La solución StationGuard

Monitoreo de ciberseguridad y funcional de la red eléctrica

La solución StationGuard

Visibilidad

Haga visibles sus comunicaciones y riesgos.

Detección de intrusión y amenazas

Utilice la innovadora metodología de lista de elementos permitidos para un análisis superior y una respuesta eficiente.

Gestión de vulnerabilidades

Investigue las amenazas reales que pesan sobre sus activos mediante una visión tanto general como detallada.

Inventario de activos

Trabaje con la lista de activos más precisa y detallada.

Monitoreo funcional

Detecte las anomalías de los dispositivos, los problemas de comunicaciones y los errores de configuración.

Sensores StationGuard

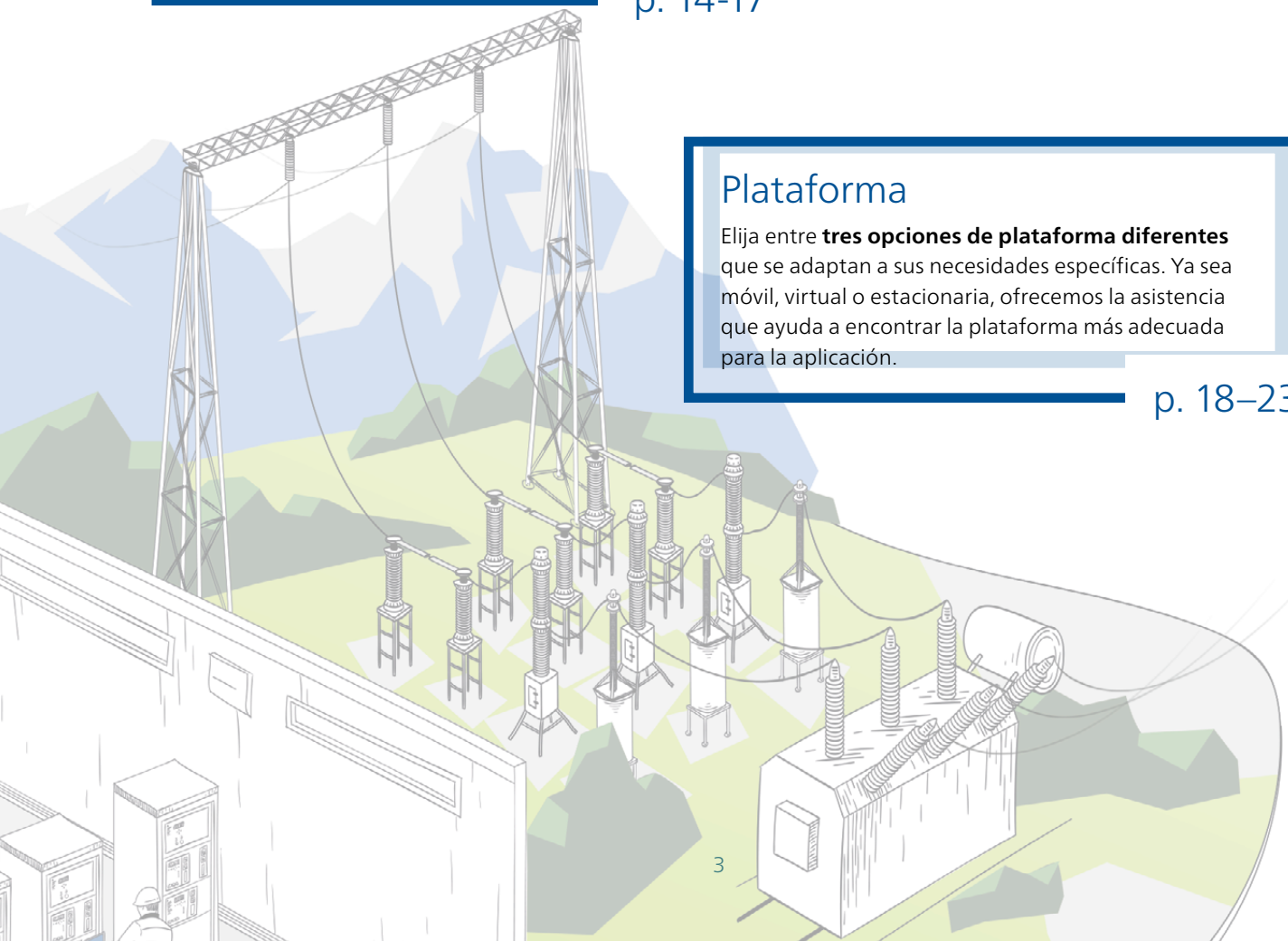
Descubra nuestra **innovadora metodología de lista de elementos permitidos (lista blanca)** para la máxima seguridad y utilidad tanto para los responsables de seguridad informática como para los ingenieros de SCADA y protección. Se detectan y analizan las ciberamenazas y los problemas funcionales y de comunicaciones, garantizando la seguridad hasta el más mínimo detalle.

