config=False

[azuread]
applications=False
azuread_audit=False
azuread_provisioning=False
conditional_access=False
devices=False
directory_roles=False
groups=False
identity_provider=False
organization=False
policies=False
risk_detections=False
risky_objects=False
security=False
service_principals=False
signins_adfs=False
signins_msi=False
signins_rt=False
signins_sp=False
summaries=False
users=False

[m365]

exo_addins=False
exo_groups=False
exo_inboxrules=False
exo_mailbox=False
powershell_calls=False
ual=False

[mde]
advanced_hunting_query=False
alerts=False
indicators=False
investigations=False
library_files=False
machine_vulns=False
machines=False
recommendations=False
software=False

[msgtrc]
setemailaddress= Si desea que Microsoft le notifique cuando esté listo el archivo de logs para su descarga, defínalo como True; de lo contrario, defínalo como False.

direction= Las opciones son All, Inbound, Outbound.

messageid= Si desea comprobar el estado o exportar el trace del mensaje, puede introducir aquí el ID del mensaje.
notifyaddress= Si desea que Microsoft le notifique cuando el archivo de logs esté listo para su descarga, introduzca aquí un correo electrónico. Si tiene `setemailaddress=False`, puede dejar este campo en blanco.

originalclientip= Si tiene una dirección IP de cliente que desea comprobar, introdúzcala aquí.

recipientaddress= Dirección de correo electrónico del destinatario sobre el que desea realizar un rastreo de mensajes.

reporttitle= Establezca aquí el título del informe.

reporttype= Las opciones son MessageTraceDetail or MessageTrace.

senderaddress= Dirección de correo electrónico del remitente sobre el que desea realizar un rastreo de mensajes.

La configuración D4IoT se parece a:

Link del texto: https://pastebin.com/Uiw5tMKc

[auth]
username=

password=
tenant=
appid=
clientsecret=
subscriptionid=
d4iot_sensor_token=
d4iot_mgmt_token=
d4iot_sensor_ip=
d4iot_mgmt_ip=

[d4iot]
mgmt_alerts=False
mgmt_devices=False
mgmt_pcap=False
mgmt_sensor_info=False
sensor_alerts=False
sensor_device_connections=False
sensor_device_cves=False
sensor_device_vuln=False
sensor_devices=False
sensor_events=False
sensor_operational_vuln=False
sensor_pcap=False
sensor_security_vuln=False

Aquí hay un archivo conf D4IoT con descripciones de los campos:

Link del texto: https://pastebin.com/nz2ZHwHH

[auth]
username= El nombre de usuario de tu cuenta. ej: AAD_upn@example.onmicrosoft.com
password= La contraseña de su cuenta. ej: AAD_password
tenant= El ID de tenant de su tenant AAD.
appid= El ID de aplicación de su servicio principal.
clientsecret= El secret de cliente de su principal de servicio (no el ID secret).
subscriptionid= Si desea comprobar todas sus suscripciones de Azure, establezca esta opción en Todas; de lo contrario, introduzca su ID de suscripción de Azure. Para varios ID, sepárelos con comas, sin espacios.
d4iot_sensor_token= Introduzca su token API del sensor D4IoT.
d4iot_mgmt_token= Introduzca su token API de la consola de gestión D4IoT.
d4iot_sensor_ip= Introduzca la IP de su sensor D4IoT.
d4iot_mgmt_ip= Introduzca la IP de su consola de gestión D4IoT.

[d4iot]
mgmt_alerts=False
mgmt_devices=False
mgmt_pcap=False

mgmt_sensor_info=False
sensor_alerts=False
sensor_device_connections=False
sensor_device_cves=False
sensor_device_vuln=False
sensor_devices=False
sensor_events=False
sensor_operational_vuln=False
sensor_pcap=False
sensor_security_vuln=False

