Guía de Seguridad de las TIC
CCN-STIC 1019

Procedimiento de Empleo Seguro
CYNET XDR



Noviembre 2026

Edita:





CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 9
6 FASE DE CONFIGURACIÓN 11
6.1 MODO DE OPERACIÓN SEGURO 11
6.2 AUTENTICACIÓN 15
6.3 ADMINISTRACIÓN DEL PRODUCTO 15
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 15
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 15
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 16
6.5 GESTIÓN DE CERTIFICADOS 16
6.6 SERVIDORES DE AUTENTICACIÓN 16
6.7 SINCRONIZACIÓN 16
6.8 ACTUALIZACIONES 16
6.9 AUTO-CHEQUEOS 17
6.10 ALTA DISPONIBILIDAD 17
6.11 AUDITORÍA 18
6.11.1 REGISTRO DE EVENTOS 18
6.11.2 ALMACENAMIENTO REMOTO 19
6.12 BACKUP 19
7 REFERENCIAS 20
8 ABREVIATURAS 21

ÍNDICE DE TABLAS

Tabla 1: Requisitos mínimos 7

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Certificado de la página. 6
Ilustración 2. Descarga del agente. 6
Ilustración 3. Instalación individual en un sólo equipo o endpoint. 9
Ilustración 4. Instalación del agente 10
Ilustración 5. Comprobación de funcionamiento correcto del agente 10
Ilustración 6. Sección para configurar el agente 11
Ilustración 7. Grupo a modificar 11
Ilustración 8. Opciones a habilitar 11
Ilustración 9. Opciones del agente a habilitar 12
Ilustración 10. Definición de la contraseña de desinstalación 12

Ilustración 11. Configuración de la misma contraseña de desinstalación en la consola 13
Ilustración 12. Activación de opción de análisis 13
Ilustración 13. Activación de opción de análisis 13
Ilustración 14. Activación de listas "Allow" 13
Ilustración 15. Activación de alertas por e-mail.....14
Ilustración 16. Activación de opciones de análisis 14
Ilustración 17. Configuración de usuario señuelo 15
Ilustración 18. Activación de las actualizaciones automáticas.....17

1 INTRODUCCIÓN

El servicio, **Cynet 360 XDR**, es la solución de Cynet que permite detectar y proteger frente a amenazas y malware en los ordenadores donde es instalado.

El servicio se divide en los siguientes componentes:

a) **Cynet XDR Endpoint**, o el "**agente**", es un componente software que se instala directamente en el ordenador o máquina que va a monitorizar y proteger. Supervisa la máquina en la que está instalado, monitorizando procesos, conexiones, archivos, entre otras funciones, continuamente en busca de amenazas para poder bloquearlas si son encontradas.

b) **Cynet XDR Console**, o la "**consola**", es una plataforma en la nube que permite a los administradores visualizar y gestionar las máquinas monitorizadas por los agentes, desde esta consola se puede comprobar la seguridad de cada ordenador, las amenazas detectadas en este y realizar diferentes acciones para gestionar la amenaza de manera remota.

   a) **Cynet XDR Backend**, integrado en la consola, permite analizar los datos recibidos del agente para determinar si se encuentran amenazas y clasificarlas. Este componente, a su vez, se divide en los siguientes:

      a. *Cynet Protector*: Ofrece tecnologías de sensores para detectar y prevenir amenazas en todo el entorno.

      b. *Cynet Responder*: Investiga las amenazas y coordina las acciones de respuesta y corrección.

      c. *Cynet Correlator*: Permite la integración y correlación de datos de alertas y actividades en incidentes procesables para descubrir amenazas en todo el entorno.

      d. *Cynet Sensor Fusion*: Recopila información de Cynet Endpoint y la distribuye a las funciones definidas anteriormente.

2 OBJETO Y ALCANCE

El presente documento recoge el Procedimiento de Empleo Seguro del servicio Cynet 360 XDR, incluyendo los siguientes componentes con sus respectivas versiones; en el caso de la consola la versión no aplica:

a) Cynet XDR Endpoint v4.29.999.19020.

b) Cynet XDR Console N/A.

El producto **Cynet 360 XDR** ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF1].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del servicio.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del servicio.

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

La consola, al estar desplegada en la nube íntegramente por Cynet, no requiere de una entrega o instalación previa. El único requerimiento es la adquisición de una licencia / suscripción a través del formulario disponible en la página referenciada en [REF2]

Para acceder a dicha página, se debe verificar que el protocolo es HTTPS y que el certificado SSL es válido, tal y como se aprecia en la Ilustración 1.

