centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1233

Procedimiento de Empleo Seguro
TEHTRIS EDR

Mayo 2025

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-188-2
Fecha de Edición: Mayo de 2025

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
2026.01.16 07:25:48 +01'00'

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

ÍNDICE

1 INTRODUCCIÓN

1. TEHTRIS EDR es una solución de seguridad avanzada diseñada para detectar y neutralizar amenazas en tiempo real en cada *endpoint* o servidor donde esté desplegada. Utiliza tecnologías heurísticas, *sandboxes* y sistemas de inteligencia artificial para monitorizar actividades a nivel de sistema, detectando comportamientos sospechosos y actividad maliciosa.
2. La interfaz, a través la cual se pueden gestionar las funcionalidades que ofrece el producto, es la interfaz web, accesible remotamente a través del protocolo HTTPS.
3. La solución se compone de tres componentes principales: la plataforma TEHTRIS XDR, el agente TEHTRIS EDR y el servidor virtual TEHTRIS EDR, proporcionando protección integral tanto en la nube como en entornos locales. Estos componentes, se encargan de las funciones siguientes:
    - **Plataforma TEHTRIS XDR**, la cual es utilizada por el administrador de la red de dispositivos finales para ser incluidos en la protección contra amenazas. Esta parte del producto funciona en la nube. En esta plataforma es donde el usuario realiza actividades de gestión.
    - **Agente TEHTRIS EDR**, se instala en los puntos finales y detecta amenazas en ellos. En la evaluación realizada, el agente se instaló en Windows.
    - **Servidor virtual TEHTRIS EDR**, es el motor encargado de buscar amenazas y neutralizarlas.
4. TEHTRIS EDR ofrece un conjunto de funciones de seguridad avanzadas que incluyen:
5. **Detección y neutralización de amenazas en tiempo real**: El sistema monitoriza continuamente los *endpoints* para detectar comportamientos sospechosos, utilizando tecnologías como heurísticas, análisis en *sandbox* e inteligencia artificial.
6. **Capacidades de anti-explotación**: TEHTRIS EDR incluye mecanismos de auto-protección que evitan que otros procesos accedan a las áreas de memoria utilizadas por el agente, garantizando la integridad del sistema durante su operación.

2 OBJETO Y ALCANCE

7. El presente documento tiene como objetivo servir de guía para la instalación y configuración segura de TEHTRIS EDR, con el fin de garantizar un uso seguro en entornos críticos y cumplir con los requisitos de seguridad de la normativa CCN-STIC.
8. TEHTRIS EDR ha sido cualificado e incluido en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) dentro de la familia de *"Endpoint Detection Response"* [REF1].
9. Todos los mecanismos criptográficos utilizados, deben concordar con los establecidos en la guía CCN-STIC-807 [REF2].

3 ORGANIZACIÓN DEL DOCUMENTO

10. El presente documento se organiza en los siguientes apartados:

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

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

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

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

4 FASE PREVIA A LA INSTALACIÓN

11. Antes de llevar a cabo la instalación, para que el cliente final adquiera el producto, este deberá abrir un ticket con el soporte de TEHTRIS EDR, enviando un correo a *support@tehtris.net* para contactar con ellos. En ese correo, se debe especificar el deseo de cargar la configuración LINCE en el producto (que es la configuración cualificada).

12. Para realizar el proceso de inscripción, es necesario contactar al fabricante mediante el correo indicado anteriormente, aunque también está disponible en su web oficial un apartado llamado "Contact Us" [REF3]. En este correo o mensaje, se adjuntará la dirección IP pública, así como los datos del usuario administrador (nombre, apellido, número de teléfono y e-mail). Estos datos estarán comparados con los ingresados en la página *enroll* y luego se utilizarán, para conectarse a la Plataforma XDR, incluyendo la dirección IP pública, la cual será introducida en una lista blanca. Se puede consultar la dirección IP pública accediendo al sitio web que está disponible en [REF4]. Después de proporcionar esta información, el equipo de TEHTRIS EDR le otorgará un *trigram* (un identificador único de tres letras utilizado para distinguir cada plataforma), para que el usuario pueda acceder al producto a través de un enlace siguiendo este formato de *endpoint*: https://xxx.tehtris.net/enroll (donde XXX es el *trigram* proporcionado).

13. Siguiendo todos los pasos que se van a describir a continuación, se consigue un acceso seguro a TEHTRIS XDR Platform.

    - Acceder a https://xxx.tehtris.net/enroll sustituyendo XXX con el *trigram* proporcionado. Seguidamente, debe ingresar los datos, aceptar el EULA y hacer *Click* en Registrar.

Figura.1. TEHTRIS XDR Platform Registration Form.

- El registro se lleva a cabo y el fabricante envía al correo electrónico registrado, la información relacionada con el certificado de cliente para acceder a la plataforma.