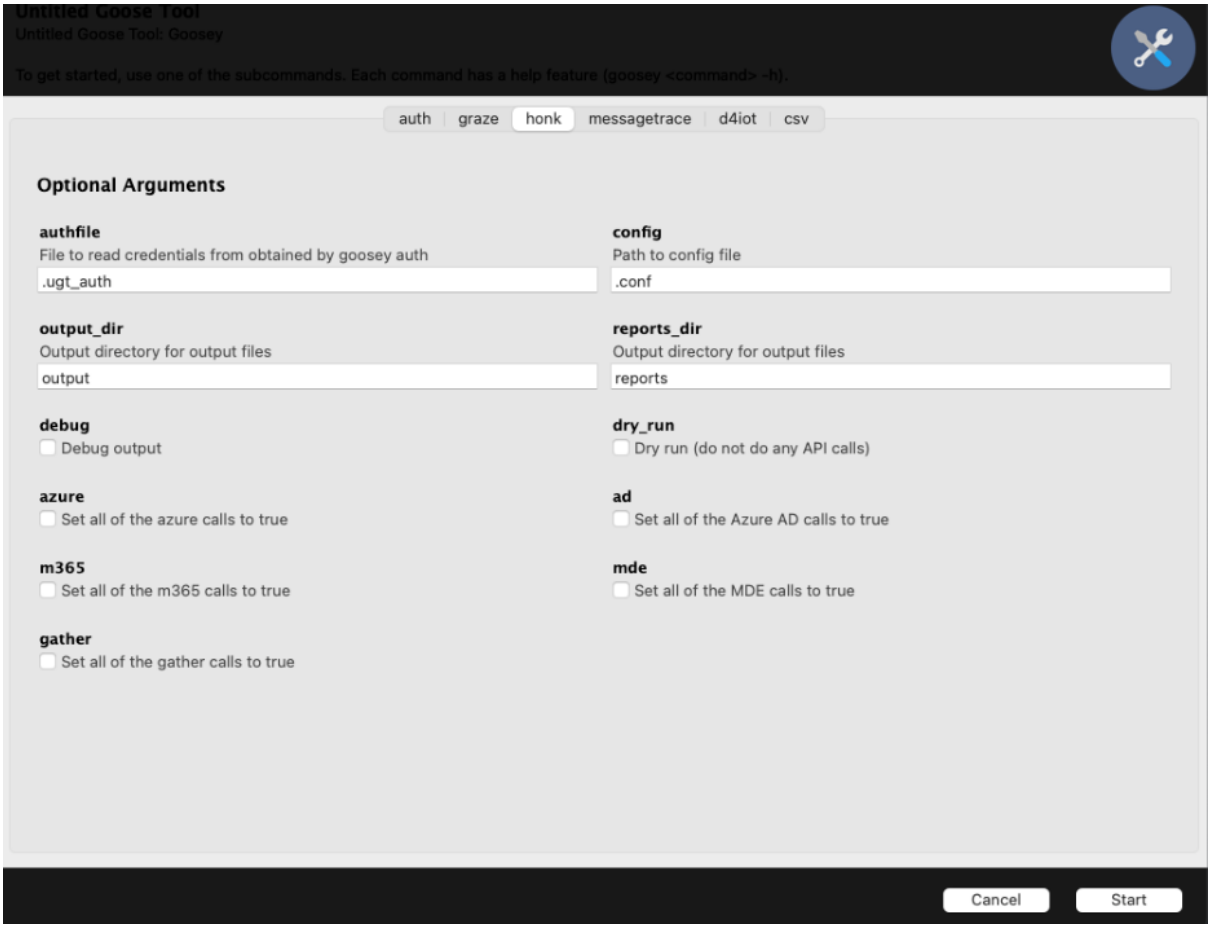
Para activar parámetros específicos, puede cambiar las apariciones de *False* a *True* (sin distinguir mayúsculas de minúsculas).

3.2. GUI

Hay una GUI simplificada basada en Gooey (https://github.com/chriskiehl/Gooey).

Para ejecutar con GUI:

Comando: ***goosey-gui***



3.3. Parámetros de Autorización

Uso: *goosey auth [-h] [-a AUTHFILE] [--d4iot-authfile D4IOT_AUTHFILE] [-c CONFIG] [--d4iot-config D4IOT_CONFIG]*
[--revoke] [--interactive] [--debug] [--d4iot]

Argumentos opcionales:
-h, --help Enseña el mensaje de ayuda con los parámetros y hace un exit.