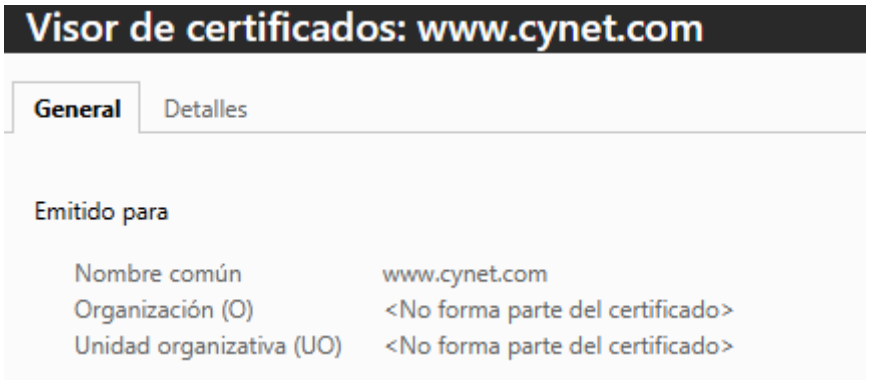


Ilustración 1. Certificado de la página.

Una vez adquirida la licencia para el uso del servicio, el usuario administrador debe iniciar sesión en la consola de Cynet [REF3], desde la cual será redirigido a la consola principal, cuyo enlace debe tener el formato *https://mssp-v3.cynet.com/**, *https://signup.cynet.com* o *https://mssp.cynet.com/**.

En esta página, es posible descargar el agente siguiendo los pasos mostrados en la Ilustración 2 para su despliegue en los equipos de la organización.

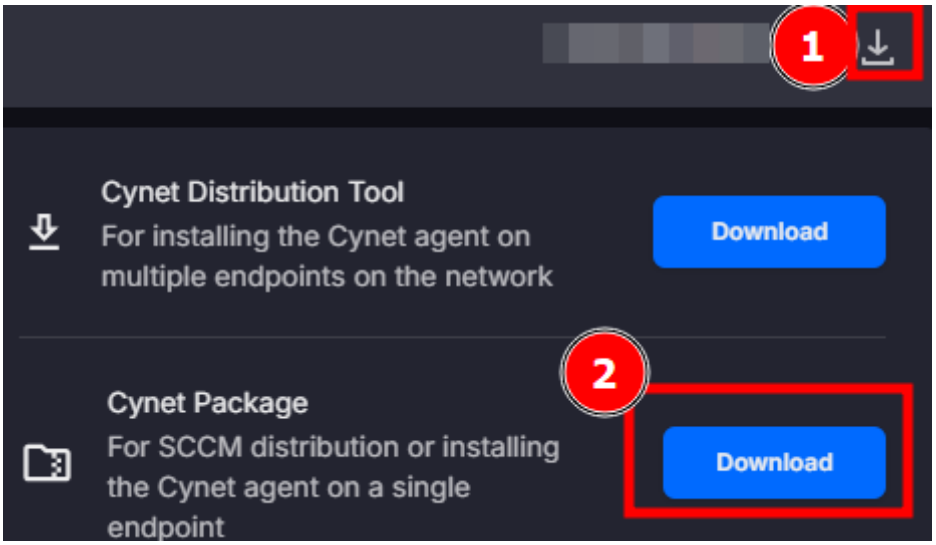


Ilustración 2. Descarga del agente.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Para este Procedimiento de Empleo Seguro, no se considera necesaria la configuración de ningún entorno de instalación seguro para la consola, porque está desplegada por parte de Cynet en un entorno cuyo acceso estará limitado a un conjunto de personas que posea autorización expresa.

Por su parte, el agente de Cynet debe instalarse en el sistema operativo Windows.

La cualificación contempló el uso de una máquina virtual con los siguientes requisitos mínimos:

Tipo	Requisitos mínimos
Hardware	• 4 CPU (1 socket, 4 cores) • Memoria: 4 GB • La capacidad del disco duro de 100 GB
Software	Windows 10 Pro, versión 22H2, OS Build 19045.5011 o superior
Topología	Requisitos de nodo simple: • Una máquina con los requisitos listados arriba. • Una dirección IP en una red con acceso a internet para que el agente pueda comunicarse con la consola.

Tabla 1: Requisitos mínimos

Los requisitos recomendados por Cynet pueden consultarse en la referencia [REF4].

Los Sistemas Operativos soportados por Cynet pueden consultarse en la referencia [REF5]. Sin embargo, se recomienda el uso de Windows 10 Pro, versión 22H2, OS Build 19045.5011 o superior.

4.3 REGISTRO Y LICENCIAS

La activación de servicios y usuarios para el acceso al servicio las proporciona el propio fabricante a través de los medios referenciados en la sección 4.1 ENTREGA SEGURA DEL PRODUCTO.

4.4 CONSIDERACIONES PREVIAS

Antes de instalar el agente de Cynet, es necesario configurar el doble factor de autenticación para las cuentas de administración en la consola de Cynet, para ello se deben seguir los siguientes pasos:

a) Inicia sesión en la consola de Cynet con una cuenta de administrador.

b) Cuando la consola de Cynet muestre un código QR y pida un código, se deberá escanear el código QR con una aplicación de autenticación como, por ejemplo, “Google Authenticator”.

c) Una vez escaneado el código QR en la aplicación seleccionada, se deberá introducir el código generado por esta aplicación en la consola de Cynet.

d) Se debe verificar que, al introducir este código, la consola debería permitir acceso a la web.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El entorno de operación aplicable para este servicio está formado por los siguientes componentes:

- Equipos con el componente Cynet XDR Endpoint (agente) instalado en él.
- Consola de administración (Cynet XDR Console), desplegada en la nube.