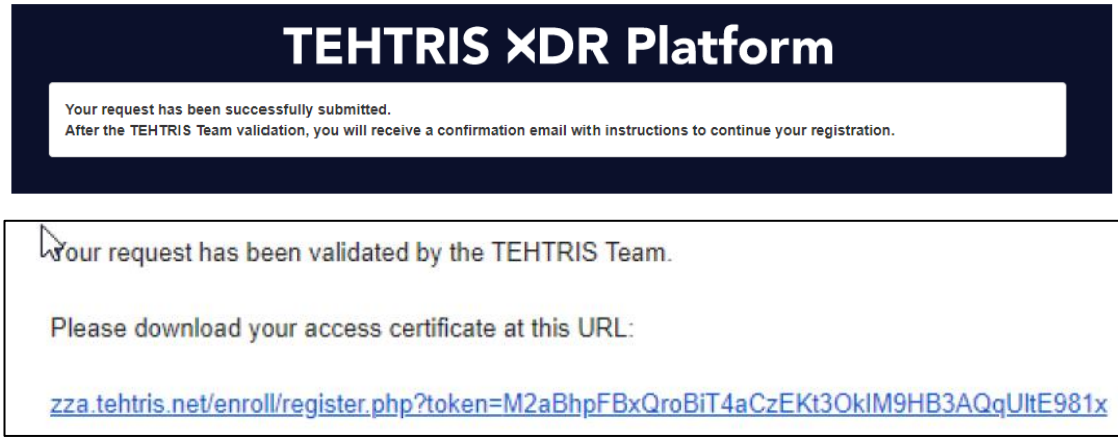

Figura.2. Enlace de descarga del certificado.

- Hacer *Click* en el enlace e introducir un código PIN que se le ha enviado a el número de móvil registrado a través de SMS.

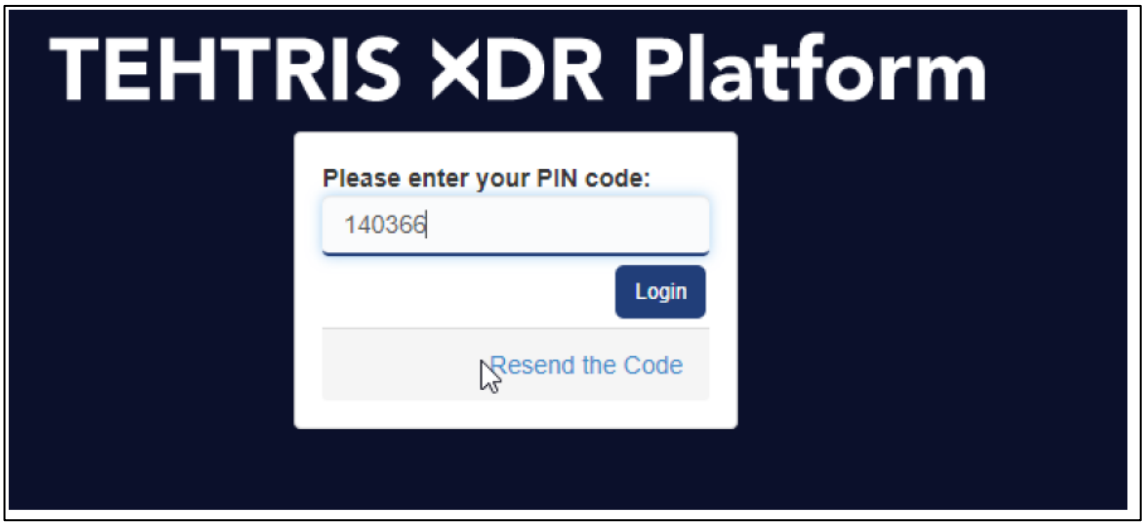

Figura.3. Enter your PIN Code.

- Descargar el certificado y guardar la contraseña de forma segura.

Figura.4. Descarga del certificado.

- Instalar el certificado en el navegador web como cualquier otro certificado de cliente personal, siguiendo los manuales de su navegador.
- Acceder a la plataforma XDR https://XXX.tehtris.net/ indicando la contraseña del certificado. Establezca una contraseña para su usuario e introduzca el código que se le ha enviado a su teléfono.

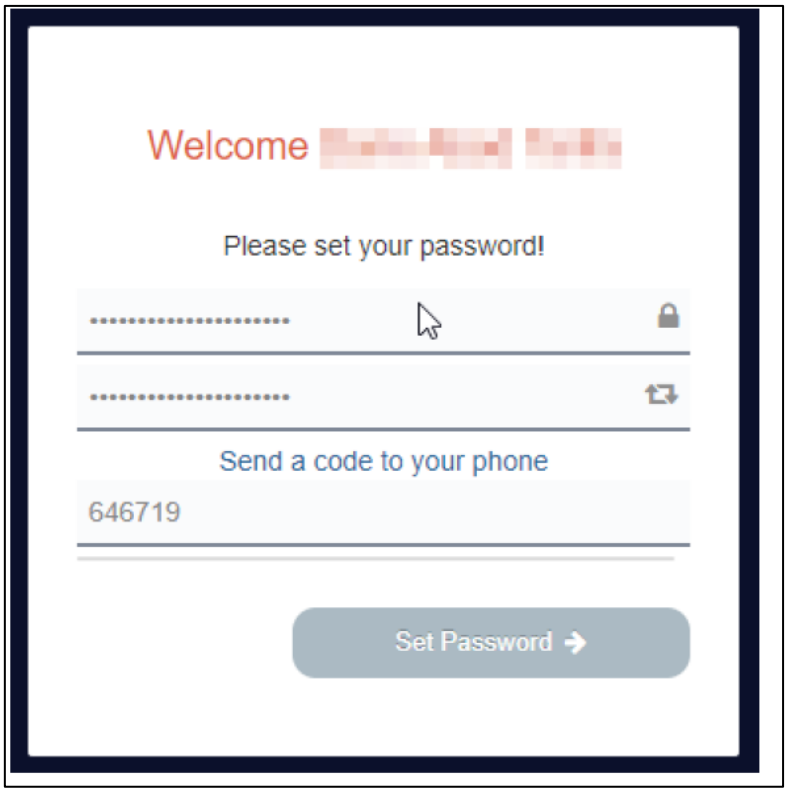

Figura.5. Inicio de sesión en la plataforma.