-a AUTHFILE, --authfile AUTHFILE
Archivo para guardar las credenciales (por defecto: .ugt_auth)

--d4iot-authfile D4IOT_AUTHFILE
Archivo para guardas las credenciales para iOt(por defecto: .d4iot_auth)

-c CONFIG, --config CONFIG
Ruta del archivo de configuración con credenciales de autorización.

--d4iot-config D4IOT_CONFIG
Ruta del archivo de configuración con credenciales de autorización de d4iot.

--revoke Revocar sesiones para usuarios con credenciales en el tokenfile (por defecto: .ugt_auth)

--interactive Modo interactivo para Selenium. Por defecto es false (sin cabecera).

--debug Activar logs de debug al disco

--d4iot Ejecutar la parte de autenticación para d4iot

3.4. CSV

Esta herramienta es una utilidad de línea de comandos de Goosey que se utiliza para convertir archivos de Goose a archivos CSV.

Uso: *goosey csv [-h] [-o OUTPUT_DIR] [-r RESULT_DIR] [--debug]*

Argumentos opcionales:
-h, --help Muestra este mensaje y sale de la aplicación
-o OUTPUT_DIR, --output_dir OUTPUT_DIR

El directorio donde se encuentran los archivos de Goose
-r RESULT_DIR, --result_dir RESULT_DIR

El directorio donde se encuentran los archivos de Goose

--debug Salida del Debug (output)

3.5. Graze: Realiza la delimitación temporal de la UAL.

La herramienta "Graze" es una utilidad de Goosey que se utiliza para realizar la delimitación temporal de la UAL. La UAL (Unidad de Actividad de Lógica) es una técnica utilizada en la detección de amenazas que implica la identificación de secuencias de eventos que podrían ser indicativos de un ataque en curso. "Graze" ayuda a definir el intervalo de tiempo para la delimitación temporal de la UAL, lo que significa que ayuda a establecer el período de tiempo para el que se va a analizar el registro de eventos en busca de patrones y señales de amenazas.

Uso: *goosey graze [-h] [-a AUTHFILE] [-o OUTPUT_DIR] [-d] [-e ENDPOINT]*

optional arguments:
-h, --help Muestra este mensaje y se sale

-a AUTHFILE, --authfile AUTHFILE
Fichero del que leer las credenciales obtenidas por goosey auth

-o OUTPUT_DIR, --output-dir OUTPUT_DIR
Directorio de salida para los sensores

-d, --debug Salida del Debug

-e ENDPOINT, --endpoint ENDPOINT
Endpoint para UAL. Puede cambiar a localhost para pruebas si está en un servidor local.

Ejecutar con valores predeterminados:

Comando: ***goosey graze***

3.6. Honk: Extrae datos dentro de rangos temporales.

La herramienta Honk sirve para extraer datos de diferentes servicios y aplicaciones dentro de rangos temporales específicos.

Uso: *goosey honk [-h] [-a AUTHFILE] [-c CONFIG] [--output-dir OUTPUT_DIR] [--reports-dir REPORTS_DIR] [--debug] [--dry-run] [--azure] [--ad] [--m365] [--mde]*
[--dry-run] [--azure] [--ad] [--m365] [--mde]

Argumentos opcionales:
-h, --help mostrar este mensaje de ayuda y salir

-a ARCHIVO DE AUTENTICACIONES, --authfile ARCHIVO DE AUTENTICACIONES
Archivo del que leer las credenciales obtenidas por goosey auth

-c CONFIG, --config CONFIG
Ruta al archivo de configuración

--output-dir OUTPUT_DIR
Directorio de salida para los archivos de salida

--reports-dir REPORTS_DIR
Directorio de salida para los archivos de salida

--debug Salida de depuración

--dry-run Ejecución en seco (no realiza ninguna llamada a la API)

--azure Establece todas las llamadas a Azure en true

--ad Establecer todas las llamadas a Azure AD en true

--m365 Establecer todas las llamadas a M365 en true

--mde Establecer todas las llamadas MDE en true

Ejecutar con las opciones por defecto:

Comando: *goosey honk*

Ejecutar con mensajes de depuración, salida al directorio my_outputs, habilitar todas las llamadas Azure:

goosey honk *--debug --output-dir my_outputs --azure*

3.7. Messagetrace

Permite a los usuarios recopilar y rastrear mensajes en Azure con diferentes opciones y argumentos para personalizar su funcionamiento.