5 FASE DE INSTALACIÓN

La consola no requiere de instalación para este Procedimiento de Empleo Seguro.

Para el agente, se pueden seguir dos métodos:

1. A través de la herramienta “Cynet Distribution Tool”, para hacer una instalación distribuida en diferentes equipos en la red de la organización. Para seguir esta instalación, se debe revisar la guía definida en [REF6].
2. A través de la instalación en equipos individuales. Se recomienda instalar el agente manualmente seguir los siguientes pasos para la instalación:

a) Se debe presionar el botón “Install” y seleccionar el botón “Download” para la opción “Cynet Package”.

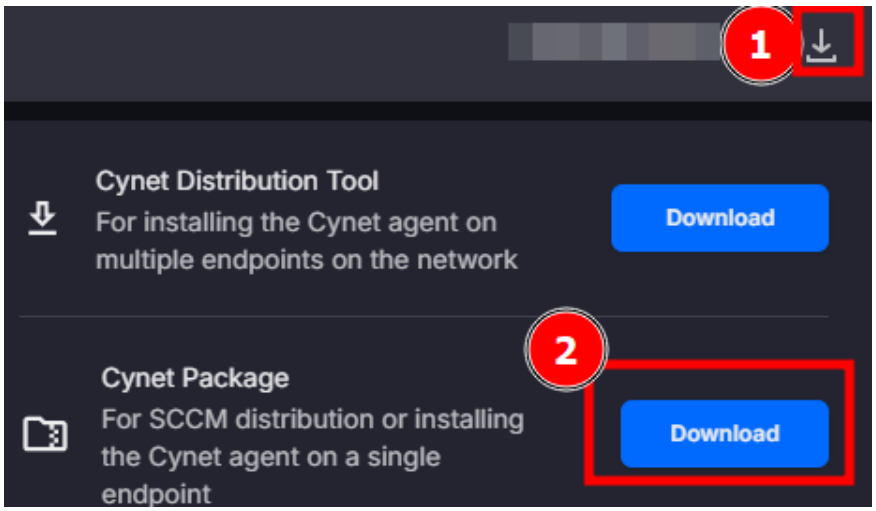


Ilustración 3. Instalación individual en un sólo equipo o endpoint.

b) Transferir el archivo descargado a la máquina Windows donde se va a instalar el agente.

c) Descomprimir el archivo descargado y, con permisos de administrador en el Sistema Operativo, ejecutar el programa “CynetMSI.msi” dentro de la carpeta descomprimida tal y como muestra la Ilustración 4.



Ilustración 4. Instalación del agente

d) Hacer clic en el botón “Next” y esperar a que se termine el proceso de instalación.

e) Ejecutar el administrador de tareas en la máquina donde se ha instalado el agente y verificar que existen procesos en segundo plano con los nombres “Cynet Memory Scanner” y “Cynet Scanner (32 bit)”, como se aprecia en la Ilustración 5.

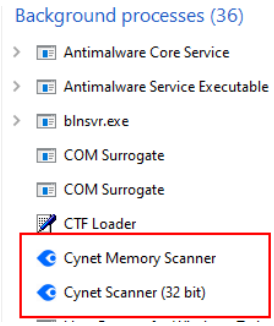


Ilustración 5. Comprobación de funcionamiento correcto del agente

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Para configurar el modo de operación seguro, se deben realizar los siguientes pasos para cada componente (agente y consola):

Agente

a) Acceder a la consola de Cynet.

b) Navegar a la sección “Settings > Groups” (Ilustración 6).

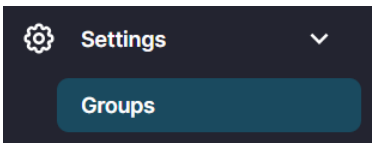


Ilustración 6. Sección para configurar el agente

c) Editar el grupo “Manually installed Agents” (Ilustración 7).

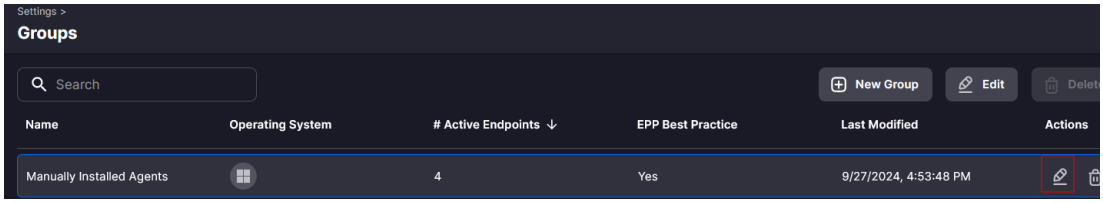


Ilustración 7. Grupo a modificar

d) Habilitar las opciones “Endpoint Protection (EPP)” y “Endpoint Detection & Response (EDR)” en modo “Prevent” (Ilustración 8).

