centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1217

Procedimiento de empleo seguro
Falcon Sensor CrowdStrike

Febrero de 2024

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.01 11:18:27 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-097-6.
Fecha de Edición: febrero de 2024.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

La plataforma Falcon de CrowdStrike ofrece una prevención contra ciber amenazas óptima, mediante el uso de inteligencia artificial (AI) y aprendizaje automático (ML) con detección y respuesta avanzada e información sobre amenazas, integrada a través de una consola de gestión altamente intuitiva. Adicionalmente ofrece visibilidad gracias a la telemetría que obtiene del *endpoint*, esta información puede ser utilizada tanto para detecciones basadas en comportamiento como para tareas de *hunting*.

Se trata de una plataforma modular, que ayuda al cliente en la implantación actual y futura de su estrategia de seguridad. De esta forma, a medida que el cliente requiera nuevas capacidades de visibilidad y protección, podrá facilitarse el acceso a estas funcionalidades de forma instantánea sin necesidad de desplegar ninguna solución, elemento, agente o entorno adicional a los desplegados inicialmente.

Las capacidades relativas a la protección de *endpoints* se basan en la detección y prevención integradas en el agente. Se dispone de motores de detección específicos basados *en machine learning* (identificando la maliciosidad de las muestras en base al análisis de morfología de los ficheros y patrones), motores *antiexploit* y análisis de Indicadores de Ataque (IoA) que se apoyan en la detección de las técnicas, tácticas y procedimientos utilizados por los principales actores maliciosos. Estas capacidades de detección permiten detectar *malware* conocido y desconocido, reducen los falsos positivos y minimizan el consumo de recursos del *host*. Todas las capacidades de detección y prevención están disponibles en el agente independientemente de si el equipo se encuentra conectado a la red o no.

Falcon ofrece la solución de reemplazo ideal para el entorno considerado combinando las capacidades de prevención más efectivas y la mayor visibilidad de la cadena de ataque con la mayor simplicidad en cuanto a arquitectura y agente desplegado.

Proporciona protección frente a todo tipo de ataques, desde *malware* sencillo orientado a entorno doméstico hasta los ataques más sofisticados utilizando múltiples mecanismos de detección de amenazas:

- *Machine learning* e inteligencia artificial: capacidades de análisis integradas en el propio agente basada en el análisis de la morfología de cada uno de los artefactos a analizar permitiendo la para la detección de malware conocido y desconocido (*zero-day*) y *ransomware*.
- Indicadores de Ataque y Comportamiento (IoAs): protegiendo contra ataques sofisticados incluyendo ataques libres de malware y ataques sin ficheros (*fileless*).
- Motor antiexploit: para parar la ejecución y la propagación de amenazas utilizando vulnerabilidades no parcheadas.
- Indicadores de Ataque (IoAs) y Compromiso (IoCs) personalizados e importables de otras fuentes.
- Capacidad de envío de ficheros a cuarentena para investigación posterior.

- *Script-based execution monitoring*: inspección y bloqueo de macros maliciosas de MS Office.
- *Sensor tampering*: protección de intentos de manipulación (desinstalación, instalación, deshabilitar, etc.) del agente incluso para usuarios con cuenta con permisos privilegiados.

Adicionalmente, Falcon proporciona capacidades operativas para facilitar la detección e investigación de alertas ya que:

- Proporciona detalles, contexto e histórico para cada detección.
- Desenmaraña la complejidad de los ataques presentando éste en forma de árbol de procesos enriquecido con información contextual y de inteligencia.
- Mapeo de las alertas con la taxonomía MITRE *Adversarial Tactics, Techniques and Common Knowledge* (ATT&CK®) facilitando el entendimiento de forma rápida incluso de los ataques más complejos.

2. OBJETO Y ALCANCE

El objetivo del presente documento es detallar las **configuraciones de seguridad del producto** *Falcon CrowdStrike*, para su funcionamiento se realice de acuerdo con unas garantías mínimas de seguridad.

Falcon CrowdStrike es un producto *software* cuya instalación se realiza en los *endpoints*, mediante el uso de agentes y es administrado desde la consola desplegada en la nube.

El agente de Falcon CrowdStrike, versión 7.05, sobre Windows, es el componente de la solución que ha sido cualificado para categoría ALTA del Esquema Nacional de Seguridad e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional, en las familias de "*Antivirus/EPP (Endpoint Protection Platform)*" y "*EDR (Endpoint Detection and Response)*".

Los sistemas operativos sobre los que puede desplegarse la versión cualificada de Falcon CrowdStrike:

- *Windows Server 2019, Windows Server Core 2019, Windows Server 2016, Windows Server Core 2016, Windows Server 2012 R2, Windows Storage Server 2021 R2, Windows Server 2012, Windows Server 2008 R2 SP1 (64-bit).*
- *Windows 10 (except Windows 10 64-bit v1511 and v1703).*

Para estudiar la posible compatibilidad del sensor con otras versiones de SO Windows sin soporte de seguridad por parte de Microsoft (por ejemplo, Windows 7 SP1 o Windows 2008 R2) se deberá consultar directamente con el fabricante, aunque bajo ningún concepto se recomienda o se cualifica el sensor para su uso sobre sistemas operativos sin soporte de seguridad.

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento está organizado en diferentes capítulos, de acuerdo con diferentes fases del ciclo de vida del producto:

a) **Apartado 4. Fase de despliegue**. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de despliegue del producto.

b) **Apartado 5. Fase de instalación**. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de instalación del producto.

c) **Apartado 6. Fase de configuración**. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) **Apartado 7. Fase de operación**. En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.

e) **Apartado 8. *Checklist***. En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

f) **Apartado 9. Referencias**. Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

g) **Apartado 10. Abreviaturas**. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE

4.1 CONSIDERACIONES PREVIAS

4.1.1 REQUISITOS DE CONECTIVIDAD DEL AGENTE CON EL CLOUD DE FALCON

La conexión saliente del agente es una conexión SSL por el puerto 443. Esta no debe ser inspeccionada o el agente no se conectará. Si la conexión se realiza a través de *proxy* (opción APP_PROXYNAME), la conexión debe no ser autenticada o el agente no se conectará. El agente debe tener salida, bien directa o bien a través de proxy a:

a) *Ts01-lanner-lion.cloudsink.net*

b) *lfodown01-lanner-lion.cloudsink.net*

En su defecto, si se prefiere, se puede definir el rango de IPs normalizadas:

EU-1	Public DNS Name	IP
Term Servers	ts01-lanner-lion.cloudsink.net	3.121.187.176
		3.121.6.180
		3.121.238.86
LFO Download	lfodown01-lanner-lion.cloudsink.net	18.184.114.155
		18.194.8.224
		3.121.13.180

4.1.2 COMPATIBILIDAD DEL AGENTE CON SISTEMAS WINDOWS

Se recomienda **consultar la tabla de compatibilidades** de los agentes con los sistemas operativos en las guías de despliegue de cada sistema, en la siguiente URL: https://falcon.eu-1.crowdstrike.com/support/documentation, bajo *"Sensor Deployment and Maintenance > Sensor Deployment > Falcon Sensor for Windows"*. En dicha tabla también se recoge **la fecha de fin de soporte** de la versión del agente.

Windows Desktop OSes	Versión	Codename	Marketing Name	LTSC Release?	Soporte de 64-bit	Soporte Enterprise IOT 64-bit	Soporte 32-bit	Soporte mínimo del sensor	Fecha Falcon EOS
Windows 11 [5]	21H2	Sun Valley	N/A	—	Sí	—	—	6.31.14505	Abril 7, 2025
Windows 10	21H2	21H2	November 2021 Update	Sí	Sí	Sí	Sí	6.33.14704	Julio 11, 2032
Windows 10	21H1	21H1	May 2021 Update	—	Sí	Sí	Sí	6.24.13806+	Junio 11, 2023
Windows 10	20H2	20H2	October 2020 Update	—	Sí	Sí	Sí	Soporta todas las versiones del sensor	Noviembre 5, 2023
Windows 10	2004	20H1	May 2020 Update	—	Sí	Sí	Sí	Soporta todas las versiones del sensor	Junio 12, 2022
Windows 10	1909	19H2	November 2019 Update	—	Sí	Sí	Sí	Soporta todas las versiones del sensor	Noviembre 6, 2022
Windows 10	1809	Redstone 5 ("RS5")	October 2018 Update	Sí	Sí	Sí	Sí	64-bit, Soporta todas las versiones del sensor. 32-bit, 6.24.13806+	Julio 8, 2029
Windows 10	1607	Redstone 1 ("RS1")	Anniversary Update	Sí	Sí	—	—	Soporta todas las versiones del sensor	Abril 21, 2027
Windows 10	1507	Threshold 1	N/A	Sí	Sí	—	—	Soporta todas las versiones del sensor	Abril 12, 2026

Tabla 1 - Compatibilidad del sensor con algunas versiones de Windows

4.1.3 PERMISOS ELEVADOS

Se debe verificar si el usuario encargado de realizar la instalación posee permisos elevados. En caso de no tener permisos elevados la instalación no podrá llevarse a cabo. Una vez finalizado el proceso de instalación, no es necesario reiniciar el sistema.