Uso: goosey messagetrace [-h] [--debug] [-c CONFIG] [-a AUTHFILE] [--output-dir OUTPUT_DIR] [--submit-report] [--gather-report] [--status-check] [--interactive
[--gather-report] [--status-check] [--interactive]

argumentos opcionales:
-h, --help mostrar este mensaje de ayuda y salir

--debug Salida de depuración

-c CONFIG, --config CONFIG
Ruta al archivo de configuración

-a AUTHFILE, --authfile AUTHFILE
Fichero del que leer las credenciales obtenidas por goosey auth

--output-dir OUTPUT_DIR
Directorio de salida para los archivos de salida

--submit-report

Envía un informe de seguimiento de mensajes

--gather-report
Recopila un informe de seguimiento de mensajes

--status-check
Automatiza la comprobación del estado tras enviar la solicitud de rastreo

--interactive
Modo interactivo para Selenium. Por defecto es false (headless).

Envío de un informe de rastreo de mensajes:

Comando: *goosey messagetrace --submit-report*

Descarga de un informe de rastreo de mensajes con Selenium interactivo:

Comando: *goosey messagetrace --gather-report --interactive*

3.8. Flujo de trabajo recomendado

1. Rellena el archivo .conf con su información y establece las llamadas deseadas en True.
2. Ejecuta goosey auth.
3. Ejecuta goosey honk.

3.9. Flujo de trabajo recomendado para la llamada UAL con límites de tiempo

1. Rellene el archivo .conf con su información.
2. Ejecuta goosey auth.

3. Ejecuta goosey graze y espera a que termine de ejecutarse.
4. Abra el archivo .conf y establezca UAL en True.
5. Ejecuta goosey honk.

3.10. Consideraciones

- Se recomienda rellenar el archivo .conf con tu información como primer paso.
- Ejecuta siempre goosey auth antes de realizar cualquier otra llamada a goosey aparte de goosey csv, que no requiere autenticación para ejecutarse.

4. Problemas conocidos

4.1. Tener % en la contraseña:

Solución: Asegúrate de evitar el símbolo % en la contraseña con %%, ya que al utilizarlo es posible que se interprete como un carácter especial y lleve a errores.

4.2. Error al intentar pip install . cuando se usa Windows y Python 3.10:

Running setup.py install for wxpython did not run successfully.

La ejecución de setup.py install para wxpython no se ejecutó correctamente.

Solución: Realiza un downgrade a la versión de Python a 3.9.x. o 3.8.x como se explica al principio. Es un problema conocido con wxpython.

4.3. Error al intentar pip install . en Mac:

ModuleNotFoundError: No module named 'certifi'

Solución: Ve a la carpeta de aplicaciones, busque su carpeta de versiones de python y haz doble clic en el archivo "Install Certificates.command" dentro de la carpeta de python para instalar el certificado.

4.4. ¿Por qué Untitled Goose Tool devuelve dos resultados para las reglas de bandeja de entrada de Exchange Online y los permisos de buzón de Exchange Online?

Solución: Tanto la API como las llamadas PowerShell son robustas y muestran información diferente, por lo que decidimos mantener ambas.

4.5. Error después de ejecutar determinadas llamadas de Azure Security Center:

Resultados de cumplimiento de Azure:

Error: (MissingSubscription) The request did not have a subscription or a valid tenant level resource provider.
Code: MissingSubscription
Message: The request did not have a subscription or a valid tenant level resource provider.

Traducción:

Error: (MissingSubscription) La solicitud no tenía una suscripción o un proveedor de recursos de nivel de tenant válido.