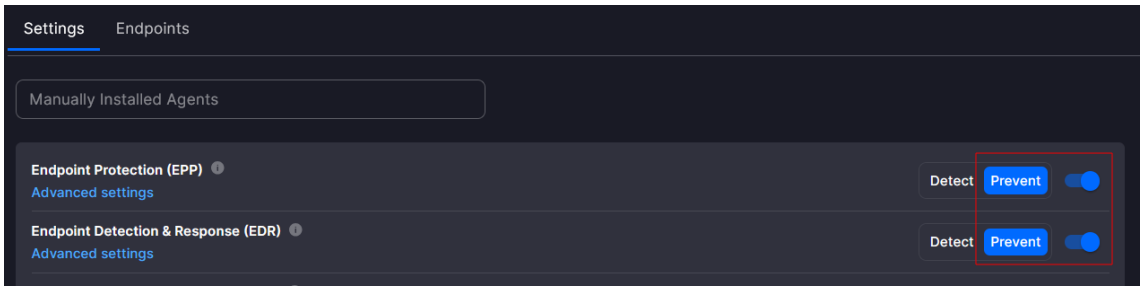


Ilustración 8. Opciones a habilitar

e) Hacer clic en el botón “Manage” debajo de la subsección “Agent Settings”.

f) Activar las opciones “Automatic Agent Update”, “Display tray icon on endpoint”, “Enable actions on endpoint” para usuarios administradores (“Admins”) (Ilustración 9).

   a. La opción “Unscanned Group Alert” debe activarse solamente en equipos ubicados en entornos de operación 24/7.

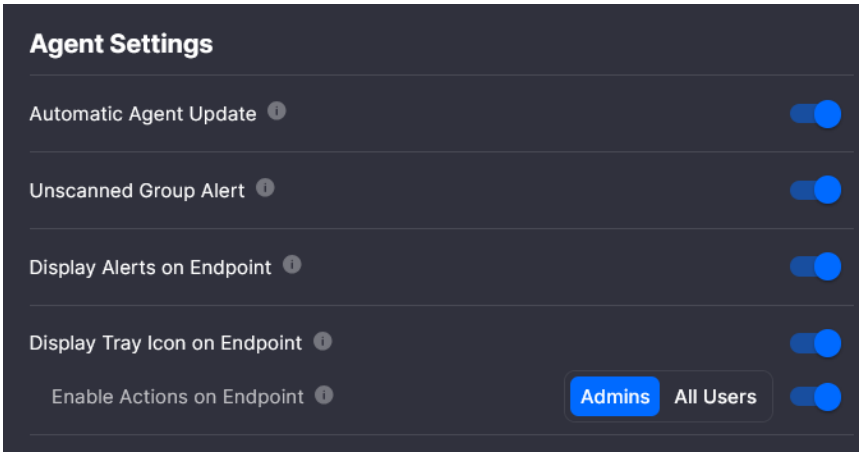


Ilustración 9. Opciones del agente a habilitar

g) En el campo “Set an Agent Uninstall Password” establecer una contraseña segura que cumpla con una longitud mínima de 8 caracteres y que contenga al menos una letra mayúscula, una letra minúscula, un número y un carácter especial de los siguientes [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”] (Ilustración 10).

Nota: Esta contraseña debe ser almacenada de manera segura por el administrador de la organización que gestionará el servicio de Cynet instalado.

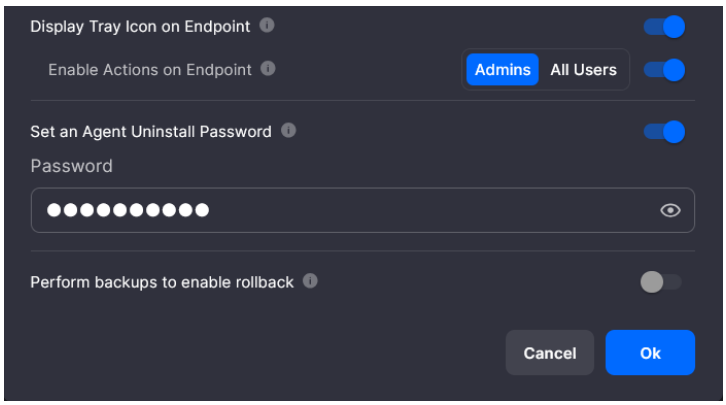


Ilustración 10. Definición de la contraseña de desinstalación

h) Hacer clic en el botón “OK” y luego en el botón “Save”.

Consola

a) En la consola de Cynet usando la misma cuenta con rol de administrador navegar a “Settings > Advanced”.

b) Habilitar la opción “Enable MSI Endpoint uninstall password” en la sección “EPS Uninstall password” e introducir la misma contraseña que en los pasos anteriores u otra contraseña que cumpla los mismos requisitos y se almacene de la misma manera (Ilustración 11).