4.2 OBTENCIÓN SEGURA DEL PRODUCTO

Durante el proceso de entrega deberán realizarse una serie tareas de comprobación, de cara a garantizar que el producto recibido no ha sido manipulado:

El instalador del agente de Falcon (Falcon lo denomina: “Sensor”) se obtiene desde el portal web https://falcon.eu-1.crowdstrike.com en la siguiente ruta: “*Hosts > Sensor Downloads*”. El acceso está protegido por usuario y contraseña. Además, tiene la posibilidad de configurar la protección 2FA.

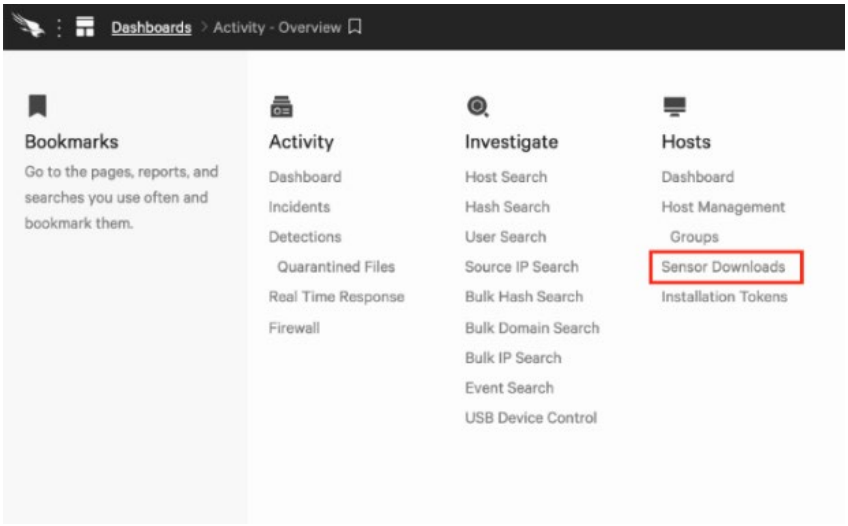

Ilustración 1 - Descarga del sensor

Se debe comprobar si el SHA256 del agente descargado coincide con el que se muestra en el portal de Falcon. Para ello, se puede utilizar cualquier aplicación de cálculo de hashes (HashCheck, CertUtil, etc), por ejemplo:

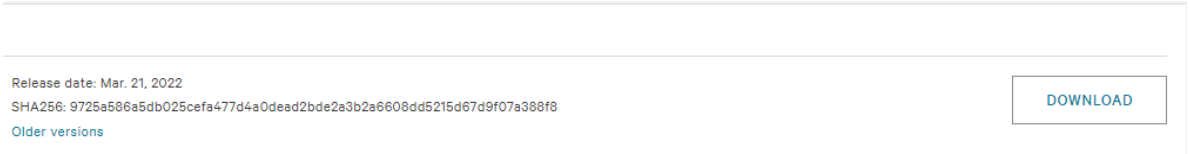

Ilustración 2 - Chequeo Hash en el portal

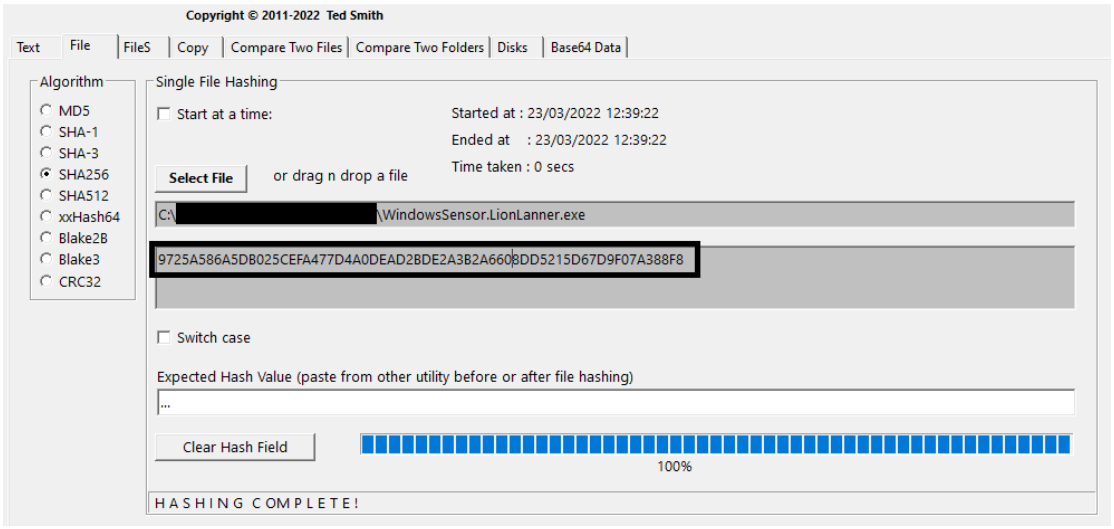

Ilustración 3 - Verificación hash del agente

Una vez comprobado el paquete de instalación del producto, se puede continuar con el proceso de instalación.

5. FASE DE INSTALACIÓN

5.1 INSTALACIÓN MANUAL POR INTERFAZ GRÁFICA (GUI)

En primer lugar, se deberá hacer doble *click* en el icono del instalador para comenzar con la instalación y será necesario tener permisos de administrador para comenzar con la misma. Una vez iniciada la instalación, el instalador muestra una ventana en la que requiere marcar la casilla de aceptación de la licencia y la política de privacidad, así como el CID del *tenant*.

En el CID (*Customer ID*) es necesario copiar el CID del *tenant* al que se conectará el agente instalado en el siguiente enlace: https://falcon.eu-1.crowdstrike.com, siguiendo la ruta: *"Hosts > Sensor Downloads"*.

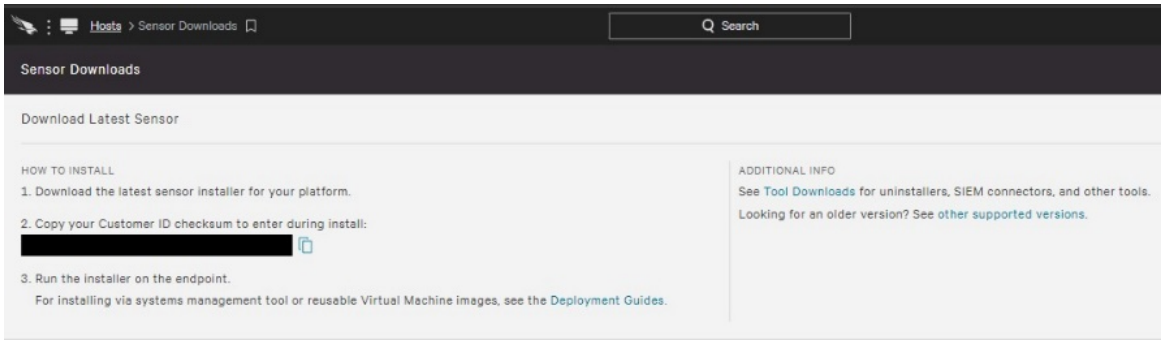

Ilustración 4 - Copia de CID

Una vez configurados los campos que requiere el instalador se procede a hacer *click* en el botón "*Install*" que se encuentra en la zona inferior derecha de la ventana.

Ilustración 5 - *Falcon Sensor Setup GUI*

Una vez finalizada la instalación, el instalador muestra una ventana donde confirma la finalización de la instalación de forma correcta. A continuación, hacer *click* en el botón "*Close*" para cerrar la ventana.

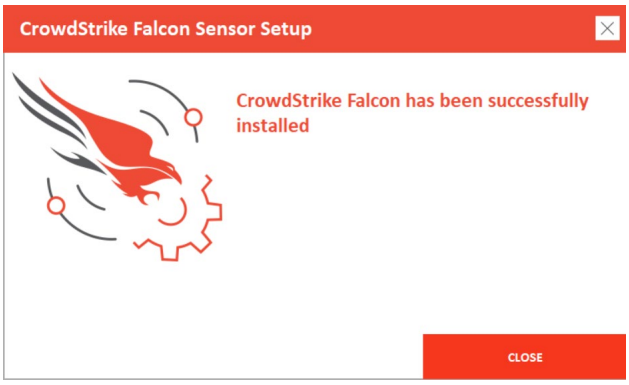

Ilustración 6 - Instalación finalizada GUI

5.2 INSTALACIÓN MANUAL A TRAVÉS DE LÍNEA DE COMANDO (CLI)

Para realizar la instalación por CLI, se debe ejecutar la consola de comando de Windows con permisos de administrador. Al igual que en la instalación por CLI se deberá proporcionar el CID, y la ruta donde se encuentra el instalador de Falcon. A continuación, se presentan los diferentes comandos de instalación posibles.