p. 4-13

Componente GridOps

El **potente sistema de gestión centralizada** ofrece un análisis exhaustivo de las alertas y la investigación de las amenazas. Mejore la gestión de las vulnerabilidades y consiga una visibilidad total de la red para mantener el control.

p. 14-17



Plataforma

Elija entre **tres opciones de plataforma diferentes** que se adaptan a sus necesidades específicas. Ya sea móvil, virtual o estacionaria, ofrecemos la asistencia que ayuda a encontrar la plataforma más adecuada para la aplicación.

p. 18–23

Seguridad informática en la red eléctrica

En los últimos años, se ha producido un aumento de los ciberataques contra los sistemas de control críticos en las instalaciones de producción y las empresas de suministro de energía. Por ello, muchas compañías eléctricas están introduciendo procesos para reducir el riesgo de ciberataques. Estas medidas se han centrado principalmente en las redes informáticas y los centros de control. Sin embargo, las subestaciones, las centrales eléctricas y las redes constituyen vectores de ataque críticos. En consecuencia, los procesos de explotación y mantenimiento de estas plantas también deben incluirse en la evaluación de riesgos de ciberseguridad.

Para garantizar que la red eléctrica esté completamente protegida contra los ciberataques, la estrategia de seguridad tiene que abordar cada nivel. El concepto de seguridad abarca desde el control de acceso físico hasta el monitoreo digital del acceso y el monitoreo de actividades sospechosas o prohibidas en la red. Esto requiere sistemas que ofrezcan un alto nivel de seguridad con un bajo mantenimiento a largo plazo. Además, deben ser fáciles de integrar en los flujos de trabajo operativos y de mantenimiento.

Cortafuegos

Los servidores de seguridad o cortafuegos garantizan que sólo determinados puntos finales puedan comunicarse con los dispositivos que hay detrás, utilizando únicamente los protocolos permitidos. Sin embargo, hay formas de eludir los servidores de seguridad.

Puntos de ataque que burlan los servidores de seguridad:

Acceso remoto para el mantenimiento y el control.

PC de mantenimiento conectados a la red o directamente a los IED.

PC de prueba conectados al bus de la estación.

Archivos transferidos a los PC utilizados en la subestación.

El núcleo desprotegido

> Sistemas críticos, cuya comunicación debe funcionar de forma confiable.

> IED sin parchear: Las actualizaciones no se pueden instalar con suficiente rapidez debido al esfuerzo que supone.

> Dispositivos antiguos con vulnerabilidades de seguridad que ya no se pueden actualizar.

Los cortafuegos no proporcionan una protección en profundidad

Hay muchas maneras de eludir un cortafuegos. Muchos sitios emplean el acceso remoto para recuperar registros de fallas o para el mantenimiento. Estas conexiones proporcionan una vía por la que puede introducirse malware en los dispositivos de una subestación.