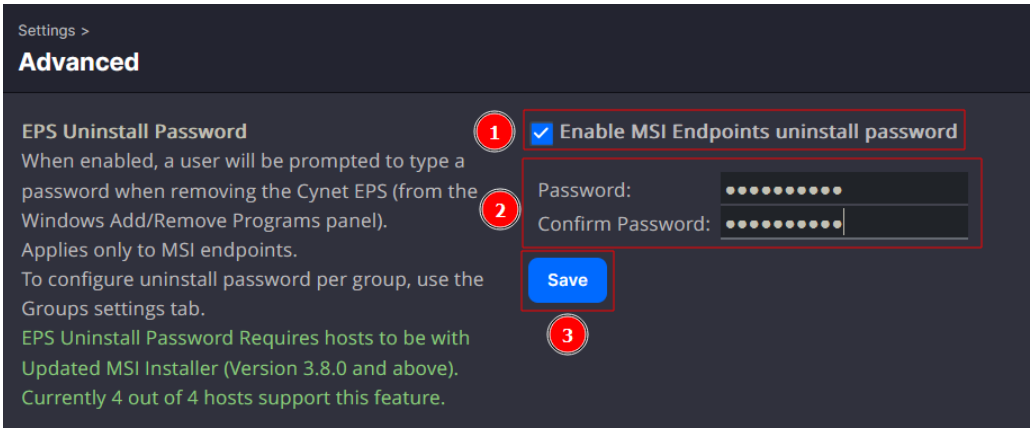


Ilustración 11. Configuración de la misma contraseña de desinstalación en la consola

c) Habilitar la opción "Unique file analysis by SOC" en la sección "Unique file analysis by SOC" (Ilustración 12).

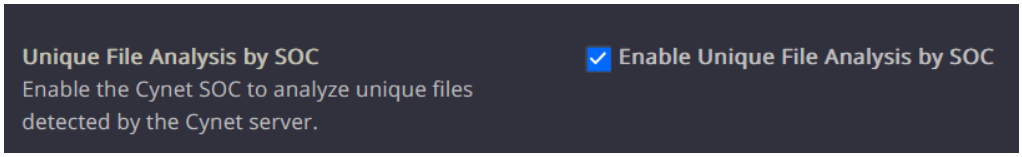


Ilustración 12. Activación de opción de análisis

d) Habilitar la opción "Enable Cynet SOC file analysis" en la sección "Cynet SOC file analysis" (Ilustración 13). **Advertencia**: esto habilita el envío de ficheros al SOC de Cynet para análisis, por lo que debe habilitarse, o no, de acuerdo a las políticas y normativa de la organización.

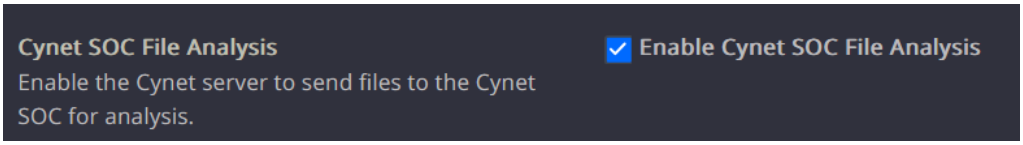


Ilustración 13. Activación de opción de análisis

e) Habilitar la opción "Enable file allowlisting" en la sección "File allowlisting" (Ilustración 14).

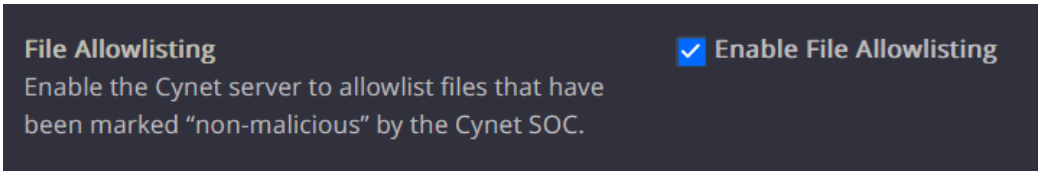


Ilustración 14. Activación de listas "Allow"

f) Guardar los cambios.

g) Navegar a la sección "Settings > Alerts" de la interfaz principal.

h) Cambiar el valor del filtro de alertas de email "Email alert filter" a "Informative" y hacer clic en "Save" para guardar los cambios (Ilustración 15).