5.3 INSTALACIÓN SIN PROXY

Para realizar la instalación a través de línea de comandos sin un proxy configurado, se realizará con el siguiente comando (desatendida):

```
WindowsSensor.exe /install /quiet /norestart CID= XXXXXXXXXXXX
```

5.4 INSTALACIÓN CON PROXY

Para realizar la instalación a través de línea de comandos con un proxy configurado y utilizando el puerto 8080, se realizará con el siguiente comando (desatendida):

```
WindowsSensor.exe APP_PROXYNAME=proxy.demo.local APP_PROXYPORT=8080 /install /quiet /norestart CID= XXXXXXXXXXXX
```

5.5 INSTALACIÓN CON PROXY (URL)

Para realizar la instalación a través de línea de comandos con un proxy configurado y utilizando una URL "*http://intranet.server.local:8888/proxy.pac*" para la distribución del fichero *proxy.pac*, se realizará con el siguiente comando:

```
WindowsSensor.exe APP_PROXYNAME=proxy.demo.local APP_PROXYPORT=8080 /install /quiet /norestart CID= XXXXXXXXXXXX
```

5.6 INSTALACIÓN DESATENDIDA VDI

Para realizar la instalación a través de línea de comandos de manera desatendida en VDI, se realizará con el siguiente comando:

```
WindowsSensor.exe /install /quiet /norestart CID= XXXXXXXXXXXXX VDI=1
```

5.7 INSTALACIÓN CON "TAGS"

Para realizar la instalación a través de línea de comandos usando tags, se realizará con el siguiente comando:

```
WindowsSensor.exe /install /quiet /norestart CID=0 XXXXXXXXXXXX
GROUPING_TAGS="SERVIDORES_APLICACION_A,PREPRODUCCION"
```

NOTA: Se recomienda sustituir los *tags* por nombres identificativos especifico del entorno al que pertenece (departamento, oficina, sede, etc)

NOTA: Los *tags* se separan con comas, y pueden incluir caracteres alfanuméricos, guiones (-) y guiones bajos (_) así como "*forward slashes*" (/).

5.8 COMPROBACIÓN DE LA INSTALACIÓN

Una vez finalizado el proceso de instalación, independientemente del tipo de instalación (línea de comandos o interfaz gráfica), se deberá proceder a realizar una prueba de conexión del agente con la consola de Falcon.