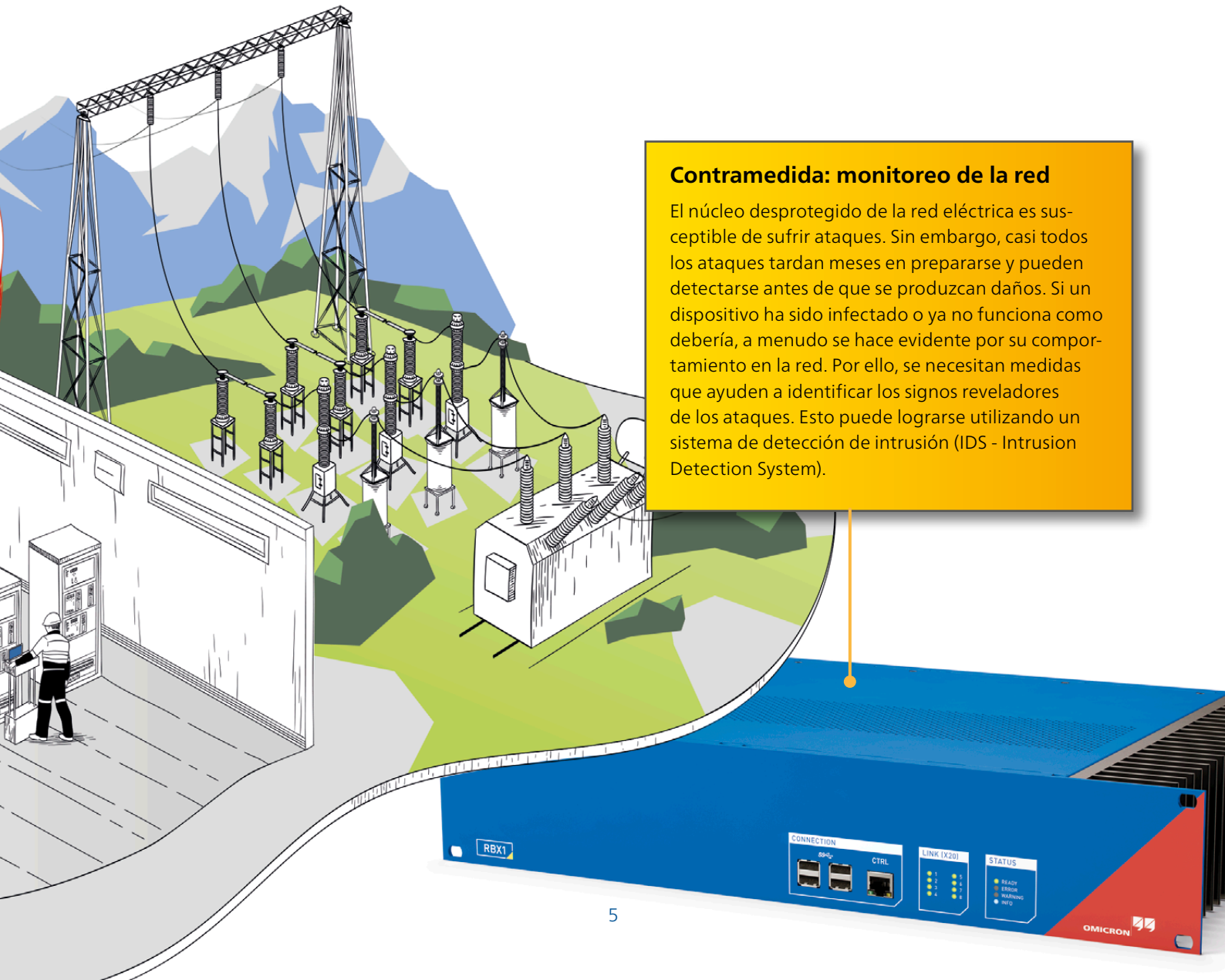
Los PC de mantenimiento y pruebas constituyen otro vector de ataque. Estos PC están conectados a toda la red o directamente a dispositivos de protección o control individuales.

Defensa en profundidad

El principio de defensa en profundidad, tal y como se establece en la norma IEC 62443, no sólo recomienda aplicar medidas que "endurezcan la coraza", sino que también introduce varias capas y niveles de repliegue que ayudan a proporcionar un nivel de seguridad por zonas.

Una de estas medidas son las actualizaciones de seguridad de los IED. Sin embargo, el esfuerzo y el coste que conllevan son elevados, por lo que las actualizaciones no siempre pueden instalarse con la suficiente rapidez. La imposibilidad de actualizar los dispositivos antiguos es habitual si el proveedor no proporciona actualizaciones.

Por lo tanto, estos sistemas deben monitorearse para garantizar la detección temprana de los ataques y minimizar sus consecuencias.



Contramedida: monitoreo de la red

El núcleo desprotegido de la red eléctrica es susceptible de sufrir ataques. Sin embargo, casi todos los ataques tardan meses en prepararse y pueden detectarse antes de que se produzcan daños. Si un dispositivo ha sido infectado o ya no funciona como debería, a menudo se hace evidente por su comportamiento en la red. Por ello, se necesitan medidas que ayuden a identificar los signos reveladores de los ataques. Esto puede lograrse utilizando un sistema de detección de intrusión (IDS - Intrusion Detection System).

Cómo funcionan los sistemas de detección de intrusión (IDS)

Los sistemas de detección de intrusión se basan típicamente en una de estas dos metodologías:

1. Metodología basada en firmas (lista de bloqueo)

El IDS busca patrones de ataques conocidos. Los escáneres de virus también utilizan esta metodología. Los sistemas de este tipo tienen una tasa de falsas alarmas más baja que las metodologías basadas en el aprendizaje. La principal desventaja es que hasta ahora se han conocido pocos ataques a los dispositivos de protección y control. Sin embargo, incluso la primera aparición de un ataque puede tener consecuencias graves, lo que significa que no tiene mucho sentido adoptar el método basado en firmas para la detección de la intrusión en la red eléctrica.