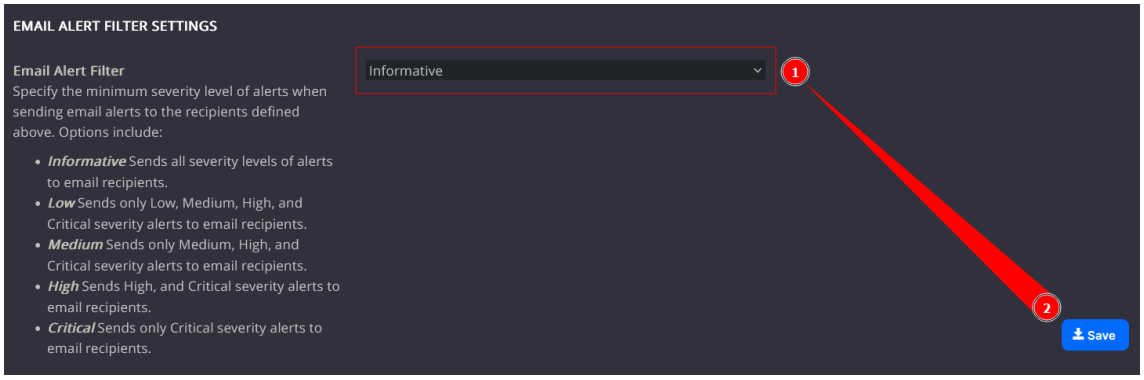


Ilustración 15. Activación de alertas por e-mail

i) Activar las opciones “Enable SSE Sandbox Analysis”, “Enable Cloud Sandbox” y desactivar la opción “Enable Local Sandbox” (Ilustración 16). **Advertencia**: esto habilita el envío de ficheros al SOC de Cynet para análisis, por lo que debe habilitarse, o no, de acuerdo a las políticas y normativa de la organización.

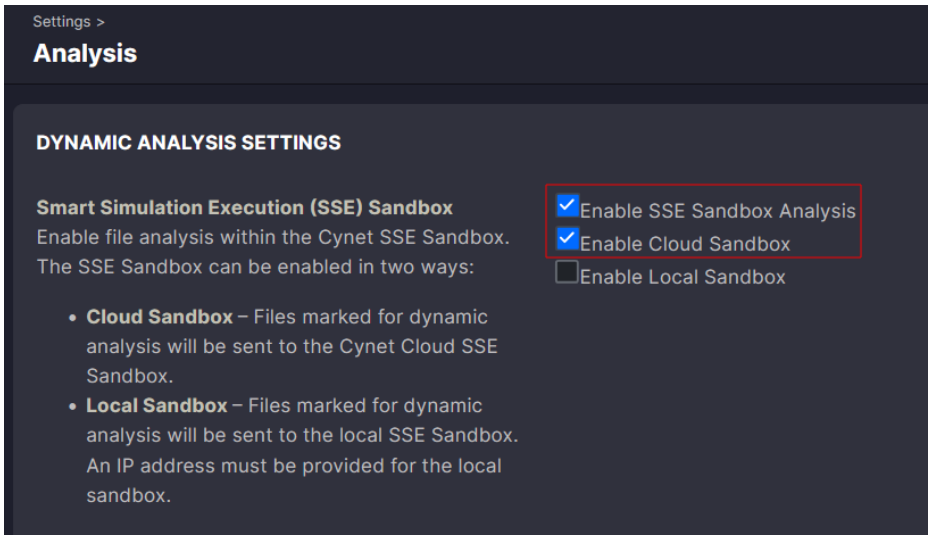


Ilustración 16. Activación de opciones de análisis

j) Navegar a la sección “Settings > Deception” y hacer clic en el botón “Create”, para crear un *honeypot* para los atacantes.

k) Establecer el grupo a “Manually Installed Agents” en “Groups”, el “User name” a un nombre señuelo como “DomainSuperAdmin33”, el “Host name” a uno señuelo como “CRMWINSERV2012”, el “User Type” a “Generic”, y finalmente hacer clic en el botón “Add”.

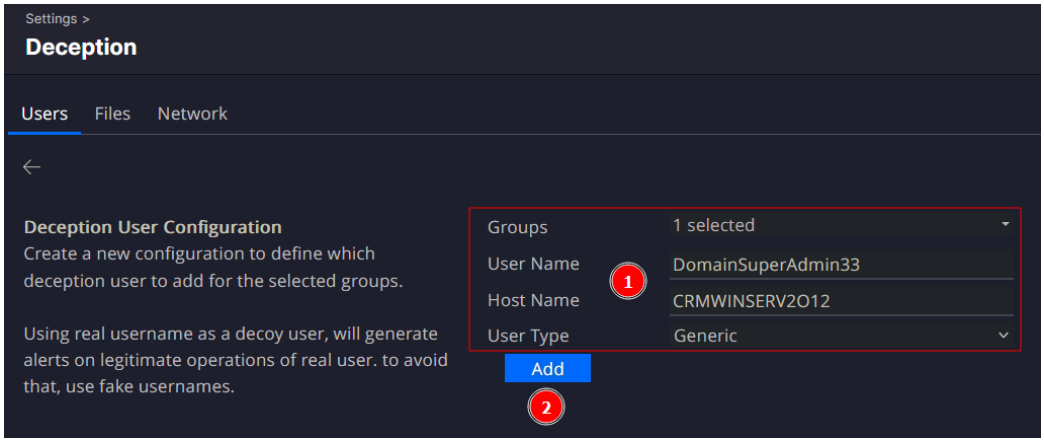


Ilustración 17. Configuración de usuario señuelo

6.2 AUTENTICACIÓN

Los mecanismos de autenticación usados por el servicio son los siguientes:

- **Usuarios locales**: Los usuarios de las máquinas Windows donde se instala el agente de Cynet se autentican de forma local en la máquina usando el mecanismo interno de Windows (usuario y contraseña).
- **Usuarios administradores**: Credenciales (usuario y contraseña) en la consola del servicio.
- **Autenticación entre componentes del servicio:** Mediante certificados digitales X.509.v3.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración del servicio se realiza principalmente de forma remota a través de la consola web, aunque iniciar un escaneo del endpoint (máquina Windows donde está instalado el agente) sí puede realizarla un administrador en esa misma máquina.