Para ello, se ejecuta la consola de comandos de Windows (*cmd.exe*) con permisos de administrador y lanzar el siguiente comando: "*sc.exe query.csagent*" (sin comillas). Si la conexión funciona correctamente, devolverá el siguiente mensaje:

```
SERVICE_NAME: csagent
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Ilustración 7 - Comprobación de instalación

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Una vez que se ha desplegado el *software*, el equipo queda configurado con las opciones por defecto, pero con ciertas protecciones deshabilitadas. CrowdStrike recomienda realizar un duplicado de la política "*default*" y ajustarla a las necesidades de la organización a la que pertenece el *Tenant*.

A continuación, se muestra una tabla con las recomendaciones de configuración de las políticas de prevención de entornos Windows. En ella se observa el tipo de sensor, la categoría, una definición y la recomendación.

Tipo	Categoría	Definición	Recomendación
Sensor Capabilities	-	Notificar a los usuarios finales	Preferencia del cliente
Sensor Capabilities	-	Ejecutables desconocidos relacionados con la detección	Activado
Sensor Capabilities	-	Ejecutables desconocidos	Activado
Sensor Capabilities	-	Protección contra manipulaciones de sensores	Activado
Sensor Visibility	Visibilidad mejorada	Datos adicionales del modo de usuario	Activado
Sensor Visibility	Visibilidad mejorada	Solo intérprete	Activado
Sensor Visibility	Visibilidad mejorada	Motor (Visibilidad completa)	Activado
Sensor Visibility	Visibilidad mejorada	Supervisión de ejecución basada en scripts	Activado
Sensor Visibility	Visibilidad mejorada	Detecciones HTTP	Activado
Sensor Visibility	Visibilidad mejorada	Detección de exploits mejorada por hardware	Activado
Sensor Visibility	Visibilidad mejorada	Redactar detalles de detección de HTTP	preferencia del cliente

Tipo	Categoría	Definición	Recomendación
Sensor Visibility	firmware	Visibilidad profunda del BIOS	Activado
Next-Gen Antivirus	Aprendizaje automático en la nube	Antimalware en la nube - Detección	Agresivo
Next-Gen Antivirus	Aprendizaje automático en la nube	Cloud Anti-malware - Prevención	Moderado +
Next-Gen Antivirus	Aprendizaje automático en la nube	Cloud Adware & PUP - Detección	Agresivo
Next-Gen Antivirus	Aprendizaje automático en la nube	Cloud Adware & PUP - Prevención	Moderado +
Next-Gen Antivirus	Aprendizaje automático de sensores	Sensor Anti-malware - Detección	Agresivo
Next-Gen Antivirus	Aprendizaje automático de sensores	Sensor Anti-malware - Prevención	Moderado +
Next-Gen Antivirus	Al escribir	Detectar en escritura	Activado
Next-Gen Antivirus	Al escribir	Cuarentena al escribir	Activado
Next-Gen Antivirus	Cuarentena	Registro de cuarentena y seguridad	Activado
Malware Protection	Bloqueo de ejecución	Bloqueo personalizado	Activado
Malware Protection	Bloqueo de ejecución	Procesos sospechosos	Activado
Malware Protection	Bloqueo de ejecución	Operaciones de registro sospechosas	Activado

Tipo	Categoría	Definición	Recomendación
Malware Protection	Bloqueo de ejecución	Scripts y comandos sospechosos	Activado
Malware Protection	Bloqueo de ejecución	Amenazas basadas en inteligencia	Activado
Malware Protection	Bloqueo de ejecución	Controladores de kernel sospechosos	Activado
Behavior-based Prevention	Mitigación de exploits	Forzar ASLR	Activado
Behavior-based Prevention	Mitigación de exploits	Forzar DEP	Desactivado
Behavior-based Prevention	Mitigación de exploits	Preasignación de aspersión en pilas	Activado
Behavior-based Prevention	Mitigación de exploits	Asignación de página NULL	Activado
Behavior-based Prevention	Mitigación de exploits	Protección contra sobreescritura SEH	Activado
Behavior-based Prevention	Secuestro de datos	Eliminación de copia de seguridad	Activado
Behavior-based Prevention	Secuestro de datos	Criptowall	Activado
Behavior-based Prevention	Secuestro de datos	Cifrado de archivos	Activado
Behavior-based Prevention	Secuestro de datos	bloqueado	Activado

Tipo	Categoría	Definición	Recomendación
Behavior-based Prevention	Secuestro de datos	Acceso a los archivos del sistema	Activado
Behavior-based Prevention	Secuestro de datos	Instantánea de volumen - Auditoría	Activado
Behavior-based Prevention	Secuestro de datos	Instantánea de volumen - Proteger	Activado
Behavior-based Prevention	Comportamiento de explotación	Actividad de explotación de aplicaciones	Activado
Behavior-based Prevention	Comportamiento de explotación	Chopper Webshell	Activado
Behavior-based Prevention	Comportamiento de explotación	Descarga automática	Activado
Behavior-based Prevention	Comportamiento de explotación	Inyección de código	Activado
Behavior-based Prevention	Comportamiento de explotación	Ejecución de JavaScript a través de Rundll3	Activado
Behavior-based Prevention	Movimiento Lateral y Acceso de Credenciales	Omisión de inicio de sesión de Windows (teclas adhesivas)	Activado
Behavior-based Prevention	Movimiento Lateral y Acceso de Credenciales	Volcado de credenciales	Activado
Behavior-based Prevention	Remediación	Remediación automatizada	Activado

Tabla 2 - Configuración recomendada de políticas de prevención de Windows

6.1.1 CONFIGURACIÓN DE POLÍTICAS DE PREVENCIÓN TRIFÁSICA

A continuación, se define un proceso de tres fases para el despliegue de la configuración de la política de prevención, ofrece una trayectoria estructurada desde el despliegue inicial hasta la plena ejecución de las políticas de prevención.

Se recomienda no sobrepasar más de 45 días para completar el despliegue completo de los sensores en todos los puntos finales elegibles y pasar a la configuración de la FASE 2. La aplicación de la configuración de la FASE 3 a todos los *hosts* no debería demorarse más de 90 días después del despliegue.

6.1.1.1 FASE 0

En esta fase, se despliegan los agentes en los *endpoints* y se configuran todas reglas en modo monitorización excluyendo la regla de *ransomware* que se configura en modo bloqueo.

Estas configuraciones de políticas son adecuadas para un escenario de despliegue rápido cuando se comparte entorno con antivirus de terceros o HIPS preexistentes. Se recomienda la ejecución de esta fase durante el menor tiempo posible para permitir que la mayoría de las aplicaciones se ejecuten mientras se clasifican las detecciones y se abordan los falsos positivos según corresponda.

Se debe establecer la configuración del aprendizaje automático (ML) en solo detección para poder clasificar las detecciones de forma segura.

Las protecciones por comportamiento habilitadas para el *ransomware* y los IOA (*Indicator of attack*) tienen una baja tasa de falsos positivos, pero se ofrece una protección inmediata contra los *exploits* más peligrosos.

6.1.1.2 FASE 1

Una vez transcurrido el periodo de tiempo recomendado con la fase 0 y observado que las reglas establecidas en monitorización no generan alertas, se ampliaría la protección a la fase 1, pasando las reglas de monitorización a bloqueo y "*allow-listing*" de IOC's definidas manualmente y de las IOS's por defecto según fabricante.

Esta configuración provisional de la política ofrece una protección sólida, el fabricante aconseja deshabilitar o desinstalar ahora otros productos antivirus de terceros. Se debe ejecutar esta fase durante el menor tiempo posible para permitir que la mayoría de sus aplicaciones se ejecuten mientras sigue clasificando las detecciones y abordando los falsos positivos según corresponda.

Se debe:

- Establecer las detecciones de ML en modo "agresivo" y las prevenciones de ML en "moderadas".
- Habilitar configuraciones de prevención adicionales basadas en IOA.

6.1.1.3 FASE 2

Una vez transcurrido el periodo de tiempo en la fase 1 recomendado por el fabricante y se observa que el número de falsos positivos es bajo o inexistente, se amplía a la fase 2. En esta fase se activa la prevención antivirus a nivel "moderado" además de las protecciones contra exploits.

Se debe:

- Establecer las prevenciones de ML en modo "moderado" si se está seguro de la correcta aplicación de todas las exclusiones necesarias.
- Habilitar la prevención contra exploits.