Código: MissingSubscription

Mensaje: La solicitud no tenía una suscripción o un proveedor de recursos de nivel de tenant válido.

Políticas de protección de la información de Azure:

Error: Operation returned an invalid status 'Not Found'

Traducción:

Error: La operación devolvió un estado no válido 'No encontrado'

Azure Assessments:

Discriminator source is absent or null, use base class ResourceDetails.

Traducción:

La fuente del discriminador está ausente o es nula, utilice la clase base ResourceDetails.

Azure SubAssessments:

Subtype value GeneralVulnerability has no mapping, use base class AdditionalData.

Subtype value SqlVirtualMachineVulnerability has no mapping, use base class AdditionalData.

Traducción:

El valor del subtipo GeneralVulnerability no tiene asignación, utilice la clase base AdditionalData.

El valor del subtipo SqlVirtualMachineVulnerability no tiene asignación, utilice la clase base AdditionalData.

Solución: Estos mensajes no son problemas.

- La llamada al resultado de cumplimiento de Azure seguirá completándose.
- La llamada a la política de protección de la información de Azure no es un error crítico.
- La llamada a las evaluaciones de Azure spamea la consola con una línea de advertencia: "Discriminator source is absent or null, use base class ResourceDetails" y se completará sin ningún problema (aparte del spam de la consola).
- La llamada a las subevaluaciones de Azure envía spam a la consola con una línea de advertencia: "Subtype value GeneralVulnerability has no mapping, use base class AdditionalData." o "Subtype value SqlVirtualMachineVulnerability has no mapping, use base class AdditionalData." y se completará sin problemas (también habrá spam de la consola).

4.6. Es posible que los usuarios de MacOS y/o sistemas *nix no puedan ejecutar el script PowerShell EXO.ps1.

Solución: Recomendamos utilizar Windows si desea ejecutar el script PowerShell.

4.7. Firefox geckodriver no está en PATH

auth - ERROR - Error getting Firefox webdriver: Message: 'geckodriver' executable needs to be in PATH.
Traducción:
auth - ERROR - Error al obtener Firefox webdriver: Mensaje: El ejecutable 'geckodriver' debe estar en PATH.

Solución: Ejecute los siguientes comandos:

#Para Windows:
webdrivermanager firefox:v0.32.0 --linkpath AUTO

#Para *nix (puede necesitar sudo):
webdrivermanager firefox:v0.32.0 --linkpath /usr/local/bin

4.8. Excesiva cantidad de errores 429 durante goosey honk

Solución: Untitled Goose Tool se encontrará rápidamente con las limitaciones de Graph API del usuario; se trata de una limitación que Microsoft tiene en las llamadas a Graph API.

5. Preguntas más frecuentes

5.2. ¿Qué sistemas operativos son compatibles con Untitled Goose Tool?
Untitled Goose Tool puede funcionar tanto en Windows como en MacOS, pero el script PowerShell es recomendado para su uso exclusivo en Windows.

5.3. ¿Qué debo hacer con los resultados?

Introduzca los resultados JSON en una herramienta de gestión de eventos e información de seguridad (SIEM), un navegador web, un editor de texto o una base de datos, editor de texto o una base de datos.

5.4. ¿Con qué frecuencia debo ejecutar la herramienta?

Los usuarios pueden ejecutar Untitled Goose Tool una vez, como una instantánea en el tiempo, o de forma rutinaria. Para determinados tipos de registro, la herramienta recogerá desde la última vez que se ejecutó la herramienta.

5.5. ¿Necesito configurar la herramienta antes de ejecutarla?

Sí, deberá editar el archivo .conf. Consulte el archivo README.md en el repositorio Untitled Goose Tool GitHub para obtener más instrucciones.

5.6. ¿Realizará Untitled Goose Tool cambios en el entorno de la nube?

No, la herramienta no puede realizar cambios en el entorno de la nube. Sólo consulta información.

5.7. ¿Cuánto tiempo se tarda en ejecutar la herramienta?

El tiempo de ejecución depende del tamaño del entorno de nube, la cantidad de actividad y la y la llamada específica establecida en el archivo de configuración.