En la configuración cualificada, la comunicación de estos administradores con la interfaz de gestión web se realiza a través de **TLS v1.2 o superior**.

NO deben permitirse protocolos inseguros para la administración.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Cynet permite gestionar usuarios mediante la consola web para que puedan realizar las funcionalidades de seguridad según los roles asociados a estos usuarios.

Existe una lista de roles predefinidos en la guía referenciada en [REF7].

Se deben tener en cuenta los siguientes aspectos para la configuración de usuarios administradores:

- **Configuración de la Política de contraseñas seguras**. Deberá cumplir con los siguientes requisitos mínimos:
  - Longitud mínima de la contraseña: ocho (8) caracteres.

  - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales.
- **Configuración de los parámetros de sesión.** Deberá cumplir con los siguientes requisitos mínimos:
  - Tiempo de inactividad de las sesiones: veinte (20) minutos, configurable siguiendo la guía [REF8].
  - Número de intentos fallidos de inicio de sesión: diez (10) intentos.
- Tiempo de bloqueo tras los intentos fallidos: los diez (10) primeros intentos fallidos bloquean al usuario indefinidamente. Otro usuario administrador de la consola o el equipo de soporte de Cynet deben desbloquear al usuario en este caso.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Para este Procedimiento de Empleo Seguro, no se requiere configuración de interfaces, puertos o servicios más que los habilitados nativamente por el sistema operativo en la máquina Windows donde se despliega el agente. El agente utiliza el protocolo TLS en su versión 1.2 y/o superior para comunicarse con la consola.

6.5 GESTIÓN DE CERTIFICADOS

Para este Procedimiento de Empleo Seguro, no se debe configurar o gestionar ningún tipo de certificado.

6.6 SERVIDORES DE AUTENTICACIÓN

Para este Procedimiento de Empleo Seguro, no se debe configurar o gestionar ningún servidor de autenticación externo.

6.7 SINCRONIZACIÓN

Los usuarios de este Procedimiento de Empleo Seguro no necesitan configurar o gestionar ningún servidor de sincronización. Las máquinas de Windows hacen uso del servidor de sincronización por defecto del sistema operativo y la consola hace uso de un sistema de sincronización gestionado por Cynet. Todos los componentes del entorno de operación deben estar sincronizados en hora para el correcto funcionamiento del servicio.

6.8 ACTUALIZACIONES

La consola de Cynet es mantenida y actualizada por el equipo de ingeniería autorizado de Cynet, por lo que el usuario administrador no debe hacer nada en la consola.

Las actualizaciones del agente de Cynet son automáticas. Para comprobar que están activadas correctamente, el usuario administrador debe seguir los siguientes pasos:

a) En el menú “Settings > Groups”, editar la opción “Manually Installed Agents”.

b) Hacer clic sobre “Manage” en “Agent Settings”.

c) Activar la opción “Automatic Agent Update” y luego hacer clic en “Ok” (Ilustración 18).

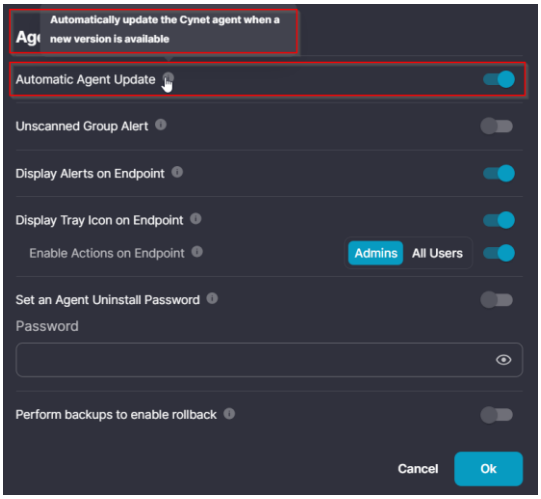


Ilustración 18. Activación de las actualizaciones automáticas

6.9 AUTO-CHEQUEOS

El agente de Cynet, en la fase de arranque, efectúa los siguientes chequeos:

- Verificación de integridad (checksum).
- Conectividad con servicios de actualización.
- Validez de los certificados empleados en la comunicación.

En el caso de que alguno de estos chequeos sea erróneo o inválido, se generará el correspondiente mensaje en el log del sistema. Se debe, por tanto, revisar y analizar la información de logs para detectar errores en los auto chequeos.