- Habilitar la configuración de política de prevención basada en IOA recomendada restante.

6.1.1.4 FASE 3

Una vez transcurrido el periodo de tiempo en la fase 2, se amplía la protección a la fase 3. En esta fase se amplía la protección, activando la prevención contra ejecuciones de scripts de automatización y el servicio de cuarentena contra ficheros office con macros.

Se debe:

- Establecer las prevenciones de ML en modo "agresivo" si se está seguro de la correcta aplicación de todas las exclusiones necesarias.
- Habilitar la prevención contra ejecuciones de scripts automatizados.
- Habilitar la opción de cuarentena para el control de ficheros office con macros o ficheros altamente sospechosos.

6.1.1.5 MATRIZ DE LAS POLITICAS DE PROTECCIÓN

A continuación, se muestra la tabla con la matriz de las políticas de protección explicadas en los puntos anteriores. En ella se puede observar los tipos de protección, las diferentes configuraciones de cada tipo y el estado de la protección, según la fase y recomendación por el fabricante.

Tipo	Configuración	Fase 0	Fase 1	Fase 2	Fase 3
Sensor Capabilities	Notify End Users	Preferencia	Preferencia	Preferencia	Preferencia
	~~Unknown Executables/Unknown Detection-Related Executables~~	-	-	-	-
	Sensor Tampering Protection	✓	✓	✓	✓
Sensor Visibility	Additional User Mode Data	✓	✓	✓	✓
	Interpreter-Only	✓	✓	✓	✓
	Engine (Full Visibility)	✓	✓	✓	✓
	Script-Based Execution Monitoring	✗	✗	✓	✓
	HTTP Detections	✓	✓	✓	✓
	Redact HTTP Detection Details	Preferencia	Preferencia	Preferencia	Preferencia
	Hardware-Enhanced Exploit Detection	✓	✓	✓	✓
	BIOS Deep Visibility	✓	✓	✓	✓
Next-Gen Antivirus	Cloud Anti-malware - Detection	Moderate	Moderate	Aggressive	Aggressive
	Cloud Anti-malware - Prevention	Disabled	Disabled	Moderate	Moderate+
	Cloud Adware & PUP - Detection	Moderate	Moderate	Aggressive	Aggressive
	Cloud Adware & PUP -Prevention	Disabled	Disabled	Moderate	Moderate+
	Sensor Anti-malware - Detection	Moderate	Moderate	Aggressive	Aggressive
	Sensor Anti-malware - Prevention	Disabled	Disabled	Moderate	Moderate+
	Detect on Write	✗	✓	✓	✓
	Quarantine on Write	✗	✗	✓	✓
	Quarantine and Security Center Registration	✗	✗	✓	✓
Malware Protection	Custom Blocking	✗	✓	✓	✓
	Suspicious Processes	✗	✗	✓	✓
	Suspicious Registry Operations	✗	✗	✓	✓
	Suspicious Scripts and Commands	✗	✗	✓	✓
	Intelligence-Sourced Threats	✗	✓	✓	✓
	Suspicious Kernel Drivers	✗	✓	✓	✓
Behavior-based Prevention	Force ASLR	✗	✗	✗	✓
	Force DEP	✗	✗	✗	✗
	Heap Spray Preallocation	✗	✗	✗	✓
	NULL Page Allocation	✗	✗	✓	✓
	SEH Overwrite Protection	✗	✗	✓	✓
	Backup Deletion	✓	✓	✓	✓
	Cryptowall	✓	✓	✓	✓
	File Encryption	✓	✓	✓	✓
	Locky	✓	✓	✓	✓
	File System Access	✓	✓	✓	✓
	Volume Shadow Copy - Audit	✗	✓	✓	✓
	Volume Shadow Copy - Protect	✗	✗	✓	✓
	Application Exploitation Activity	✗	✓	✓	✓
	Chopper Webshell	✗	✓	✓	✓
	Drive-by Download	✗	✓	✓	✓
	Code Injection	✗	✓	✓	✓
	JavaScript Execution Via Rundll3	✗	✓	✓	✓
	Windows Logon Bypass ("Sticky Keys")	✗	✓	✓	✓
	Credential Dumping	✗	✓	✓	✓
	Advanced Remediation	✗	✓	✓	✓

Tabla 3 – Matriz fases de protección

6.2 AUTENTICACIÓN

En este apartado se incluye la información general sobre el acceso a la consola Falcon y su configuración.

NOTA: Hay que tener en cuenta que, en caso de necesitar abrir una incidencia con el soporte de Falcon es necesario utilizar Google Chrome, ya que es el navegador recomendado por el

fabricante. No obstante, la herramienta funcionaría en otros navegadores, aunque no sea lo recomendado por Falcon.

1. Para acceder a la consola, se debe navegar a la URL del cloud de Falcon:
   - **EU-1: *https://falcon.eu-1.crowdstrike.com***
2. Se introduce las credenciales en la pantalla de inicio de sesión.
3. En la siguiente pantalla, se ingresa el token 2FA. La primera vez que inicie sesión, se pedirá que se configure un token 2FA. Los proveedores comunes de 2FA incluyen *Duo Mobile, winauth, JAuth* y *GAuth Authenticator.*
4. La complejidad de las contraseñas de usuario no es configurable. Por defecto, los parámetros de robustez de contraseñas que permite el producto son los siguientes:
   - Longitud mínima de 12 caracteres.
   - No más de 2 caracteres repetidos seguidos.
   - La contraseña debe contener al menos 1 carácter de cada uno de estos conjuntos:
     - Números.
     - Letras mayúsculas.
     - Minúsculas.
     - Caracteres especiales:
       (~ ! @ #?$ % ^ & * ( ) - _ = + [ ] { } | ; : , . < > / ?).
   - No contener secuencias de 4 o más caracteres de estos conjuntos ordenados:
     - Numérico, como *0123* o *6789*
     - Alfabético, como *abcd* u *opqr*
     - Distribución del teclado, como *qwer* o *asdf*
   - No puede ser una de las 5 contraseñas utilizadas anteriormente por el usuario.
   - El usuario se bloquea si se introduce una contraseña errónea 5 veces. Esta configuración no se puede modificar ya que viene predefinida por el fabricante.

Además, se recomienda que las contraseñas tengan una vigencia de máximo 60 días.

La sesión de la consola se cierra a los 60 minutos de inactividad. Sin embargo, esta configuración se puede editar desde la sección del visor del *Dashboard* donde dice: "*stay signed in when viewing deshboards* (permanecer conectado al navegar en la sección *Dashboard*)". **En cualquier caso, se recomienda configurar el cierre de sesión con el menor tiempo posible de inactividad.**

6.3 ADMINISTRACIÓN DEL PRODUCTO

La gestión del producto se realiza de forma remota, vía navegador web HTTPS a través de las siguiente URL:

- **EU-1: *https://falcon.eu-1.crowdstrike.com***

6.3.1 CONFIGURACIÓN DE ADMINISTRADORES

Falcon, por defecto, tiene varios perfiles de administrador creados. Estos perfiles representan los diferentes tipos de acceso. Esta funcionalidad se puede aplicar a cualquier suscripción de producto Falcon:

- ***Falcon Console Guest*** es un rol de acceso limitado y solo con permisos de lectura. Los usuarios asignados a este rol pueden iniciar sesión en Falcon y ver la documentación y su propio perfil de usuario. También pueden acceder al Portal de soporte para revisar artículos de la base de conocimientos, leer la documentación del portal web y usar el chat para obtener ayuda automatizada.
- ***Falcon Administrator*** puede acceder a todas las funciones de la consola, con la excepción de ciertas funciones de RTR.
- ***Workflow Author*** puede crear y editar *workflows* (Flujos de trabajo).
- ***Dashboard Admin*** puede compartir y editar *Dashboards* personalizables compartidos.
- ***Prevention Policy Manager*** puede crear, modificar y eliminar directivas de prevención. Los usuarios con este rol también pueden ver paneles, administración de host, administración de detecciones, exclusiones de archivos y directivas de actualización de sensores (agentes).
- ***Desktop Support Analyst*** puede instalar/desinstalar sensores y agregar/administrar tokens de instalación. Los usuarios asignados a este rol también pueden ver las secciones: Administración de host, administración de detecciones, exclusiones de archivos y Paneles.
- ***Help Desk Analyst*** puede ver las secciones: Detecciones, administración de host, *tokens* de instalación, directivas de prevención, exclusiones de archivos, directivas de actualización de sensores y paneles.

La siguiente matriz muestra el conjunto de permisos asociados a cada perfil administrador:

Roles	Falcon Administrator	Falcon Security Lead	Falcon Analyst	Falcon Analyst - Read Only	Quarantine Manager	Endpoint Manager	Detections Exceptions Manager	Remediation Manager
Manage detections	Y	Y	Y	-	-	-	-	-
Manage exclusions	Y	-	-	-	-	-	Y	-
Manage quarantined files	Y	Y	Y	-	Y	-	-	-
Change prevention settings	Y	-	-	-	-	-	-	-
Manage custom IOCs	Y	-	-	-	-	-	Y	-
Manage sensor deployment	Y	-	-	-	-	Y	-	-
Reset users' credentials	Y	Y	-	-	-	-	-	-
Add/remove users	Y	-	-	-	-	-	-	-
Manage API credentials	Y	-	-	-	-	-	-	-
Enable/Disable Detections	Y	-	-	-	-	-	-	-
Share and edit shared customizable dashboards	Y	-	-	-	-	-	-	-
Manage Activity > Remediations	Y	-	-	-	-	-	-	Y
Manage host groups	Y	-	-	-	-	Y	-	-
Delete hosts	Y	-	-	-	-	-	-	-