4.1 ENTREGA SEGURA DEL PRODUCTO

14. TEHTRIS EDR se entrega como un servicio que incluye tanto componentes para instalar localmente como en la nube. El Agente TEHTRIS EDR se instala localmente, TEHTRIS XDR Platform es accesible a través de la nube y el Servidor Virtual TEHTRIS puede ser instalado tanto localmente, como en la nube.

15. El proceso de entrega segura al acceso a la plataforma TEHTRIS XDR es el indicado en **4.FASE PREVIA A LA INSTALACIÓN**.

16. El Agente TEHTRIS EDR y Servidor virtual TEHTRIS EDR se entregan de manera segura, siguiendo la siguiente dinámica:

    - **Descarga de Archivos**: El instalador del Agente TEHTRIS EDR es posible descargarlo desde el menú de la Plataforma TEHTRIS XDR del cliente.
      En cuanto al Servidor Virtual TEHTRIS EDR el fabricante facilita un enlace mediante un correo electrónico desde donde se puede descargar este componente en forma de ISO. El fabricante proporciona, adjunto en el mismo correo, un PowerPoint donde se describe el proceso de instalación y se indica el hash (SHA-256) de la ISO.
    - **Verificación de Integridad**: Antes de iniciar la instalación, se verifica que el Hash recibido coincide con el archivo original. Esto se hace, para asegurar que no han sido modificados.
    - **Instalación y Configuración**: Los componentes se instalan localmente y se configuran para comunicarse de manera segura con la plataforma TEHTRIS XDR utilizando HTTPS (HTTP sobre TLS v1.2).

4.2 ENTORNO DE INSTALACIÓN SEGURO

17. Un entorno de instalación debe garantizar que solo personal autorizado tenga acceso al sistema. Esto incluye restricciones en el acceso físico y lógico, con autenticación basada en certificados y contraseñas seguras para el acceso a la consola de administración TEHTRIS XDR Platform. Además, existe una lista blanca de IP autorizadas para acceder a la plataforma XDR.

4.3 REGISTRO Y LICENCIAS

18. La asignación de licencias en TEHTRIS EDR, se basa en los elementos de red proporcionados por el cliente. Estos elementos deben de ser enviados a la siguiente dirección de correo *support@tehtris.net*.

19. La licencia se configura en el servidor TEHTRIS ED, durante la fase de instalación se solicitará al administrador una clave, está habrá sido transmitida por TEHTRIS mediante los canales oficiales. En el caso del agente, la licencia se obtiene automáticamente del servidor, cuando se establece la primera conexión entre ambos componentes.

20. TEHTRIS crea una licencia para cada Servidor TEHTRIS EDR según:

    - La dirección IPv4, la máscara de subred y la puerta de enlace de la interfaz "Management" (MGMT) (1)
    - La dirección IPv4, la máscara de subred y la puerta de enlace de la interfaz "Production" (PROD) (2).
    - La dirección IP pública de la interfaz *Management* (1).
        - Nota: si el dispositivo puede salir a través de varias IP públicas y el cliente no puede determinar con precisión cuál se utilizará, se solicitará el conjunto mínimo de posibles IP públicas.

21. El equipo de TEHTRIS seguidamente, preparará el servicio de validación de licencias para recibir este nuevo dispositivo. Esto es simplemente una cadena de caracteres que se utilizará durante la fase final de la instalación de cada dispositivo.

22. Una vez generada la licencia, el equipo de TEHTRIS enviará una nota de entrega al cliente o socio que contiene toda la información técnica necesaria para la instalación de la VM.

4.4 CONSIDERACIONES PREVIAS

23. En cuanto a la plataforma TEHTRIS XDR, la principal consideración previa es tener conexión a internet y estar dado de alta en la plataforma para hacer uso del servicio.

24. A continuación, se van a declarar algunos de los pre-requisitos necesarios para configurar la máquina virtual necesaria para desplegar el Servidor Virtual TEHTRIS EDR en el caso de que la instalación sea local:

    - **VMWare Host**: Hay que asegurarse de usar versiones 6.7 o superiores para *VMWare ESXi*.
    - **Boot Mode**: Configur la VM para arrancar en modo BIOS, no UEFI.
    - **Copias de seguridad**: Planificar copias de seguridad, utilizando métodos basados en instantáneas o las herramientas integradas de *VMWare*.
    - **Almacenamiento**: Usar dos discos duros:

- Uno para el sistema (instalación del SO).
- Uno para el almacenamiento de datos. Se recomiendan unidades Flash/SSD para un mejor rendimiento.

- Características VM:
  - RAM: 8GB.
  - CPU: 4Vcpu.
  - HDD1: 16 GB.
  - HDD2: 500 GB.