Los auto chequeos y el monitoreo de integridad de la consola se gestionan de manera centralizada por Cynet, dado que este componente está desplegado en la nube. Este componente está diseñado para funcionar continuamente, con procesos automáticos que garantizan su rendimiento, integridad y disponibilidad sin necesidad de intervención directa por parte del usuario final.

6.10 ALTA DISPONIBILIDAD

La consola de Cynet está diseñada para ofrecer alta disponibilidad mediante la implementación de arquitecturas en la nube redundantes, asegurando que los usuarios puedan acceder a los servicios de manera continua, sin interrupciones. La gestión de la alta disponibilidad es una responsabilidad directa de Cynet, que garantiza la operatividad de los servicios a través de diversas estrategias.

La combinación de redundancia geográfica, balanceo de carga y capacidades avanzadas de recuperación ante desastres asegura que los usuarios puedan confiar en que los servicios estarán disponibles en todo momento.

En caso de que se produzca una interrupción, Cynet gestiona el proceso de recuperación, asegurando que el servicio vuelva a estar operativo lo más rápido posible sin intervención del usuario final.

Por su parte, se debe desplegar el agente de Cynet correspondientemente si las necesidades de disponibilidad de la organización así lo requieren.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

El servicio puede registrar, principalmente, cuatro (4) tipos de eventos:

- **Eventos relacionados al acceso de usuarios**: Relativos a iniciar sesión y cerrar la sesión en la consola de Cynet.
- **Eventos relacionados con el cambio de credenciales**: Relativos al cambio de la contraseña de los usuarios administradores registrados en la consola de Cynet.
- **Cambios en la configuración del servicio**: Generados en base a los siguientes eventos / acciones:
    a) Hacer cambios en un "Asset Group".
    b) Editar las políticas.
    c) Editar en el menú "Settings".
    d) Crear un usuario en la consola.
    e) Crear un rol en la consola.
    f) Cambiar el rol de un usuario en la consola.
- **Eventos relacionados con la funcionalidad del producto**: Generados en base a las siguientes acciones:
    a) Guardado de "Auto remediation".
    b) Ejecución de "Custom Remediation actions".
    c) Bloquear tráfico.
    d) Borrar un fichero.
    e) Borrar un servicio.
    f) Borrar una "Task".
    g) Deshabilitar NICs.
    h) Deshabilitar un servicio.
    i) Deshabilitar una "Task".
    j) Deshabilitar un usuario.
    k) Habilitar/Activar un usuario (cuando ha sido bloqueado por intento de acceso por fuerza bruta).
    l) Reiniciar / hacer reboot del sistema.
    m) Ejecutar un "command".
    n) Ejecutar un "script".
    o) Aislar / Desaislar.
    p) Eliminar un proceso.
    q) Poner en cuarentena/Sacar de cuarentena un archivo.

r) Cambiar IP.

s) Descargar archivos.

t) Verificar archivo.

u) Enviar a evaluación del SOC.

v) Enviar a análisis del SOC.

w) Red de “deception”.

x) Analizar host.

y) Establecer estado de alerta.

z) Mostrar alertas.

6.11.2 ALMACENAMIENTO REMOTO

El servicio cuenta con posibilidad de conectarse a un servidor remoto por parte de los usuarios administradores para el almacenamiento de registros de auditoría.

Para la cualificación y este Procedimiento de Empleo Seguro, no se recomienda la configuración de un servidor remoto por parte de los usuarios administradores, pues la información de registros de auditoría está almacenada y gestionada íntegramente por Cynet.

6.12 BACKUP

El servicio está diseñado para almacenar información y ofrece capacidades de respaldo de forma centralizada, gestionadas y configuradas íntegramente por Cynet.

Cynet gestiona la realización periódica de copias de seguridad

7 REFERENCIAS

REF1 CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic/763-cynet-3604-29-999-19020-cynet-xdr-console-n-a?ic=1

REF2 Cynet All-in-One Cybersecurity Solutions
https://www.cynet.com/quote-request/?hsCtaAttrib=118726328103

REF3 Login
https://signup.cynet.com/login

REF4 Hardware Requirements for Agent Installation
https://help.cynet.com/en/articles/108-hardware-requirements-for-agent-installation

REF5 Supported Operating Systems
https://help.cynet.com/en/articles/47-supported-operating-systems

REF6 Network Installation Guide
https://help.cynet.com/en/articles/84-network-installation-guide

REF7 Global Users and Roles
https://help.cynet.com/en/articles/64-global-users-and-roles

REF8 Inactivity Timeout Duration
https://help.cynet.com/en/articles/315-inactivity-timeout-duration

8 ABREVIATURAS

CPU	Central Processing Unit
EDR	Endpoint Detection and Response
ENS	Esquema Nacional de Seguridad
EPP	Endpoint Protection Platform
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
MSI	Microsoft Software Installer
OS	Operating System
QR	Quick Response
SOC	Security Operations Center
SSE	Security Service Edge
SSL	Secure Sockets Layer
TLS	Transport Layer Security
XDR	Extended Detection and Response