Tabla 4 - Roles de usuario en *Falcon Prevent*

6.4 GESTIÓN DE USUARIOS

6.4.1 AGREGAR USUARIOS

La herramienta permite la creación manual de usuarios, a través de los siguientes pasos:

- Ir a *Falcon Users > User Management* en la consola de Falcon.
- Hacer clic en "*Add User*" en la parte superior derecha de la ventana
- En el diálogo que aparecerá, introducir la dirección de correo electrónico, el nombre y los apellidos del usuario. Si se tiene previsto habilitar el inicio de sesión único (SSO), la dirección de correo electrónico del usuario debe coincidir exactamente con la información de su IdP.
- Seleccionar los roles que se les asignarán al usuario. Sólo se mostrarán las funciones asociadas a las suscripciones de Falcon adquiridas, como *Falcon Prevent* o *Falcon Insight*.
- Haga clic en "*Add User*". Si el SSO no está habilitado en el entorno, CrowdStrike envía un correo electrónico automático al usuario, solicitando que se cree una contraseña de *Falcon* y se configure el 2FA. Si el SSO está habilitado, CrowdStrike no envía un correo electrónico automático al usuario.

6.4.2 ELIMINAR USUARIOS

Para eliminar usuarios, se debe acceder con un usuario con un rol administrativo, como "*Falcon Administrator*" o "*Falcon Intel Admin*". Un usuario con un rol "*Falcon Security Lead*" puede restablecer las contraseñas de los usuarios y los tokens de 2FA, pero no puede gestionar los usuarios o las funciones de los usuarios.

Para eliminar usuarios:

- Hacer clic en "*Falcon Users > User Management*" en la consola de Falcon. También se puede eliminar un usuario haciendo clic en el menú de los tres puntos dentro de los detalles del usuario.
- Junto al usuario que se desea eliminar, hacer clic en el menú de tres puntos y seleccionar "*Delete user*".
- Cuando aparezca el mensaje de confirmación, hacer clic en "*Delete*".

6.4.3 MODIFICAR ROL DE USUARIOS

Es posible modificar el rol de un usuario en cualquier momento siguiendo los siguientes pasos, desde una cuenta de usuario con permisos de "*Falcon Administrator*" o "*Falcon Intel Admin*".

- Hacer clic en "*Falcon Users > User Management*" en la consola de Falcon.
- Junto al usuario en cuestión, hacer clic en el menú de tres puntos y seleccionar "*View user details*".

- Hacer clic en "*assign roles*" y de la lista que se muestra, seleccionar los roles que se desea asignar.
- Finalmente hacer clic en "*assign*".

6.5 SERVIDORES DE AUTENTICACIÓN

6.5.1 SINCRONIZAR FALCON CON AZURE

La herramienta tiene la posibilidad de integrar *Azure Active Directory* para poder usar las mismas credenciales. Los requisitos para ello son:

- Necesario un usuario con rol de "*Falcon Administrator*" u "*Horizon Admin*".
- Rol de Azure AD de administrador global (consulte los detalles de Microsoft aquí).
- Función de propietario de sus suscripciones específicas (consulte los detalles de Microsoft aquí)

Antes de iniciar la integración estándar, se debe ir a la página de registro guiado:

- Ir a *Falcon > Cloud Security > Cloud Accounts Registration*.
- Clic en "*Add new account*" en la pestaña Azure.
- Seleccionar "*Guided registration* "como método de registro.

"*Guided registration*" en *Falcon Horizon* muestra instrucciones paso a paso que se deben seguir en Azure AD.

NOTA: Cada paso realiza un cheque de validación para comunicar si el paso se ha realizado correctamente antes de pasar al siguiente. Si algo no funciona, Falcon Horizon indica con precisión el motivo y la solución de error.

6.5.2 CONECTAR CON AZURE

Como se indica en la siguiente imagen, se debe crear un *App Registration* en *Azure* o elegir uno existente.

Falcon Horizon accede a los recursos de Azure utilizando un servicio de aplicación, por lo que es necesario tener un *App Registration* en su lugar que sirva como tal.

NOTA: Los números de los pasos en la tabla corresponden a las opciones que se muestran en la imagen.

Numero de paso	Descripción
1	En este paso, se notifica a *Falcon Horizon* que se está creando un nuevo *App Registration* en su tenant de Azure usando el *Microsoft Azure Portal*, o que se utiliza un *App Registration* de un *tenant* previamente integrado en *Falcon Horizon* y quiere hacer algún tipo de cambios en él.

2	Este punto se muestran las instrucciones para crear un nuevo *App Registration* en el *tenant* de *Azure*.
3	Este paso se necesita el ID de la aplicación y el ID del *Tenant* de registro de la *App Registration* creado. Esta información es para que CrowdStrike pueda generar un certificado necesario en el siguiente paso. El ID del *Tenant* se puede encontrar en: *Microsoft's documentation*.
4	La comunicación segura entre *Falcon Horizon* y *Azure App Registration* en el Tenant se realiza mediante la API de *Microsoft Graph*, por lo que necesita autenticarse con credenciales seguras. En el siguiente paso, CrowdStrike genera un certificado que se debe descargar en la máquina local y para después cargar en *Azure App Registration*. Este certificado se convierte en las credenciales para *Microsoft Graph API*.
5	Estas son las instrucciones para subir el certificado a tu *Azure App Registration* como *client secret*. Una vez más, este certificado sirve como credencial para la API de *Microsoft Graph*. Una vez terminada la carga del certificado, hacer clic en "*validate*" y comprobar que la conexión funciona correctamente.

Tabla 5 - Pasos conexión *Falcon – Azure*

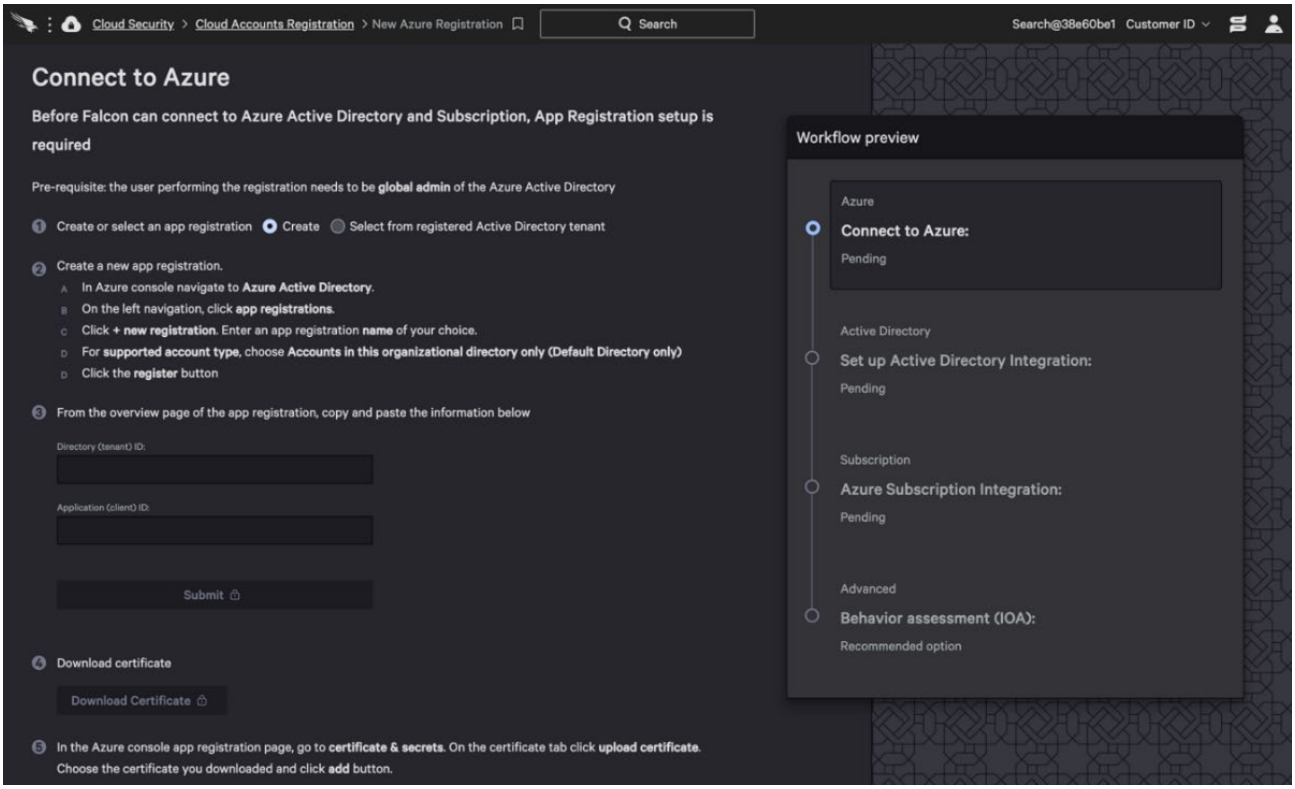

Ilustración 8 - Comprobación de instalación

6.5.3 INTEGRACIÓN AZURE ACTIVE DIRECTORY

En esta página se muestra cómo conceder a *Falcon Horizon* permisos de "*Graph* API" de solo lectura en Azure. La detección de configuraciones poco seguras en el Directorio Activo es fundamental para mantener la estructura de seguridad del entorno de Azure.

Con los permisos de Microsoft Graph API de sólo lectura, Falcon Horizon supervisa y detecta las configuraciones poco seguras de Active Directory.

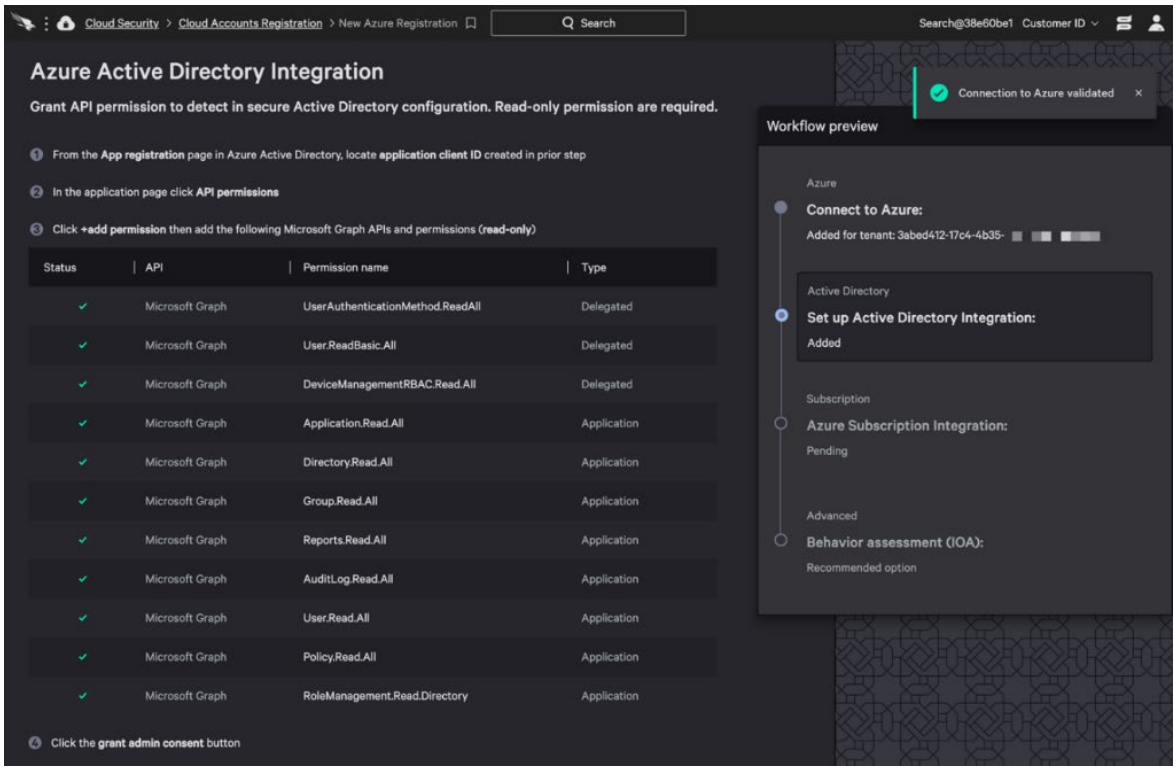

Ilustración 9 - Integración Azure AD

A continuación, se definen los pasos a seguir según recomienda el fabricante para la integración con *Active Directory*.

Numero de paso	Descripción
1-3	A pesar de que *App Registration* y el certificado están configurados, *Falcon Horizon* no puede acceder a su Azure AD hasta que habilite los permisos en *Graph API* de sólo lectura. Durante estos pasos, Se está configurando para conceder a Azure varios permisos de *Microsoft Graph API* a su *App Registration* previamente configurado. Los permisos necesarios son de sólo lectura. NOTA: Si ya se han añadido los permisos y la columna de Estado muestra el *check* verde en la columna de "*status*", se puede omitir esta página.

4	Este paso permite conceder los permisos de sólo lectura en Azure, mientras que el botón "*Validate*" en *Falcon Horizon* sólo valida que se hayan configurado correctamente dichos permisos. Una vez concedidos los permisos enumerados en Azure, hacer clic en "*Validate*" para comprobar si se han aplicado correctamente. *Falcon Horizon* muestra el estado de éxito o fracaso de cada permiso de manera individual.

Tabla 6- Pasos a seguir para la Integración Azure AD

6.5.4 INTEGRACIÓN DE LA SUSCRIPCIÓN DE AZURE

Esta página indica cómo conceder roles de solo lectura a las diferentes subscripciones.

La detección de configuraciones incorrectas en las subscripciones de Azure es también una parte crítica del mantenimiento de la estructura de seguridad del entorno de Azure. Con los roles "*Identity and Access Management (IAM)",* Falcon Horizon supervisa y detecta configuraciones de recursos no seguras en las subscripciones de Azure.

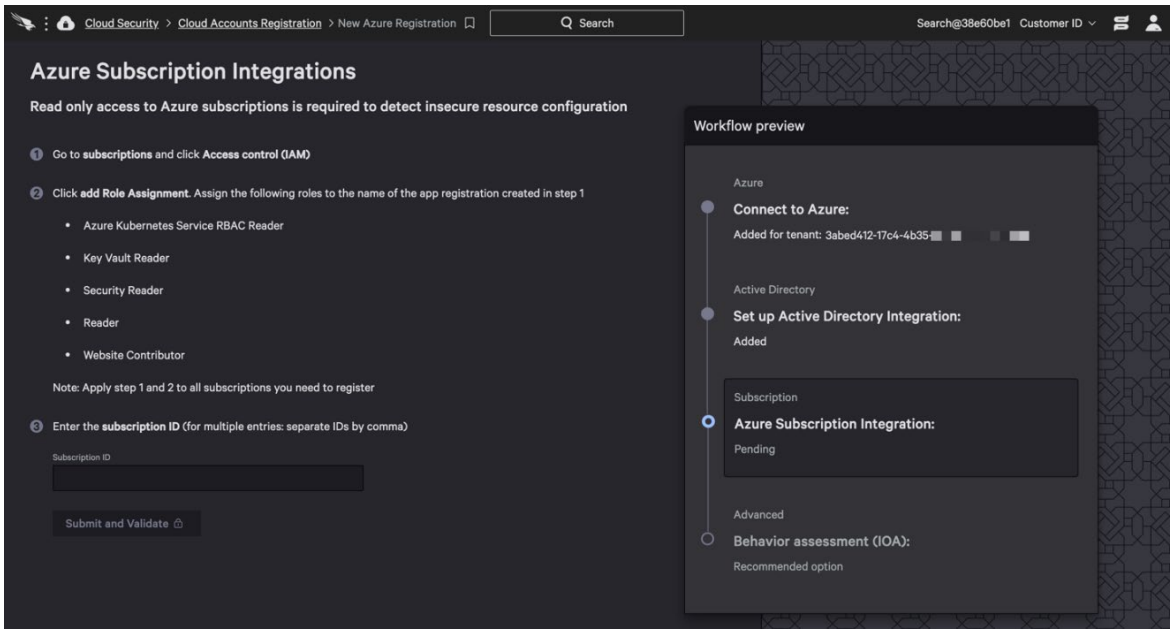

Ilustración 10 - Integración subscripciones Azure

A continuación, se definen los pasos a seguir según recomienda el fabricante para la integración con las subscripciones de Azure:

Numero de paso	Descripción
1-2	Estos pasos necesitan que se añadan los roles de sólo lectura al *App Registration* para cada una de las suscripciones de Azure que se quieran monitorizar. Esto se hace utilizando IAM.