25. El fabricante proporcionará un código, que será necesario para la instalación del Servidor Virtual EDR 5.1.SERVIDOR VIRTUAL TEHTRIS EDR.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

26. En esta sección, se van a detallar los componentes del entorno operacional que se comunican con los componentes principales de TEHTRIS EDR descritos en *1.INTRODUCCIÓN*. Estos elementos son los siguientes:

- **Servidor de Licencias TEHTRIS**, es un servidor que contiene las licencias y actualizaciones de TEHTRIS EDR. El servidor virtual TEHTRIS EDR se comunica con él utilizando HTTPS (HTTP sobre TLS v1.2).
- **Nube TEHTRIS**, es la infraestructura en la nube de TEHTRIS que soporta la TEHTRIS XDR Platform y la interfaz de gestión.
- **Interfaz de usuario**, es la infraestructura utilizada por el usuario para acceder a TEHTRIS XDR Platform y donde se instalan los Agentes TEHTRIS EDR. La comunicación con la interfaz de gestión se realiza a través de HTTPS (HTTP sobre TLS v1.2).

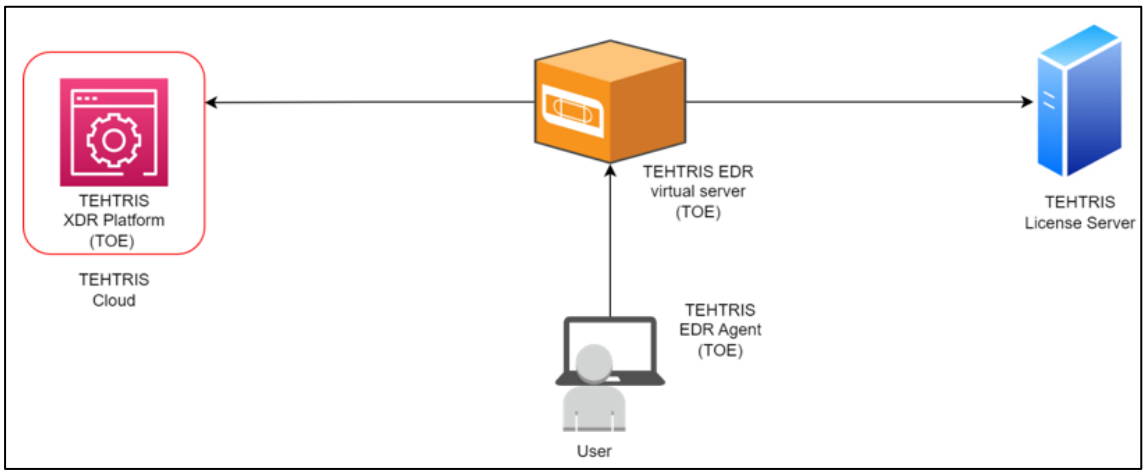

Figura. 6. Diagrama del entorno operacional.

5 FASE DE INSTALACIÓN

5.1 SERVIDOR VIRTUAL TEHTRIS EDR

27. El fabricante proporciona el componente “servidor virtual TEHTRIS EDR”, a través de un archivo ISO. Este archivo ISO se debe virtualizar en un *VMware ESXi*. Siguiendo los requisitos de hardware y red indicados por el fabricante *4.4.CONSIDERACIONES PREVIAS*. Una vez registrada la máquina virtual en el servidor de virtualización, se siguen los siguientes pasos para proceder con la instalación de este componente.

    - Arrancar la máquina virtual desde el archivo ISO de TEHTRIX y seleccionar la opción “BORRAR disco completo + Iniciar INSTALACIÓN de la versión 1.0 de TEHTRIX”.

Figura.7. Boot the VM from TEHTRIX ISO file.

28. Una vez el proceso de iniciación está hecho, se deben introducir los siguientes parámetros:

    - Indicar la dirección IP de la interfaz de gestión, esta interfaz establecerá conexión con la plataforma de TEHTRIS EDR.

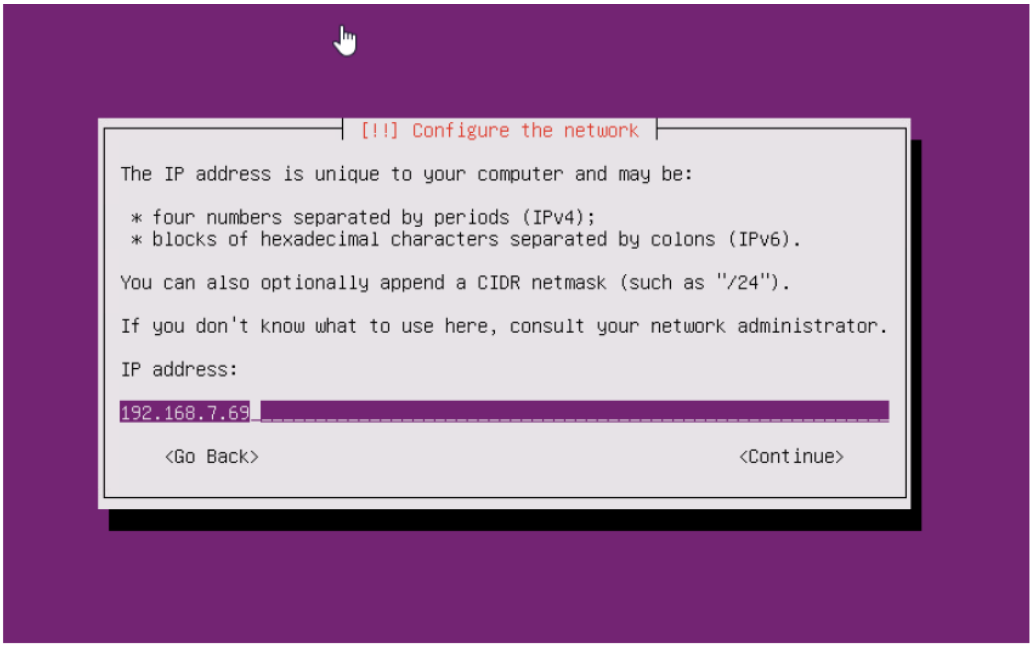

Figura.8. Configure the Network (IP).