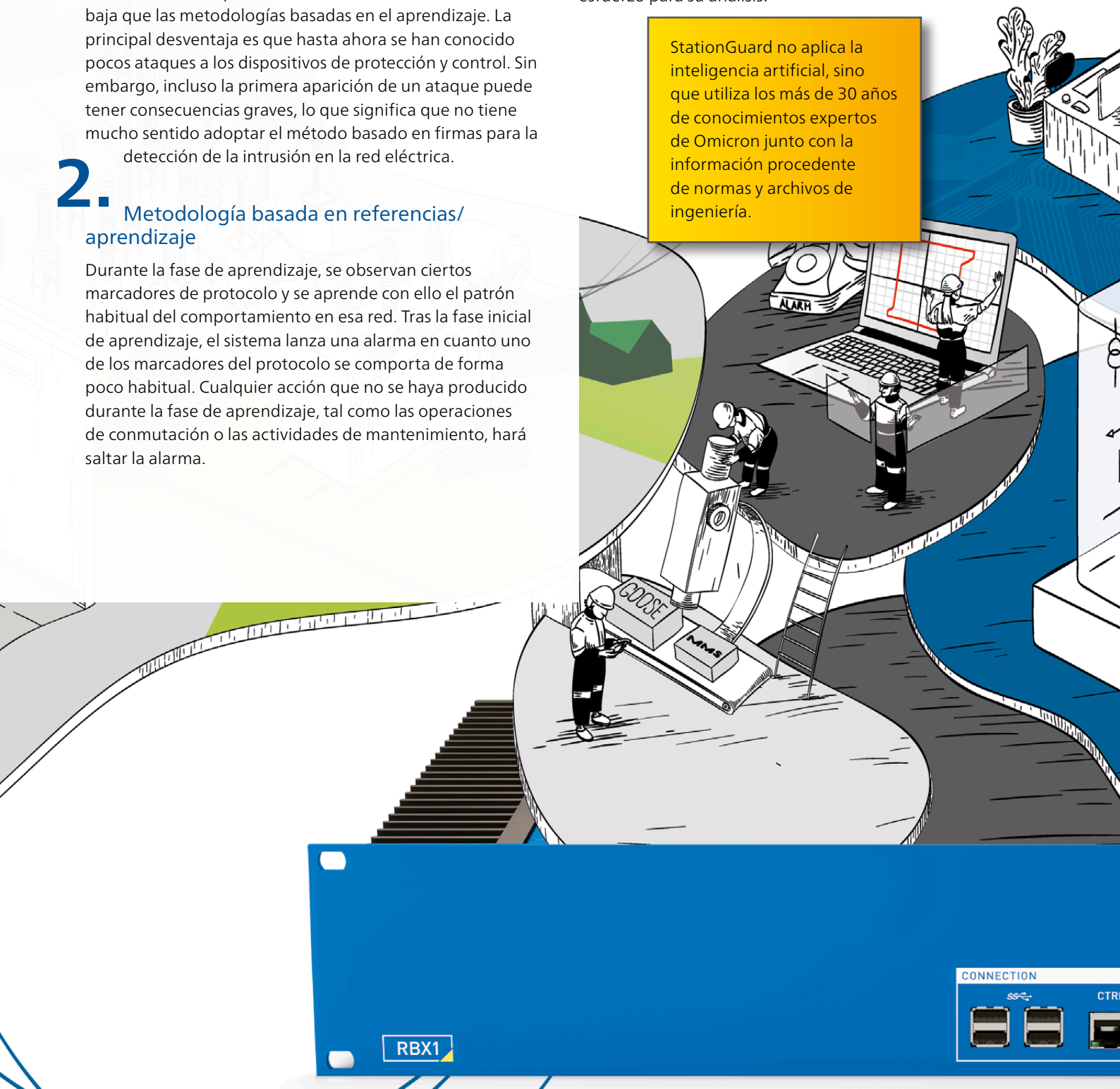
2. Metodología basada en referencias/ aprendizaje

Durante la fase de aprendizaje, se observan ciertos marcadores de protocolo y se aprende con ello el patrón habitual del comportamiento en esa red. Tras la fase inicial de aprendizaje, el sistema lanza una alarma en cuanto uno de los marcadores del protocolo se comporta de forma poco habitual. Cualquier acción que no se haya producido durante la fase de aprendizaje, tal como las operaciones de conmutación o las actividades de mantenimiento, hará saltar la alarma.

3.