Numero de paso	Descripción
	Nota: Para realizar estos pasos con éxito, se requiere que el usuario sea el propietario de la suscripción (es decir, para esas suscripciones se debe tener el permiso de propietario en Azure).
3	Finalice la integración especificando uno o más IDs de suscripción de Azure que pertenezcan al *Tenant* que tiene su *App Registration* del paso anterior. A estos se les asignarán evaluaciones de configuración. Los IDs de suscripción se pueden encontrar en la página de suscripciones en el Portal de Microsoft Azure. Cada ID es un número de identificación de 32 dígitos que tiene varios guiones (-) para hacerlos más fáciles de leer. Hay que incluir los guiones y separar las suscripciones múltiples con comas. Al hacer clic en "*Submit*" y "*Validate*", se registran las suscripciones en *Falcon Horizon*. Nota: Debido a los retrasos en Microsoft Azure entre el momento en que se añaden la asignación de funciones y el momento en que se provisionan realmente dichas asignaciones, es posible que se tenga que esperar varios minutos al hacer clic en "*Submit*" y "Validate" y obtener un resultado satisfactorio para todos los ID de las suscripciones. También, se puede hacer clic de forma periódica hasta que todas las suscripciones se añadan con éxito. Cada una de sus suscripciones a Azure está asociada exactamente a un tenant de Azure. Es posible que tenga varias suscripciones asociadas a un Tenant, pero también es posible que tenga varios Tenant. En cualquier caso, aquí sólo se enumeran las suscripciones para un Tenant.

Tabla 7 - Pasos subscripciones Azure

Falcon Horizon ahora monitorea las configuraciones incorrectas y verifica el cumplimiento de las políticas elegidas.

NOTA: Las actualizaciones pueden tardar hasta dos horas en estar disponibles.

Esto es lo que se ha realizado:

- Se Creó un Registro de aplicaciones de Azure como principal servicio de aplicaciones para Falcon Horizon.
- Se ha añadido un certificado en Azure que Falcon Horizon utiliza para el acceso del cliente.
- Se ha dado a la App Registration permisos y roles de sólo lectura para que Falcon Horizon los utilice.
- Se ha especificado a Falcon Horizon qué suscripciones de Azure debe supervisar.

6.6 GESTIÓN DE CERTIFICADOS

El sensor Falcon utiliza TLS 1.2 para comunicarse con la nube CrowdStrike. No se admiten otros protocolos, incluidos SSL o versiones anteriores de TLS.

El sensor Falcon hace uso de certificados. Se recomienda consultar el siguiente link para verificar que el host confía en la autoridad de certificación de CrowdStrike.

Los hosts deben conectarse a la nube de *CrowdStrike* en el puerto 443 durante la instalación inicial. Si su entorno restringe el acceso a Internet, permita el tráfico hacia y desde nuestros FQDN o direcciones IP.

El sensor Falcon utiliza el anclaje de certificados para defenderse de los ataques "*man-in-the-middle*". Algunas configuraciones de red, como la inspección profunda de paquetes, interfieren con la validación de certificados. Por tanto, se debe desactivar "*deep packet inspection*" (también llamada "interceptación HTTPS" o "interceptación TLS") o configuraciones de red similares.

Después de la instalación del agente, éste abre una conexión TLS permanente a través del puerto 443 y mantiene esa conexión abierta hasta que se apaga el punto final o se termina la conexión de red.

Dependiendo del entorno de red, es posible que se tenga que permitir el tráfico TLS a través del puerto 443 entre la red y las direcciones de red de la nube de Falcon:

Si se requiere autorización por dirección IP en lugar de FQDN, consultar Direcciones IP en la nube de Falcon para obtener una lista de las direcciones IP utilizadas.

6.7 AUDITORÍA

Falcon dispone en la sección de auditoría de varios tipos de logs:

- ***Machine-Learning Prevention Monitoring***: este panel muestra el malware que se habría bloqueado en el entorno durante el periodo de tiempo seleccionado en función de las diferentes configuraciones de Prevención de Aprendizaje Automático (Cauteloso, Moderado, Agresivo o Extra Agresivo).
- ***Falcon UI Audit Trail***: proporciona información de referencia sobre los cambios realizados en la configuración: quién lo ha hecho, sobre qué, etc…
- ***API Audit Trail***: proporciona los registros de auditoría de las acciones realizadas a través de las APIs de Falcon basadas en OAuth2.
- ***Prevention Policy Audit Trail***: muestra el registro de auditoría de todas las políticas.
- ***Prevention Policy Debug***: se utiliza para depurar problemas con la configuración de la prevención que no se ha establecido.
- ***Sensor Visibility Exclusions Audit***: este panel muestra las rutas de los archivos desactivadas de la visibilidad de los sensores y que han tenido ejecuciones de procesos

en ellas durante el periodo de tiempo seleccionado. Se recomienda examinar las rutas de archivos que se muestran para asegurarse de que efectivamente se han excluido de toda visibilidad de los sensores (es decir, si el *malware* u otros ataques se dirigen a estas rutas de archivos, no se registrarán, detectarán o evitarán).

6.8 REGISTRO DE EVENTOS

La funcionalidad "*Events Data Dictionary*" proporciona información de referencia sobre los eventos encontrados, según la configuración de las políticas de prevención habilitadas. Estos eventos se pueden encontrar en: *Investigate > Event Search. Event Search*.

Ya que el motor de búsqueda de eventos de Falcon funciona con la tecnología Splunk, se recomienda visitar el siguiente enlace para obtener más información acerca del funcionamiento de Splunk.

Para ver las diferentes tipos de registros, se recomienda consultar: Events Data Dictionary en el portal de documentación de Falcon.

6.9 RETENCIÓN DE EVENTOS

Existen varias configuraciones de retención de eventos dentro de la plataforma CrowdStrike:

a) Los sumarios de detección se conservan durante un año. Se accede bajo demanda a los metadatos relacionados con todas las amenazas generadas desde la plataforma Falcon.

b) Se proporciona una retención de 90 días para los detalles de la detección. Se accede bajo demanda a los detalles forenses completos de todas las amenazas detectadas por la plataforma Falcon.

c) Se proporciona una retención de 1 año para los datos almacenados en el gráfico de indicadores de CrowdStrike, incluidas las ejecuciones de procesos, las búsquedas de dominios y las conexiones de red.

d) Se proporciona una retención de 7 días (también están disponibles múltiples opciones de retención de 15, 30 y 90 días con costes adicionales) para la telemetría sin procesar como parte de *Threat Graph Standard*. Se accede bajo demanda a un registro histórico completo de más de 400 tipos de eventos de puntos finales, utilizado para la detección retrospectiva, la búsqueda de amenazas y las investigaciones. Existen opciones para conservar hasta 90 días de telemetría sin procesar si es necesario.

e) También existe la opción de enviar externamente los datos de telemetría sin procesar para utilizarlos en un almacén de datos local o en un lago de datos para el almacenamiento indefinido de esos datos a través de *Falcon Data Replicator*. Estos datos también pueden utilizarse para la correlación con otros tipos de registros recopilados (es decir, SIEM) si se desea.

7. FASE DE OPERACIÓN

7.1 MONITORIZACIÓN DE INCIDENTES

En la operativa habitual de *Falcon CrowdStrike* se debe:

a) **Revisar las alertas**. Estas están ordenadas por severidad: Critica, alta, media, baja e informativa.

b) **Resolver lo antes posible las alertas de tipo CRITICA**, siguiendo con las de tipo ALTA, posterior con las de tipo MEDIA y finalmente las de tipo BAJA e INFORMATIVAS.

c) **Realizar la exportación de *logs*** y enviar a un SIEM o *Syslog*.

d) En caso de tener una detección, analizar para **comprobar el verdadero origen de la amenaza.**

