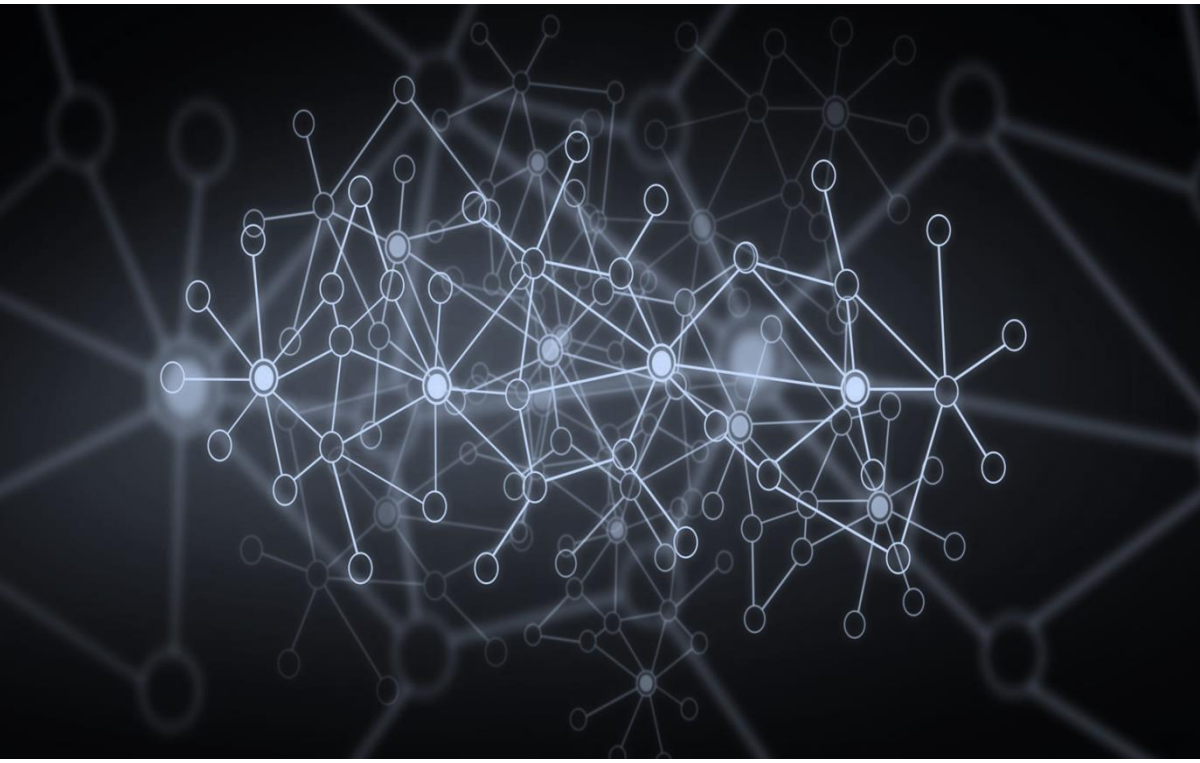
Seguridad Industrial



Cómo prevenir ciberataques en redes de control industrial

GRUPO CMC
Calle Caleruega 81, 3ª planta
28033 Madrid
(+34) 91 555 62 38
marketing@grupocmc.es
http://www.grupocmc.es

Hablamos de ciberseguridad y el uso de Machine Learning y la Inteligencia Artificial (IA) para prevenir ciberataques en redes de control industrial.

En los últimos años, los Sistemas de Control Industrial de los que depende gran parte de nuestra infraestructura crítica y nuestra industria manufacturera, han sido objetivos cada vez más de sofisticados ciberataques.

En parte, esto es una consecuencia de la inevitable convergencia de la Tecnología Operacional (OT) con la Tecnología de la Información (TI). Como en todas las esferas de la informática, las ventajas de una mayor conectividad de red a través de estándares abiertos como Ethernet y TCP / IP, así como el ahorro de costes derivado de la sustitución de equipos propietarios industriales por hardware y software estándar, tienen el costo de mayor vulnerabilidad.

Sin embargo, aunque el impacto de una violación de seguridad en la mayoría de los sistemas de TI se limita a pérdidas financieras, los ataques a redes de control industrial tienen el potencial adicional de destruir equipos, amenazar la seguridad nacional e incluso poner en peligro la vida humana.

Con esta distinción fundamental también surge una diferencia preocupante en los perfiles y las motivaciones de posibles atacantes. Si bien la mayor parte del ciber crimen moderno está motivado por la recompensa financiera, las redes de control industrial se han convertido recientemente en objetivos atractivos para el terrorismo y la guerra cibernética. Como consecuencia, los recursos financieros y humanos disponibles para sus perpetradores pueden ser un orden de magnitud mayor que los de los ciber delincuentes convencionales.

¿Porque la necesidad de una solución como **SCADAguardian**?
En el pasado no muy lejano, las redes de control industrial no eran vulnerables a ciberataques ya que estas:

- Estaban aislado de IT
- Ejecutaban bajo protocolos propietarios
- Incorporaban hardware especializado
- Funcionaban con sistemas operativos propietarios
- Y usaban redes físicas distintas a las de IT

Hoy en día esta situación ha cambiado drásticamente. Las instalaciones industriales son especialmente vulnerables a ciberataques:

- Las redes de control industrial están Integradas con la red IT empresarial.
- Más y más las redes de control industrial utilizan protocolos de internet
- Funciona con hardware de uso general con orígenes informáticos
- Utilizando sistemas operativos de IT convencionales y en muchos casos obsoletos como el caso del uso continuado de sistemas operativos como WIN XP.
- Cada vez se utiliza más fibra y redes inalámbricas

Los Componentes de Redes de Control Industrial son en gran parte la causa de esta vulnerabilidad. Los PLC y RTU son computadoras de baja rendimiento diseñadas para controlar componentes físicos como válvulas, bombas, motores, etc.

Se comunican a través de protocolos propietarios que son propensos a ataques personalizados y sufren otras vulnerabilidades como:

- La falta de autenticación
- La falta de encriptación
- Puertas traseras
- Desbordamiento de búfer
- Ataques personalizados para controlar componentes físicos

A pesar de estos y muchos otros desafíos, hay soluciones como **SCADAguardian** de Nozomi Networks que pueden ayudar a garantizar la seguridad y fiabilidad de las redes de control industrial, y en particular aquellas que emplean soluciones de Control de Supervisión y Adquisición de Datos (SCADA).

Aprendizaje Del Entorno – Uso de Machine Learning e Inteligencia Artificial
Durante la primera fase de la implantación (fase aprendizaje) Nozomi Networks crea automáticamente un mapa del entorno en el que se despliega y escanea sus componentes para detectar vulnerabilidades. Los algoritmos de detección que incorpora también examinan la configuración de cada sistema y comprueban si existen problemas que podrían suponer fisuras ante posibles ataques.

Algunas de las funcionalidades principales de **SCADAguardian** se resumen:
Detecta Intrusiones

- Exploración y ataques MITM
- Ataques complejos o de día cero

Detecta comportamiento No Autorizado

- Acceso remoto

- Configuraciones no autorizadas
- Descargas
- Cambios en la lógica del controlador
- Modificaciones en proyectos PLC
- Conexiones a Internet o red empresarial
- Autenticación PLC y más

Detecta Vulnerabilidades

- Identificación automatizada de activos con vulnerabilidades
- Vista dedicada y con búsqueda de todas las vulnerabilidades con sus severidades

Detecta Incidencias de Estado

- Configuraciones erróneas
- Contraseñas o configuraciones débiles
- Parches que faltan
- Vulnerabilidades conocidas
- Puertos abiertos
- Activos nuevos o no sensibles
- Comunicación de nivel cruzado o de zona
- Tormentas de tráfico generadas por dispositivos
- Mal funcionamiento de comunicaciones de Internet inseguras
- Comunicación no encriptada
- Fallas de comunicación

Aprende Automáticamente

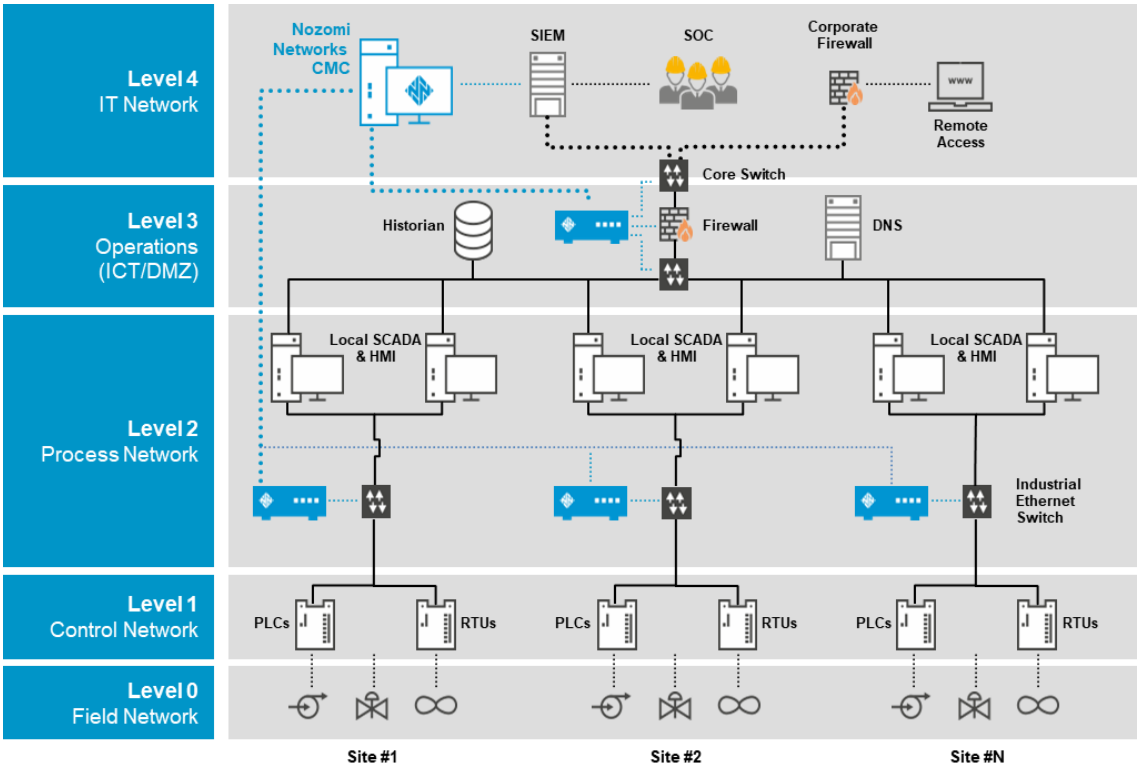
- No se requiere ninguna intervención manual para cambiar el producto de modo aprendizaje al modo de protección, aunque se puede operar en modo manual si se desea.
- La detección de anomalías y la vigilancia de seguridad cibernética comienzan lo más rápido posible

La solución **SCADAguardian** es actualmente la más avanzada del mercado debido a tres factores fundamentales:

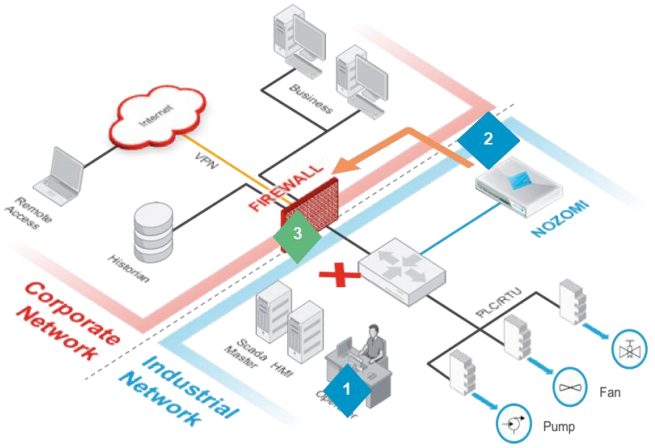
- Su capacidad de análisis del comportamiento de la infraestructura industrial en tiempo real.
- La detección avanzada de ciberataques basada en firewall; la visibilidad total de las operaciones en diferentes plantas o centros a través de cuadros de mando personalizables.
- De fácil integración en los propios sistemas de los operadores.

Su capacidad para operar en tiempo real permite enriquecer la información recopilada sobre el entorno con datos reales de actividad y crear un perfil actualizado de las operaciones. Este modelo es utilizado por los algoritmos de detección de amenazas como referencia para determinar si cierta acción se corresponde con el comportamiento rutinario del sistema o si se trata, por el contrario, de un incidente anómalo que precisa atención como, por ejemplo, llamadas masivas a un sistema desde una red de bots.

Ejemplo de arquitectura



Protección Activa - Integración con Firewall



1 Monitorization
SCADAguardian detecta las siguientes amenazas:

- Detecta Intrusiones
- Detecta Comportamiento no autorizado
- Detecta vulnerabilidades
- Detecta incidencias de estado

2 Detection
Las políticas definidas por el usuario se examinan rápidamente y se activa la acción correspondiente

3 Protección Activa
El firewall responde de acuerdo con la acción configurada por el usuario (bloqueo de nodo, bloqueo de enlace o sesión de eliminación) y mitiga el problema.
Nozomi se integra con NGFW de Fortinet, Palo Alto, y Checkpoint

Alerta y Toma de Decisiones Automatizadas

En la fase de explotación, la solución envía alertas automáticamente a través de un mecanismo de notificación integrado para que los administradores dispongan de información sobre la causa del problema.
Cuando SCADAguardian es empleada con la solución de cortafuegos de Fortinet, la solución en su conjunto es capaz de modificar automáticamente la política de cortafuegos en los FortiGate para bloquear el tráfico sospechoso en tiempo real (bloque de nodo, bloque de enlace, o terminación de la sesión).
La solución proactiva de Fortinet-Nozomi Networks proporciona una solución de detección sofisticada proactiva para las redes de control industrial con remediación y contención proactiva de amenazas dentro de un entorno industrial.

Gestión Centralizada

SCADAGuardian también ofrece una única plataforma de gestión centralizada que permita gestionar miles de dispositivos, ofreciendo las siguientes características:
Visibilidad centralizada y detección de amenazas: Ofrece cuadros de mando configurables que muestran la seguridad cibernética y las métricas operativas clave para la red de control industrial. También ofrece una herramienta de reporting dinámico que brinda respuestas inmediatas sobre cualquier aspecto del estado de la red o del proceso.

Arquitectura escalable y flexible: La aplicación se escala fácilmente a miles de sitios industriales con un rendimiento óptimo. Incluye la opción de configuración multiusuario

Solución de Clase Empresarial: El control de acceso a la aplicación es granular y basado en roles. La aplicación ofrece integración con los SIEM de mercado más comunes, firewalls y sistemas de autenticación de usuarios. La integración con entornos IT / OT mediante Open API y Protocol SDK simplifica cualquier integración.

En la actualidad, SCADAguardian monitoriza más de 100.000 dispositivos industriales de clientes multinacionales, entre los que se cuenta el gigante energético italiano Enel, que proporciona electricidad a más de 61 millones de clientes en el mundo.