- Indicar la máscara de red.

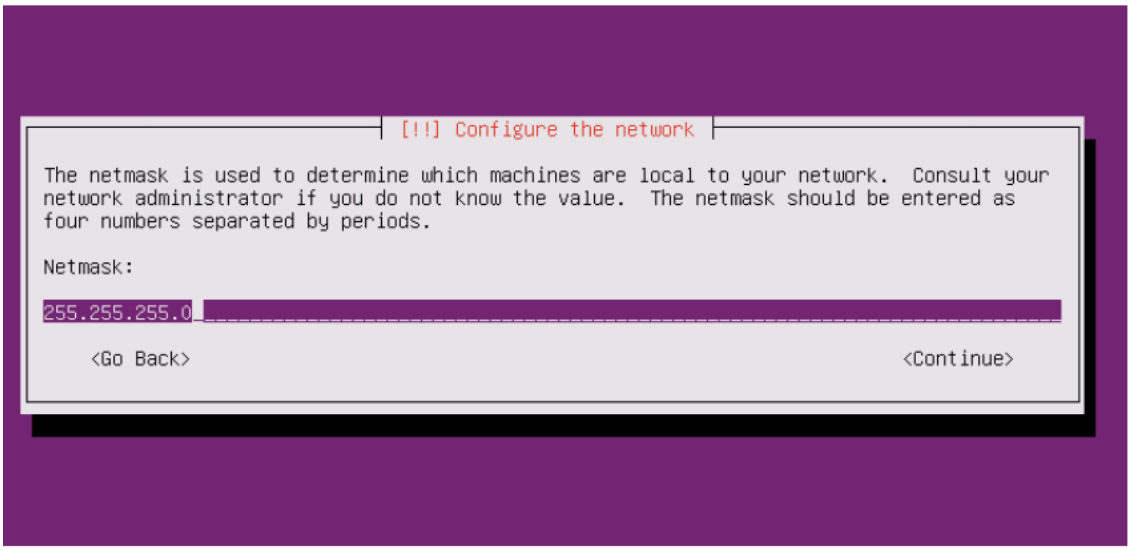

Figura.9. Configure the Network (Netmask).

- Indicar el Gateway.

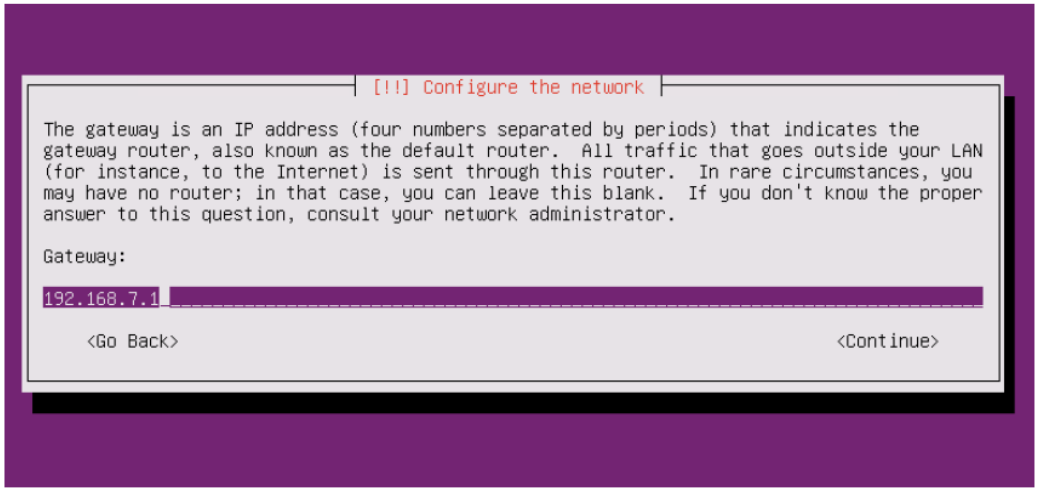

Figura.10. Configure the Network (Gateway).

29. Una vez configurados los parámetros de red, habrá que introducir la clave que es proporcionada por el fabricante para finalizar la instalación.

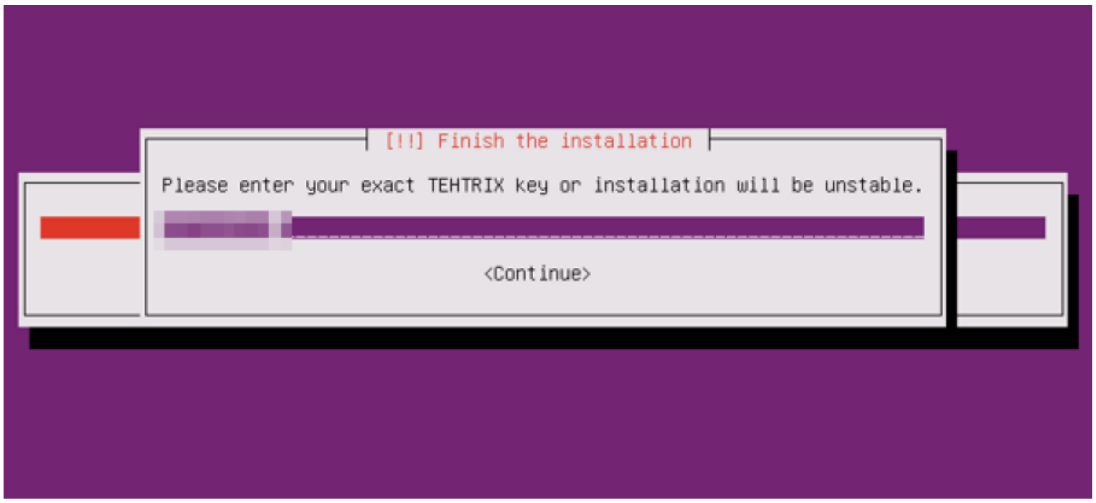

Figura.11. Finish the installation.

5.2 AGENTE TEHTRIS EDR

30. La instalación del agente se lleva a cabo, siguiendo los siguientes pasos:
    - Arrancar el instalador proporcionado por el fabricante como administrador.

31. Hacer *Click* en “next”.

Figura.12. TEHTRIS EDR set-up.

32. Seleccionar y aceptar los términos del acuerdo de licencia y hacer *click* en "next".

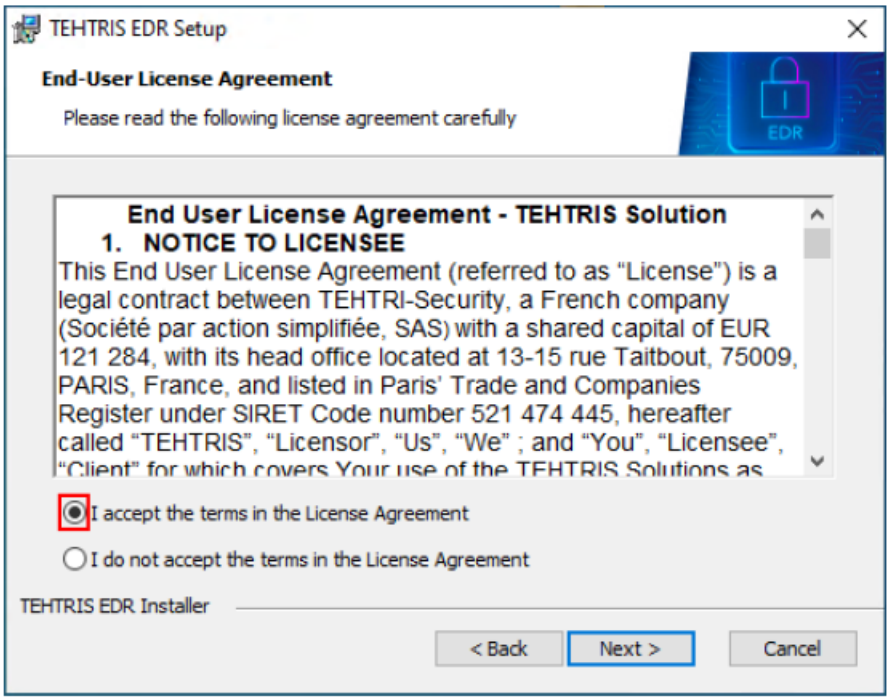

Figura.13. License Agreement.

- Indicar la IP del servidor, en el campo "server address" y escribir un "tag" como etiqueta que se atribuye al endpoint para después poder asignar políticas dependiendo de esos tags. Esta etiqueta debe tener la siguiente forma XXX_YYY, donde 'XXX' es un código proporcionado por TEHTRIS e 'YYY' es elegido por el administrador.

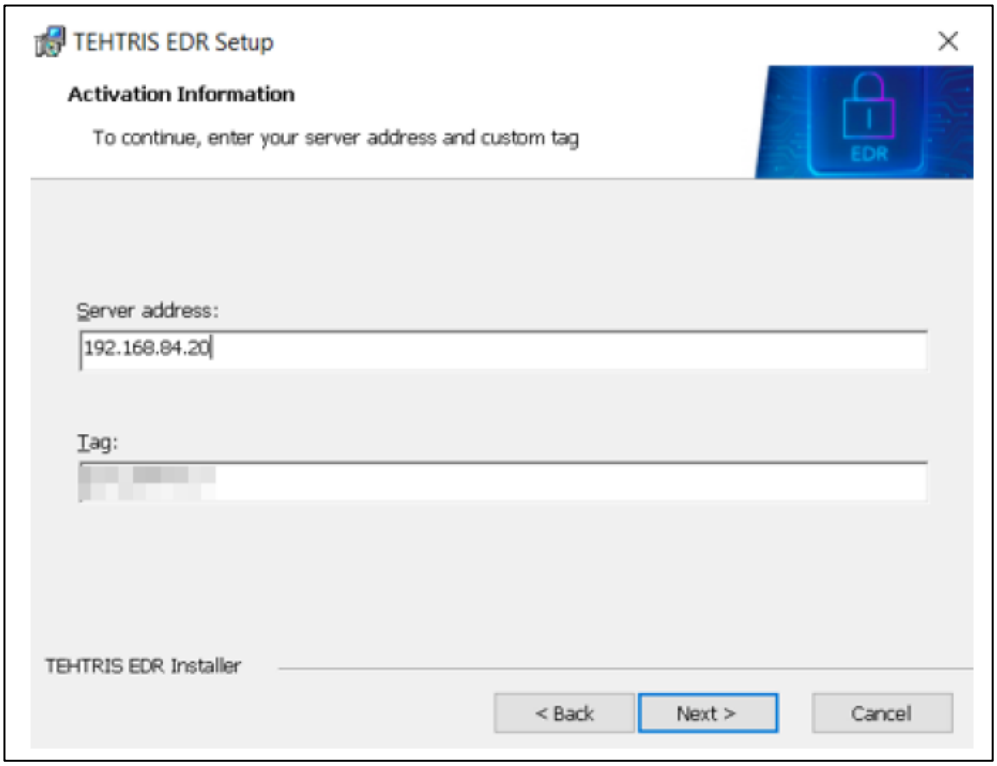

Figura.14. Activation information.

- Hacer *Click* en install.

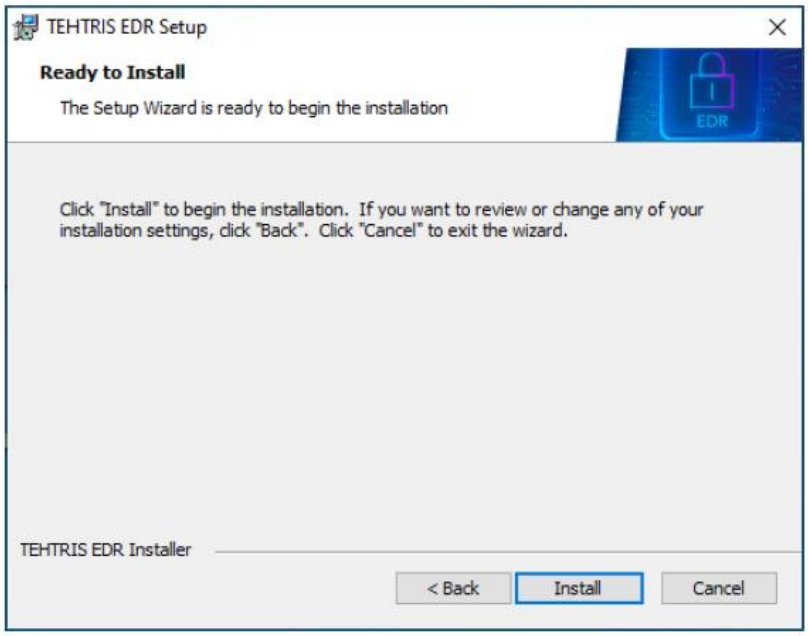

Figura. 15.Ready to install.

- Hacer *Click* en “finish”.

Figura.16. Completing the TEHTRIS EDR set-up.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

6.1.1 ACTIVA EL MODO LINCE

33. De acuerdo con la cualificación realizada, para lograr la configuración cualificada del producto, se contacta al soporte de TEHTRIS y se abre un ticket solicitando la provisión de la "Configuración LINCE". En la sección *4. FASE PREVIA A LA INSTALACIÓN*, se ofrece la información de cómo contactar con ellos.

6.2 AUTENTICACIÓN

34. El acceso al sistema se realiza mediante el uso de certificados y username/contraseña. La autenticación se configura para cada usuario de la plataforma, asegurando que solo personal autorizado puede modificar configuraciones o acceder a datos sensibles.

35. No se recomienda el uso de claves pre-compartidas, ya que el producto permite el uso de certificados.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN REMOTA

36. El producto se administra remotamente a través de de la Plataforma TEHTRIS XDR, una interfaz web activada por el fabricante para cada cliente. La URL tiene la siguiente estructura: https://FQDN.tehtris.net. Donde el campo "FQDN" es variable según cada cliente.

37. La administración de TEHTRIS EDR se puede realizar de manera remota, mediante el protocolo HTTP sobre TLS. Este producto solo permite versiones de TLSv1.2 o superiores, en las que se hace uso de las siguientes cipher-suites reflejadas como recomendadas en la guía CCN-STIC-807 [REF2].

    - TLS v1.2:
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS v1.3:
        - TLS_AES_256_GCM_SHA384
        - TLS_CHACHA20_POLY1305_SHA256
        - TLS_AES_128_GCM_SHA256

38. No se recomienda el uso de HTTP o protocolos como Telnet**,** ya que no aseguran una comunicación segura entre entidades.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

39. TEHTRIS EDR requiere de una configuración adecuada de las interfaces de red, puertos y servicios para asegurar su correcto funcionamiento y minimizar los riesgos de exposición

a amenazas externas. Las comunicaciones entre el Agente y el Servidor Virtual de TEHTRIS EDR, se realizan a través de puertos seguros empleando TLS v1.2 o superior, garantizando así la protección de los datos en tránsito.

40. Solo deben estar abiertos los puertos necesarios para la operación de TEHTRIS EDR, restringiendo el acceso a las interfaces de administración únicamente a IP autorizadas. Los puertos que deben estar habilitados se indican en el manual que TEHTRIS facilita al usuario [REF5].

41. Se requieren dos interfaces por dispositivo:

    - La interfaz "Management" (MGMT) (1) – Transmite flujos de aplicación y administración hacia Internet.
    - La interfaz "Production" (PROD) (2) – Transmite flujos de agentes.

42. La interfaz (1) debe tener una dirección IPv4 fija y dedicada durante toda la vida útil del dispositivo.

    - Esta dirección se utiliza durante la fase de arranque del dispositivo para recuperar datos de Internet.
    - No se puede cambiar en el futuro.
    - Por lo tanto, se debe tener cuidado al elegir esta dirección, ya que el dispositivo debe reinstalarse desde cero si necesita ser modificada.

43. La interfaz (2) debe tener una dirección IPv4 dedicada.

    - Las dos interfaces deben estar en subredes diferentes.
        - Ejemplo válido:
            - IP MGMT: 192.168.1.1 – Máscara de red MGMT: 255.255.255.0
            - IP PROD: 192.168.2.1 – Máscara de red PROD: 255.255.255.0
        - Ejemplo no válido:
            - IP MGMT: 192.168.1.1 – Máscara de red MGMT: 255.255.255.0
            - IP PROD: 192.168.1.2 – Máscara de red PROD: 255.255.255.0

6.5 ACTUALIZACIONES

44. Las actualizaciones de seguridad y funcionalidad son críticas para mantener el sistema protegido contra las últimas amenazas. TEHTRIS se encargará de las actualizaciones de los componentes TEHTRIS XDR y servidor EDR, según un sistema de citas concertadas con el cliente.

45. Las actualizaciones del agente se podrán descargar desde la propia Plataforma TEHTRIS XDR. Para instalar las actualizaciones, será necesario seguir el procedimiento previamente descrito en la sección 5.2 **¡Error! No se encuentra el origen de la referencia.**AGENTE TEHTRIS EDR.

6.6 AUDITORÍA

6.6.1 REGISTRO DE EVENTOS

46. A continuación, se muestran qué eventos se registran en TEHTRIS EDR:

Tipo	Descripción
Log de acceso	Muestra una alerta cuando un EDR se conecta a un dispositivo.
Alerta de antivirus	Puntuación de la base de datos de antivirus de TEHTRIS y Virus Total.
Alerta heurística	Todos los eventos con comportamiento o acciones sospechosas basadas en alertas heurísticas diseñadas por TEHTRIS EDR.
Red	No utilizado.
Oletools	Alertas del módulo Office Scan. Permite verificar todas las macros en archivos de Office. Existe un enlace para ver la macro en modo pasivo.
Alerta Sandbox	Puntuación del Sandbox de TEHTRIS.
USB	Registros recuperados del monitoreo de USB.
YARA	Detección de análisis de memoria en vivo.

Tabla 1.Tipos de eventos.

47. Cuando se muestra información en el panel de "Registros", los registros se pueden exportar en un archivo en formato CSV.

6.6.2 ALMACENAMIENTO LOCAL

48. El sistema TEHTRIS EDR genera registros detallados de los eventos de seguridad, que incluyen desde accesos de usuarios hasta detección de amenazas. Estos eventos son almacenados en formato seguro y pueden ser auditados a través de la Plataforma TEHTRIS XDR por los administradores para revisar la actividad del sistema y responder a incidentes. El administrador y usuarios autorizados podrán acceder a la información de auditoria desde la interfaz de gestión remota.

7 FASE DE OPERACIÓN

49. Una vez completada la instalación y configuración del sistema, es crucial implementar los siguientes protocolos durante las fases de funcionamiento y mantenimiento:

    - Revisar periódicamente los registros de auditoría generados por el servicio para identificar cualquier comportamiento inusual.
    - Asegurarse de que los administradores estén bien capacitados en el uso y la operación correcta del servicio.
    - Mantener las credenciales de acceso de los administradores seguras y protegidas.
    - Gestionar los usuarios aplicando el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.
    - Revisar las políticas de seguridad para asegurarse de que la configuración no sea menos segura que el perfil de protección estándar.

8 REFERENCIAS

50. A continuación, se indica la información pública y enlaces que se han referenciado a lo largo de la guía.

[REF1] Taxonomía de EDR (Endpoint Detection Response) - CCN-STIC-140-B2-M, Noviembre 2022

[REF2] Criptología de empleo en el Esquema Nacional de Seguridad (CCN-STIC-807), mayo 2022

[REF3] Web_Official_Tehtris-Contact

[REF4] Identifica_IP_Publica_Whats_My_IP

[REF5] TEHTRIS User Guide (Manual facilitado por TEHTRIS)

9 ABREVIATURAS

AES	Advanced Encryption Standard
BIOS	Basic Input/Output System
CCN	Centro Criptológico Nacional
CCN-STIC	Centro Criptológico Nacional - Seguridad de las Tecnologías de la Información y las Comunicaciones
CPSTIC	Catálogo de Productos y Servicios de Seguridad TIC
CPU	Central Processing Unit
CSV	Comma-Separated Values
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
EDR	Endpoint Detection Response
ENS	Esquema Nacional de Seguridad
EULA	End User License Agreement
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
HDD	Hard Disk Drive
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
LINCE	Listed INformation on Cybersecurity Evaluation
MAC	Media Access Control
PIN	Personal Identification Number
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SMS	Short Message Service
SO	Sistema Operativo
SSD	Solid State Drive
TEHTRIS EDR	TEHTRIS Endpoint Detection and Response
TEHTRIS XDR	TEHTRIS Extended Detection and Response
TIC	Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

VM	Virtual Machine
VMWare ESXi	VMware Elastic Sky X Integrated
XDR	Extended Detection Response
YARA	Yet Another Recursive Acronym (used for malware detection)

PUBLICACIONES DE DEFENSA

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