Ficha técnica.

Greinfort

OBSERVE | UNDERSTAND | PREDICT



Fecha: 02/2025
Referencia documento: Ficha técnica
Versión: 1.0

Este documento ha sido generado por Greinfort para uso exclusivo de Greinfort y su contenido es confidencial. Este documento no puede ser difundido a terceros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de Greinfort. En el caso de ser entregado en virtud de un contrato, su utilización y difusión estarán limitadas a lo expresamente autorizado en dicho contrato. Greinfort no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Índice

1. Contenido del documento. 4
1.1. Alcance. 4
1.2. Servicio Greinfort. 4
2. Descripción del producto. 4
2.1. Introducción. 4
2.2. Beneficios. 5
2.3. Diferenciadores 8

1. Contenido del documento.

1.1. Alcance.

Este documento es una descripción de producto que contiene las características principales, casos de uso, beneficios y diferenciadores del servicio Greinfort para vigilar infraestructura OT.

1.2. Servicio Greinfort.

Greinfort es una tecnología centrada en ofrecer monitorización en tiempo real para organizaciones que cuenten con infraestructura OT.

Utiliza tecnologías avanzadas basadas en I+D propio para realizar, entre otras funciones, inventario de activos, detección de anomalías mediante diferentes estrategias, gestión de vulnerabilidades o análisis de tráfico.

Con ello se previenen y mitigan amenazas de ciberseguridad, asegurando la infraestructura digital, datos sensibles y comunicaciones. A su vez, constituye una pieza fundamental para el cumplimiento de ciertos estándares y normativas de seguridad (ISO 27001, NIS2, etc.).

2. Descripción del producto.

2.1. Introducción.

En el sector industrial actual, la ciberseguridad es una cuestión capital. Las amenazas son cada vez más sofisticadas, y la clásica vigilancia del perímetro ya no es suficiente. Debido al cambio de paradigma hacia la hiperconectividad que supone el concepto de Industria 4.0 y superiores, la frontera entre internet, la zona IT y la zona OT se difuminan, y surgen nuevos riesgos.
Esta causa, junto a la demanda de protección de la producción, y la presión normativa ejercida por las Administraciones Públicas y los reguladores, hace cada vez es más necesario contar con soluciones de ciberseguridad OT que den respuesta integral a estas necesidades, como es Greinfort.

La tecnología de Greinfort, permite tener visibilidad de los activos en la red, detectar anomalías en base al tráfico de red, comprobar sus estadísticas o patrones de comportamiento, descubrir vulnerabilidades a mitigar, o bloquear conexiones maliciosas.

El despliegue de la solución es totalmente flexible, y se puede instalar on-prem o en la nube, mediante sensores hardware propiedad del cliente o del proveedor, o incluso de manera totalmente virtualizada.

Todo ello con el fin de que los responsables de planta puedan dormir tranquilos.

2.2. Beneficios.

Los beneficios del servicio Greinfort, se fundamentan en las siguientes características y capacidades.

Servicio de vigilancia y reporting: monitorización en tiempo real del estado de la ciberseguridad en fábrica, con reportes periódicos de riesgos, alertas y vulnerabilidades detectadas.
Foco: especializada en OT, no es una solución de IT adaptada. Se convierte así en el "vigilante lógico" de las fábricas, dando un paso más allá y sumándose a la habitual vigilancia física con la que ya contaban.

Mercado: está orientado, tanto a gran empresa, como a pymes, lo que permitirá democratizar su uso, así como a cualquier sector que tenga un proceso industrializado. Se trata, por tanto, de una solución altamente diversificable.

Precio y customización: se es consciente de que cualquier inversión en seguridad supone un gran esfuerzo económico ya que, por un lado, las soluciones comerciales suelen tener un coste elevado y, por otro, las soluciones *open source* requieren generalmente de personal técnico especializado para su gestión, además de estar sujetas a posibles riesgos como vulnerabilidades por falta de mantenimiento del código, o incluso abandono del proyecto y falta de soporte. La oferta es modulable en base al *bundle* de servicios contratados adicionales a Greinfort, y/o de los subcomponentes de la solución de vigilancia adquiridos, lo que otorga al cliente gran flexibilidad.

Facilidad de uso: La herramienta dispone de una interfaz sencilla con la que interactuará el cliente (versión desktop y mobile), y estará adaptada a perfiles no técnicos del área de fábrica, evitando complejas consolas con exceso de información.

Permisos basados en roles: permite definir qué capacidades asignar a cada operador de su compañía en la interacción con Greinfort.

Multisonda/multisede: Greinfort permite de forma nativa agregar fuentes de tráfico de diferentes sondas, ya sea en la misma planta, o dispersas geográficamente, de tal manera que todas ellas se puedan vigilar y gestionar desde la misma interfaz de usuario en el aplicativo.

No Intrusividad: Se trata de una solución no intrusiva, es decir, ofrece seguridad sin interferir en el funcionamiento habitual de la planta. La mayoría de las capacidades de detección se basan en técnicas pasivas de inferencia, y el escáner activo es muy poco agresivo, además de opcional.
Estandarización: Soporta los protocolos de comunicación OT más extendidos, esto es: Modbus TCP/IP, BACnet, Profinet, Siemmens communication, OPC UA, Ethernet/IP, DNP3, Ethernet POWERLINK, EtherCAT y Ether-S-Bus...

Tecnología: Integración con módulo de IA para prevención de ciberataques.

Alertas: Análisis de vulnerabilidades conectando con la NVD del NIST, detección de amenazas mediante firmas o patrones conocidos, IDS, IA/ML mediante diferentes algoritmos basados en el análisis de los resúmenes de las sesiones, o el payload de los paquetes, así como honeypots o señuelos.

Comunicaciones proactivas: las alertas pueden programarse para ser enviadas a operadores según configuración específica.

Análisis remoto: capacidad para poder realizar un análisis puntual del estado de una planta industrial sin desplegar la solución en fábrica, sino a través del estudio en remoto en laboratorio del tráfico proporcionado por el cliente en un fichero pcap.

- **Integración:** soporta bases de datos de vulnerabilidades de terceros y gran volumen de eventos.

- **Integración con terceros:** Greinfort provee la capacidad de enviar las alertas activas generadas a un tercer sistema como puede ser un SIEM (*Security Information and Event Management*), para su ingesta y correlación con otras fuentes de logs. Para ello, hace uso del protocolo syslog.

- **Escalabilidad:** el servicio puede crecer de manera fácil agregando más sondas a la solución de monitorización.

- **Interacción vía API:** para customizar integraciones de manera sencilla, para necesidades de cliente especiales.

2.3 Casos de uso.

Algunos casos de uso relacionados con las capacidades de la solución son los siguientes:
Inventario de activos: permite al cliente de manera totalmente automática averiguar qué dispositivos tiene en su red y las comunicaciones que realizan, tanto a nivel interno como contra el exterior; en la mayoría de los casos detectará dispositivos o rutas que ni siquiera tenía constancia de que se estaban produciendo. Lista todos los activos, permite asignarle etiquetas y propiedades, e incluso posibilita customizar la tabla con nuevas columnas para tener un inventario online y a medida.

- **Detección de dispositivos inalámbricos:** sobre todo útil en infraestructuras críticas o entornos en los que, por política de seguridad, se prohíbe a empleados y cadena de suministro acceder con terminales móviles. Inventaría y controla todos los elementos WiFi y Bluetooth en las inmediaciones de la sonda.

- **Mapa de red:** dibuja en tiempo real el diagrama de red de su planta (o subredes) industriales, tanto a nivel topología, como cumplimiento normativo. Permite detectar problemas a nivel visual y revisar problemas de segmentación que no cumplan con las buenas prácticas de los modelos PURDUE e ISA/IEC 62443, de cara a hacer una segregación adecuada de zonas y conductos.

- **Detección de anomalías:** genera, en tiempo real y de manera totalmente automática, anomalías basadas en diferentes estrategias para la protección de la planta industrial:

    - Reglas estáticas (nuevas conexiones, dispositivos, cambios de puerto o protocolo, fingerprinting, man-in-the-middle...).
    - Sistema de detección de intrusiones.
    - Algoritmos de IA/Machine learning que analizan el tráfico de la red.

Estas anomalías se traducen en alertas que el cliente podrá gestionar en todo su ciclo de vida desde la interfaz, mediante las notificaciones proactivas o en un tercer sistema como es su SIEM, para asegurar la planta.

- **Vulnerabilidades:** la identificación de vulnerabilidades asociadas a servicios desplegados en los dispositivos presentes en la red permite su adecuada gestión (parcheado físico o virtual, por ejemplo), para evitar que las debilidades sean explotadas por un atacante.

- **UEBA:** caso de uso especial de anomalía basada en variables de proceso. Mediante técnicas de minería de procesos, pueden detectarse irregularidades que impacten a nivel de ciberseguridad, o incluso seguridad física (*safety*) de empleados o de clientes (por manipulación de los procesos productivos).

- **Honeypot:** caso de uso especial de detección de anomalías, mediante sistema señuelo. No solo permite detectar una potencial amenaza, sino conocer con cierto detalle las técnicas utilizadas por el adversario.

- **Bloqueo de tráfico:** capacidad de bloqueo de conexiones maliciosas desde la red industrial con el exterior, mediante integración con el firewall del cliente. Totalmente opcional y de política configurable (informativa, semi-supervisada o automática). Permite automáticamente mitigar amenazas externas.

- **Análisis de tráfico:** trazabilidad de comunicaciones entre dispositivos de la red interna o para con el exterior, útil de cara a realizar análisis forenses y/o segregar adecuadamente la red.

- **Reportes de servicio:** informes automáticos con carácter periódico con información relevante del servicio, para facilitar el procesamiento de información. Reportes de vulnerabilidades, equipos no autorizados, niveles de *scoring*, conexiones contra IPs externas, etc.

- **Cumplimiento normativo:** todas las capacidades de identificación, protección, detección y respuesta previamente descritas dan soporte a la implantación de ciertas medidas de seguridad impuestas por normas y estándares nacionales e internacionales de seguridad, como pueden ser ISO27001, ENS, ISA/IEC 62443, NIST CSF, NIS2, etc.

2.3. Diferenciadores.

Existen otras soluciones en el mercado, algunas de cuyas capacidades se asemejan a las de Greinfort. Los aspectos diferenciadores que considerar son los siguientes:

- **Simplicidad:** Greinfort es una herramienta simple, intuitiva y de fácil uso. Tenemos años de experiencia en el área de producto de ciberseguridad y consideramos que esto es clave para su éxito, puesto que los usuarios no necesitan ser expertos para

gestionar su seguridad en planta, ni ofrecemos (y cobramos) por funcionalidad superflua.

- **No necesidad de externalización:** la tecnología es de tan fácil manejo, que subcontratar su gestión será una decisión puramente de negocio, y no de competencias técnicas.

- **Flexibilidad:** Greinfort se ofrece con diferentes modalidades para adaptarse a las necesidades del cliente.

- **Asequible:** tratamos de democratizar el acceso a este tipo de tecnología, que originalmente debido a su alto coste estaba únicamente reservado a grandes empresas o multinacionales, para que pueda ser contratada incluso por cualquier PyME con procesos productivos industriales de alto valor.

- **Customizable:** escuchamos al cliente y sus necesidades. Muchas de las capacidades y mejoras asociadas al servicio provienen directamente del *feedback* de nuestros clientes.

- **Soberanía nacional:** debido al panorama geopolítico turbulento actual, muchas organizaciones y administraciones públicas regionales, nacionales y comunitarias están desincentivando la contratación y uso de soluciones foráneas (USA, Israel, Rusia…). Nuestra solución es 100% producto *made in EU* (Galicia, España), tanto a nivel de I+D como de soporte de fabricante.

Greinfort Solutions S.L
Maria Berdiales 20, 4th fl.
36203 | Vigo | Spain
(+34) 886 251 058
info@greinfort.com

greinfort.com