e) A través de los "*Threat Indicators (Technique)*", **analizar aquellos binarios** que han lanzado o no una detección (firmas, *Deep Learning*, *exploits*, etc…) y son **considerados sospechosos**. Tanto el análisis de RCA como los detalles de EDR permitirán realizar una limpieza preventiva del binario que, si bien no ha detonado una amenaza, tras los pasos de análisis se descubre sospechoso e inadecuado, pudiendo de forma centralizada realizar la limpieza global.

f) Verificar que los agentes están **correctamente actualizados**.

g) Verificar que los **administradores disponen de MFA**.

h) Verificar que el **modo de operación seguro** sigue operativo de acuerdo con su configuración inicial.

i) **Agregar exclusiones** para silenciar las detecciones de aprendizaje automático basadas en sensores. Se puede configurar las exclusiones para que se apliquen a todos los hosts o a grupos específicos de hosts. Para más información sobre la configuración, se recomienda consultar: *Detection Management*.

7.2 ARCHIVOS EN CUARENTENA

El sensor Falcon puede poner en cuarentena los archivos sospechosos basándose en sus políticas de prevención. Cuando el sensor detecta un archivo sospechoso que intenta ejecutarse, el archivo es codificado, renombrado y movido a un directorio de cuarentena en el propio host.

Para utilizar la cuarentena, primero se debe habilitar la función a través de una política de prevención. Se puede revisar y tomar medidas sobre los archivos en cuarentena mediante la supervisión de las detecciones.

El sensor solo pone en cuarentena los archivos binarios y los archivos *PowerShell*. Si hay archivos que no se quieren poner en cuarentena y enviar a la nube de *CrowdStrike*, se recomienda configurar una exclusión. Para más información, consultar: Exclusiones.

7.3 EXCLUSIONES

Si Falcon está mostrando alertas que se consideran falsos positivos, se pueden crear exclusiones para evitar este tipo de detecciones/bloqueos que tengan relación con las alertas detectadas.

7.3.1 ANTES DE EMPEZAR

Las exclusiones se aplican a los hosts en función de su pertenencia a un grupo. Es necesario configurar los grupos de hosts antes de crear una exclusión. Para más información, se recomienda visitar la sección Gestión de grupos de hosts.

Las exclusiones permiten crear una lista de permitidos específica, pero no es la única forma de ajustar las detecciones que se producen. Se recomienda revisar la configuración de la política de prevención para ver si alguna política está configurada a un nivel más agresivo que el recomendado por las mejores prácticas del fabricante. Estas políticas podrían desencadenar ciertas detecciones sobre la actividad que no se necesita visualizar. Para obtener más información, consultar la configuración de la política de prevención.

7.3.2 CONOCER LAS EXCLUSIONES

Ocasionalmente, Falcon puede detectar o impedir actividades que se desean permitir en el entorno. Al crear exclusiones, se puede evitar que se vean detecciones que no se desean ver, y permitir procesos que de otra manera se impedirían.

Las exclusiones que se crean forman una lista permitida que define explícitamente la actividad de confianza conocida de la organización.

Se pueden crear los siguientes tipos de exclusiones:

Tipo de Exclusión	Descripción	¿Logs de eventos?
Machine learning (ML) exclusion	Para rutas de archivo conocidas, detener todas las detecciones y prevenciones basadas en ML o impedir la subida de archivos a la nube de CrowdStrike.	Si
Indicator of attack (IOA) exclusion	Interrumpir todas las detecciones y prevenciones de comportamiento para una IOA que se basa en una detección generada por CrowdStrike	Si
Sensor visibility exclusion	Para las rutas de archivos de confianza que desee excluir de la supervisión de los sensores, disminuir la recogida de eventos de los sensores y detenga todas las detecciones y prevenciones asociadas.	La mayoría de los eventos no se registran
	Utilizar las exclusiones de visibilidad de los sensores con extrema precaución. Los posibles ataques y el malware asociados a los archivos excluidos no se registrarán, ni se detectarán ni tampoco se evitarán.	

Tabla 8 - tipos de exclusiones

La información sobre la configuración de cada tipo de exclusión se puede consultar en: Exclusion type.

7.4 RESPUESTA EN TIEMPO REAL

7.4.1 RESPUESTA EN TIEMPO REAL

La respuesta en tiempo real permite ejecutar comandos en el host de Windows directamente desde la consola de Falcon. La respuesta en tiempo real proporciona opciones más sofisticadas de respuesta a incidentes que la propia red que contiene un host, y permite la conexión a un host en línea inmediatamente desde cualquier lugar.

Se puede utilizar la respuesta en tiempo real para realizar muchas tareas comunes de respuesta y reparación, entre otras son:

- Listar procesos en ejecución y matar procesos
- Mostrar las conexiones de red
- Navegar por el sistema de archivos, obtener o eliminar archivos y realizar muchas operaciones del sistema de archivos
- Cargar archivos
- Reiniciar o apagar remotamente un *host*
- Gestionar y ejecutar sus propios scripts o ejecutables personalizados
- Capacidades adicionales para hosts Windows
- Recuperar volcados de memoria
- Consultar, crear o modificar claves del registro
- Recopilar registros de diagnóstico e información de estado sobre un host

Para más información, visitar: Real Time Response en la documentación del fabricante.

7.4.2 AISLAR UN *HOST* DE LA RED

Desde el panel de control de un host o de una detección, se puede restringir el servicio de red de un host para aislarlo de toda la actividad de la red. Para cambiar el estado de contención de un host, se puede hacer clic en la opción *network containment option* en el panel de control del host. Las opciones disponibles son las siguientes:

- ***Network Contain***: Hacer clic para aislar un host de la red
- ***Lift Containment***: Hacer clic para levantar el aislamiento de un host.
- ***Lift Containment Pending***: El estado está pendiente de pasar de un estado aislado a un estado sin aislamiento.
- ***Containment Pending***: El estado está pendiente de pasar de no aislado a aislado.

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la firma del instalador			
Instalación en un entorno seguro, con *Update Cache* y un *Message Relay*			
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de operación seguro activado según recomendaciones			
Revisión políticas de prevención de amenazas			
Revisión de políticas de control de dispositivos			
Revisión de políticas de control de navegación			
Revisión de políticas del firewall de Windows			
Revisión de políticas de control de aplicaciones			
Revisión de políticas de control de fuga de datos			
Activación de la autenticación multi-Factor			
Revisión de política de ejecutables desconocidos			
Revisión de política de ejecuciones basadas en scripts			
Revisión de política de detecciones HTTP			
Revisión de política de visibilidad profunda de la BIOS.			
Revisión de política de “Cloud Anti-malware”			
Revisión de política de “Sensor Anti-malware”			

ACCIONES	SÍ	NO	OBSERVACIONES
Revisión de política de detecciones de escritura			
Revisión de política de cuarentena y seguridad			
Revisión de política se scripts y comandos sospechosos			
Revisión de política de amenazas basadas en inteligencia			
Revisión de política de Criptowall			
Revisión de política de secuestro de datos			
Revisión de política de acceso a los archivos del sistema			
Revisión de política de explotación de aplicaciones			
Revisión de política de movimiento lateral y acceso de credenciales			
Revisión de política de remediación automatizadas			
Revisión de política de volcado de credenciales			
Revisión de política de Ejecución de JavaScript a través de Rundll3			
Revisión de política de Chopper Webshell			

9. REFERENCIAS

[REF1] *Falcon Documentation*
https://falcon.eu-1.crowdstrike.com/documentation

10.ABREVIATURAS

AD	*Active Directory*
EDR	*Endpoint Detection and Response*
FQDN	*Fully Qualified Domain Name*
HTTPS	*Hyper Text Transfer Protocol Secure*
IOA	*Indicator of attack*
MFA	*Multi Factor Authentication*
ML	*Machine Learning*
RCA	*Root Cause Analysis*
SIEM	*Security Information and Event Management*
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL