



HOJA DE DATOS

Asset Intelligence

Céntrese en los incidentes de TO e IoT que de verdad importan

Nozomi Networks **Asset Intelligence™** actualiza de manera continua los sensores de **Guardian™** con datos enriquecidos de dispositivos de TO e IoT para que pueda identificar y resolver rápidamente las alertas de seguridad más importantes.

La detección de anomalías de Guardian para IoT utiliza millones de perfiles de recursos de TO e IoT para identificar recursos y generar alertas sobre anomalías para toda la empresa.

Vea

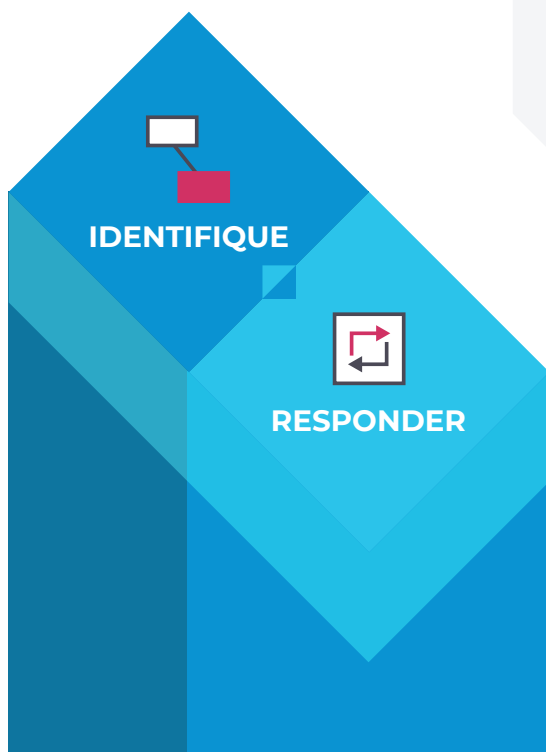
Todos los comportamientos y dispositivos de TO e IoT en sus redes para un conocimiento sin igual

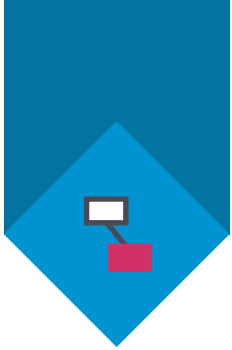
Detecte

Amenazas, vulnerabilidades, riesgos y anomalías cibernéticos para una respuesta más rápida

Unifique

Amenazas, vulnerabilidades, riesgos y anomalías cibernéticos para una respuesta más rápida





Identifique

Inteligencia que reduce el tiempo medio de respuesta (MTTR)

Identifique rápidamente las anomalías peligrosas

Datos actualizados de dispositivos de TO e IoT

Clasifica los recursos con gran precisión para acelerar el proceso de aprendizaje para entornos de TO e IoT

Compara la actividad en tiempo real con las líneas de base seguras, incluso durante la fase de aprendizaje, a fin de detectar comportamientos potencialmente peligrosos

Datos enriquecidos de perfiles de recursos y de comportamientos

Proporciona información detallada sobre los dispositivos, que incluye:

- Tipo
- Fabricante
- Comportamiento
- Configuración (software instalado)
- Protocolos utilizados

Elimine automáticamente las alertas sobre anomalías benignas

Detección avanzada de anomalías para IoT

Utiliza la inteligencia de millones de perfiles de recursos de TO e IoT para determinar cuándo generar alertas sobre comportamientos anómalos

Elimina las alertas generadas por comportamientos anómalos que son benignos, ya que reconoce cuándo algo «nuevo» o «diferente» no representa un riesgo, de modo que usted puede concentrarse en los incidentes «reales»

Proporciona el contexto para gestionar los riesgos de TO e IoT

Ofrece información constantemente actualizada que proviene del monitoreo de millones de recursos para reconocer los comportamientos «normales»

Compara los comportamientos nuevos con los perfiles de dispositivos para identificar riesgos de confiabilidad ocasionados por amenazas cibernéticas y anomalías operativas

Detección de anomalías de avanzada para TO e IoT



Identificación rápida de recursos

Garantiza un inventario de recursos preciso



Alertas precisas de anomalías

Acelera la respuesta ante incidentes



Asset Intelligence para redes dinámicas

Mantiene un inventario y una detección precisos



Responder

Alertas detalladas y herramientas forenses para una respuesta rápida

Responder rápidamente utilizando información precisa y detallada

Analizar rápidamente los incidentes y simplificar los procesos de TI/TO

Inteligencia de recursos precisa

Garantiza perfiles de recursos actualizados a través de la experiencia de Nozomi Networks Labs, un equipo de investigadores especializados en seguridad

Ofrece perfiles precisos basados en el análisis de millones de dispositivos en uso en distintos sitios de todo el mundo y en el laboratorio de pruebas de Nozomi Networks

Procesos de seguridad de TI/TO simplificados

Reduce los costes con una única solución integral de detección de anomalías de TO e IoT

Se integra con la infraestructura de seguridad de TI para simplificar los procesos de seguridad; consult: nozominetworks.com/integrations

Armoniza los datos de seguridad en las herramientas empresariales para una respuesta coherente

Alertas útiles y detalladas

Proporciona alertas detalladas que detectan anomalías importantes de seguridad y confiabilidad

Agrupar las alertas por incidentes, proporcionándole al personal de seguridad y de operaciones una vista simple, clara y consolidada de lo que está sucediendo en la red

Análisis forense rápido

Centra los esfuerzos con Smart Incidents™, que:

- Correlaciona y consolida las alertas
- Proporciona un contexto operativo y de seguridad
- Suministra capturas automáticas de paquetes

Decodifica incidentes con Time Machine™ antes y después de las instantáneas del sistema

Proporciona respuestas rápidas con una poderosa herramienta de consultas ad hoc



La investigación continua de recursos reduce el tiempo de respuesta ante anomalías perjudiciales y amenazas activas.

Productos y Servicios



SAAS

Vantage acelera la respuesta de seguridad con una detección de amenazas y una visibilidad inigualables en sus redes de OT, IoT y TI. Su plataforma SaaS ampliable le permite proteger varios recursos, en cualquier lugar. Puede responder con mayor rapidez y eficacia a las amenazas cibernéticas, garantizando una resiliencia operativa.

Requiere sensores



PERÍMETRO O NUBE PÚBLICA

Guardian proporciona una seguridad y una visibilidad de TO e IoT robustas para la industria. Combina detección de recursos, visualización de redes, evaluación de vulnerabilidades, control de riesgos y detección de amenazas en una sola aplicación. Guardian comparte datos tanto con Vantage como con CMC.



PRODUCTO

The **Central Management Console** (CMC) consolida el control de riesgos y la visibilidad de TO e IoT en todos sus sitios distribuidos, tanto en el perímetro como en la nube pública. Se integra con su infraestructura de seguridad de TI para lograr flujos de trabajo optimizados y respuestas más rápidas ante amenazas y anomalías.



SUSCRIPCIÓN

El servicio **Asset Intelligence** ofrece actualizaciones de perfil regulares para lograr una detección más rápida y más precisa de las anomalías. Lo ayuda a enfocar los esfuerzos y reducir el tiempo promedio de respuesta (MTTR).



SUSCRIPCIÓN

El servicio **Threat Intelligence** ofrece inteligencia continua para amenazas y vulnerabilidades de TO e IoT. Le ayuda a estar al tanto de las amenazas emergentes y de las nuevas vulnerabilidades y a reducir su tiempo promedio de detección (MTTD).



COMPLEMENTO DE GUARDIAN

Smart Polling agrega sondeo activo de bajo volumen a la detección pasiva de recursos de Guardian, mejorando el rastreo de recursos, la evaluación de vulnerabilidades y la monitorización de seguridad.



COMPLEMENTO DE GUARDIAN

Los **Recolectores de datos para sitios remotos** son sensores de bajos recursos que capturan datos desde las ubicaciones distribuidas y los envían a Guardian para su análisis. Mejoran la visibilidad y reducen los costes de implementación. deployment costs.

Nozomi Networks

La solución líder para la seguridad y la visibilidad de la tecnología operativa y del internet de las cosas

Nozomi Networks acelera la transformación digital protegiendo la infraestructura crítica así como a las organizaciones industriales y gubernamentales de las ciber-amenazas. Nuestra solución proporciona una visibilidad excepcional de la red y de los activos, capacidad de detección de amenazas e información detallada sobre los entornos OT e IoT. Los clientes confían en nosotros para minimizar el riesgo y la complejidad al tiempo que maximizan la resiliencia operativa.