Además, el sistema sólo conoce los marcadores de protocolo, pero no entiende lo que está sucediendo en la subestación. Esto significa que los mensajes de alarma producidos sólo pueden ser interpretados por especialistas en informática que tengan conocimientos de automatización de compañías eléctricas. Por lo tanto, hay un elevado número de alarmas que requieren mucho esfuerzo para su análisis.

StationGuard no aplica la inteligencia artificial, sino que utiliza los más de 30 años de conocimientos expertos de Omicron junto con la información procedente de normas y archivos de ingeniería.



La metodología de StationGuard

Los sistemas de automatización y SCADA de las compañías eléctricas son deterministas, lo que significa que su comportamiento está claramente definido, incluso en situaciones excepcionales, por ejemplo, durante incidencias de protección.

Aprovechando esta característica, se puede aplicar una metodología completamente nueva para la detección de ciberataques. Dado que conoce la función de cada dispositivo, StationGuard crea un modelo de todo el sistema de automatización y, a continuación, compara en directo cada uno de los paquetes de la red con este modelo del sistema. Esto corresponde a una metodología de lista de elementos permitidos (lista blanca), en la que se describen todos los comportamientos permitidos y todo lo que se desvíe de ellos activa una alarma. Con esta metodología también pueden detectarse tipos de ataques completamente nuevos.

La lista de elementos permitidos de StationGuard entra en detalle a un nivel granular. Incluso los valores de las señales en los mensajes se evalúan utilizando el modelo del sistema. Esto no sólo permite detectar ciberamenazas y actividades prohibidas, sino que también se pueden detectar problemas en las funciones de automatización y SCADA. Por eso hemos denominado a la combinación de detección de intrusión y monitoreo de funciones "Monitoreo de seguridad funcional". Llevamos investigando esta metodología desde 2010. La combinación de conocimientos sobre el sistema eléctrico y la seguridad es lo que hace que StationGuard sea tan eficaz.

No es necesaria una fase de aprendizaje para configurar StationGuard. Sólo se requiere que el usuario haga algunas descripciones de la finalidad de cada dispositivo. En el caso de los sistemas IEC 61850, este proceso puede acelerarse ampliamente importando archivos SCL.

Ventajas

- Pocas falsas alarmas, ya que StationGuard conoce los procesos de los sistemas eléctricos
- Las alarmas son comprensibles sin conocimientos de los protocolos
- Detección confiable de acciones no autorizadas

La metodología de lista de elementos permitidos (lista blanca) de Stat

Seguridad a nivel granular

El hecho de que todo el tráfico de la red se monitoree y valide con gran detalle significa que no sólo se detectan las amenazas a la seguridad informática, tales como las codificaciones ilegales y las operaciones de control no autorizadas. StationGuard también identifica errores de comunicación, problemas de sincronización horaria y, a partir de ahí, diferentes tipos de anomalías en la subestación. Si el IDS también aplica el diagrama unifilar, entonces no hay prácticamente ningún límite a la profundidad a la que se puede llevar a cabo el monitoreo.

Por ejemplo: actualmente, StationGuard reconoce 35 códigos de alarma diferentes para GOOSE, que van desde simples errores en el número de secuencia hasta mediciones complejas, tales como retardos excesivamente largos en la transmisión de mensajes. En este último caso, se miden los tiempos de llegada de los paquetes y se comparan con las marcas horarias de los eventos dentro de los mensajes. Si el tiempo de transmisión medido es más largo de lo que permite la norma IEC 61850-5, StationGuard emite una alarma que indica que puede haber un problema con el IED remitente, la red o la sincronización horaria.

Se analiza con el mismo grado de detalle en el caso del protocolo IEC 60870-5-104. Station-Guard también guarda informes de estados críticos y errores de codificación para docenas de otros protocolos de tecnología operativa.

Comunicaciones MMS, IEC 60870-5-104 y DNP3

StationGuard sabe qué puntos de datos controlan qué funciones. Por ejemplo, el mismo comando puede utilizarse para controlar un interruptor de potencia, un cambiador de tomas y para cambiar los ajustes del modo de prueba de un dispositivo. El efecto en la subestación es muy diferente en cada caso. StationGuard puede hacer esta distinción y sabe qué dispositivo debe controlar qué y en qué situación. Estos permisos ajustados están documentados y pueden revisarse en StationGuard.

Otros protocolos

StationGuard realiza una inspección a fondo de paquetes en docenasprotocolos, tanto de sistemas eléctricos como de IT clásica. Así, StationGuard no sólo detecta violaciones del código en estos protocolos, sino también si los números de puerto, p. ej., de las conexiones remotas, son secuestrados por aplicaciones no previstas (suplantación de puertos).

Protocolos soportados (inspección profunda de paquetes)

- IEC 61850
- IEC 60870-5-104
- DNP3
- PRP/HSR
- ModBus TCP
- Sincrofasor
- DLMS/COSEM
- AMI
- TASE.2/ICCP
- S7
- EtherCAT
- Profinet
- ...
- FTP, HTTP
- RDP
- NTP
- ARP, DHCP, ICMP
- MySQL, MS SQL, PostgreSQL
- HTTPS, SSH (detección de aplicaciones, sin descifrado)
- telnet
- RIPv2
- SSDP
- ...

Ventajas

> Cada paquete se compara con el modelo del sistema (lista de elementos permitidos)

> Se detectan problemas funcionales y de comunicaciones, además de ciberamenazas

> StationGuard supervisa la función de seguridad de todas las comunicaciones en la subestación y el sistema SCADA

Respuestas más rápidas con mensajes de alerta comprensibles

Para configurar, operar y mantener los sistemas de detección de intrusión (IDS) convencionales, se necesitan tanto especialistas en informática como técnicos de automatización y control. Ambos tipos de especialistas deben estar de guardia las 24 horas del día para ayudar a analizar la causa de las alarmas. Los costes que esto conlleva son inaceptables para muchas compañías eléctricas. StationGuard ofrece a las compañías eléctricas una nueva alternativa de bajo mantenimiento.

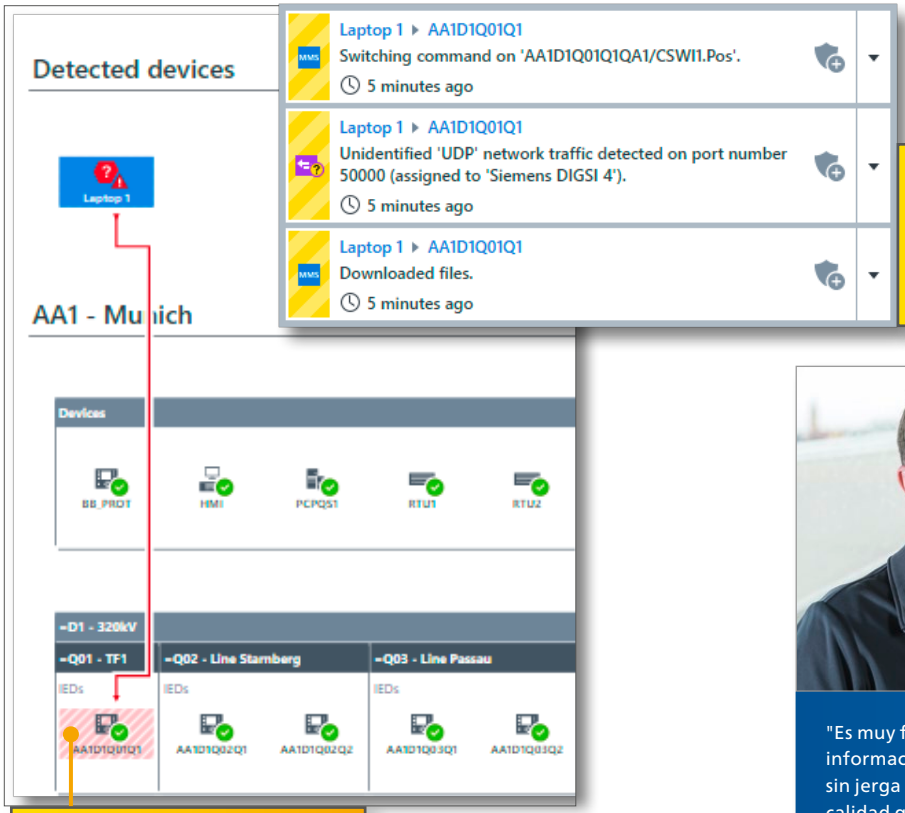
StationGuard conoce las funciones típicas de las subestaciones y cómo está previsto que se utilicen los equipos informáticos, tales como los PC de ingeniería y PC de pruebas. Como toda esta información está disponible de forma automática, StationGuard se configura rápidamente y está listo para proteger la red, sin necesidad de ninguna fase de aprendizaje.

Identificar de forma confiable la causa de las alertas

Las alertas desencadenadas por un sistema de seguridad deben ayudar al operador, no causar más confusión. Por lo tanto, las alertas del StationGuard no sólo aparecen en una lista de eventos, sino que se muestran gráficamente en el diagrama general. Los eventos del sistema eléctrico detrás de los paquetes de red se identifican y se muestran con una terminología clara.

Consideremos el siguiente ejemplo: Un PC de pruebas intenta controlar el interruptor de potencia utilizando el protocolo MMS. El mensaje de alerta correspondiente no se visualiza utilizando términos de protocolo, sino que se interpreta en función de lo que realmente ocurrió en la subestación. Contiene información del siguiente tipo: ¿Qué ha ocurrido exactamente? ¿Cuál es el dispositivo responsable?

Esto permite a los responsables de seguridad informática, así como los ingenieros de SCADA y de protección colaborar de forma eficiente para determinar la causa de una alerta. Los ingenieros de subestaciones pueden entender los mensajes de alerta del IDS como si estuvieran estudiando un registro de operaciones, una lista de eventos o una lista de advertencias en su HMI o controlador de estación.



Mensajes de alarma claramente comprensibles atribuidos a eventos en la planta.

De un vistazo, queda claro qué dispositivo ha causado la alarma y en qué bahía.

"Es muy fácil trabajar con StationGuard. Toda la información necesaria se muestra de forma clara y sin jerga informática. Y todo ello con el alto nivel de calidad que esperamos de OMICRON".

Yann Gosteli
Jefe de sistemas de automatización de subestaciones de CKW AG, Suiza

Funcionamiento normal

StationGuard analiza todas las comunicaciones y sabe con precisión qué información puede o no transmitirse en cada momento. ¿Qué dispositivos pueden estar activos ahora? ¿Qué comandos de control están permitidos, y tiene sentido la respuesta a los mismos? ¿Qué valores de medición se transmiten? ¿Es correcta la temporización de los mensajes? Esto permite detectar cualquier problema probable con los equipos o la red con prontitud o incluso antes de que fallen.

Este completo monitoreo funcional y de seguridad es único y ofrece ventajas que van mucho más allá de las que normalmente se esperan de un sistema de detección de intrusión (IDS).

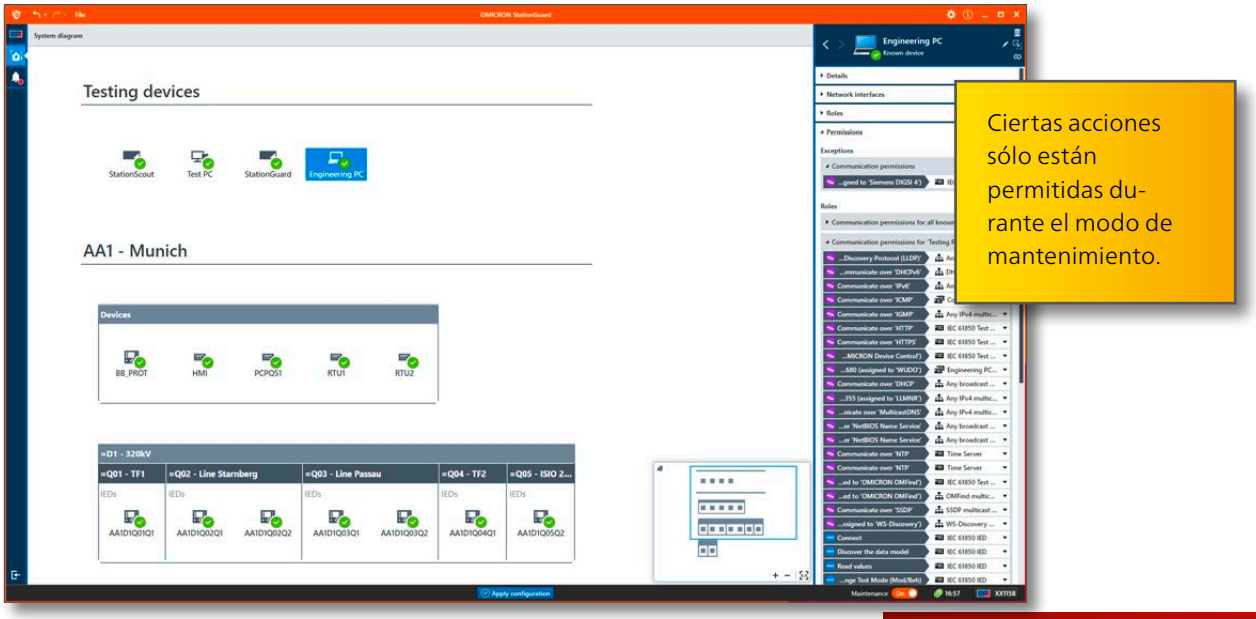
La interfaz gráfica de usuario permite a los ingenieros de protección y control familiarizarse rápidamente con StationGuard, ya que se ajusta a los diagramas de la documentación y a la vista de eventos de los controladores de la estación.

Mantenimiento y puesta en servicio

Las pruebas y el mantenimiento son importantes y no deben dar lugar a falsas alarmas, pero aun así hay que garantizar un alto nivel de seguridad. Para cumplir estos requisitos, StationGuard ofrece un "modo de mantenimiento". La actividad de mantenimiento y pruebas sólo se permitirá cuando este modo se active.

En muchos escenarios de ataque se aprovechan las vulnerabilidades del protocolo del proveedor o de las interfaces web. Por lo tanto, StationGuard puede emitir una alarma si se produce una comunicación con las herramientas del fabricante durante el funcionamiento normal y sólo lo permite mientras se está en modo de mantenimiento. Los PC de ingeniería y los equipos de pruebas pueden registrarse en StationGuard antes de utilizarse, de forma que puedan realizarse las tareas autorizadas sin que se disparen falsas alarmas.

Esto no tiene ningún efecto adverso en la seguridad durante las pruebas: Si un PC de prueba infectado se comunica de forma sospechosa, se activará una alarma.



Ventajas

- Los responsables de seguridad informática y los ingenieros de SCADA y protección entienden las alarmas
- Menos falsas alarmas durante las pruebas de rutina manteniendo un alto nivel de seguridad
- Sin fase de aprendizaje, protección inmediata

Detección de anomalías y errores de configuración

Monitoreo funcional

StationGuard no sólo detecta las ciberamenazas y las acciones prohibidas en las redes de automatización de las compañías eléctricas y de SCADA; también notifica los eventos críticos y las anomalías, tal como las fallas de los dispositivos electrónicos inteligentes (IED), los errores de configuración y los problemas de red, registrándolos para su posterior análisis. Además, todas las transferencias de archivos se registran con sus nombres, por ejemplo, cuando se descargan los registros de perturbaciones.

A continuación, se presentan algunos ejemplos de problemas de funcionamiento que pueden detectarse:

Cambios en la configuración de IED

Si la configuración de un dispositivo cambia, StationGuard emite una alarma.

StationGuard monitorea permanentemente los campos de revisión de la configuración a partir de los mensajes en la red para detectar cambios en la configuración de los dispositivos.

Por ejemplo, detecta el error común de puesta en servicio de que las configRevs son diferentes en los lados del emisor y receptor de la comunicación.

Errores de configuración

Si la configuración de un dispositivo es incorrecta, StationGuard emite una alarma. Detectará los errores inmediatamente.

StationGuard compara continuamente los parámetros de configuración IEC 61850 con las especificaciones de los archivos de entrada o SCL anteriores.

Se detectan los típicos errores de configuración, tal como una configuración VLAN incorrecta, parámetros GOOSE erróneos o datasets incorrectos.

Severity	Date and time	Message
⚠	2020-10-31 11:21:30.907+01:00	Test PC ▸ AA1D1Q01Q1 Unidentified 'UDP' network traffic detected on port number 50000 (assigned to 'Siemens DIGSI 4').
⚠	2020-10-31 10:42:15.255+01:00	AA1D1Q01Q1 ▸ GOOSE multicast address Configuration revision (ConfRev) newer than expected in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:42:15.255+01:00	AA1D1Q01Q1 ▸ GOOSE multicast address Unexpected VLAN identifier in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:42:15.255+01:00	AA1D1Q01Q1 ▸ GOOSE multicast address Wrong destination MAC address in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:40:25.165+01:00	AA1D1Q03Q1 ▸ GOOSE multicast address Unknown GOOSE 'AA1D1Q03Q1Protection/LLN0GOgcb_2' found on network.
⚠	2020-10-31 10:09:52.866+01:00	Test PC ▸ AA1D1Q01Q1 Switching command on 'AA1D1Q01Q1QA1/CSWI1.Pos'.

Registro de eventos con diversas anomalías detectadas

Problemas de red y de sincronización horaria

StationGuard detecta la ralentización de las transmisiones de mensajes GOOSE y las fallas en la sincronización horaria.

StationGuard mide el tiempo de transmisión de los mensajes comparando las marcas horarias del remitente con las marcas horarias de llegada de los paquetes. Se dispara una alarma si esta medición revela un error.

En la mayoría de los casos, los problemas de sincronización horaria provocan estas alarmas. Utilizando el mismo método, StationGuard también detecta si el tiempo de respuesta de un IED se ralentiza debido a una sobrecarga, a un ataque de denegación de servicio o a que la red es excesivamente lenta.

Comandos de control IEC-104 e IEC 61850

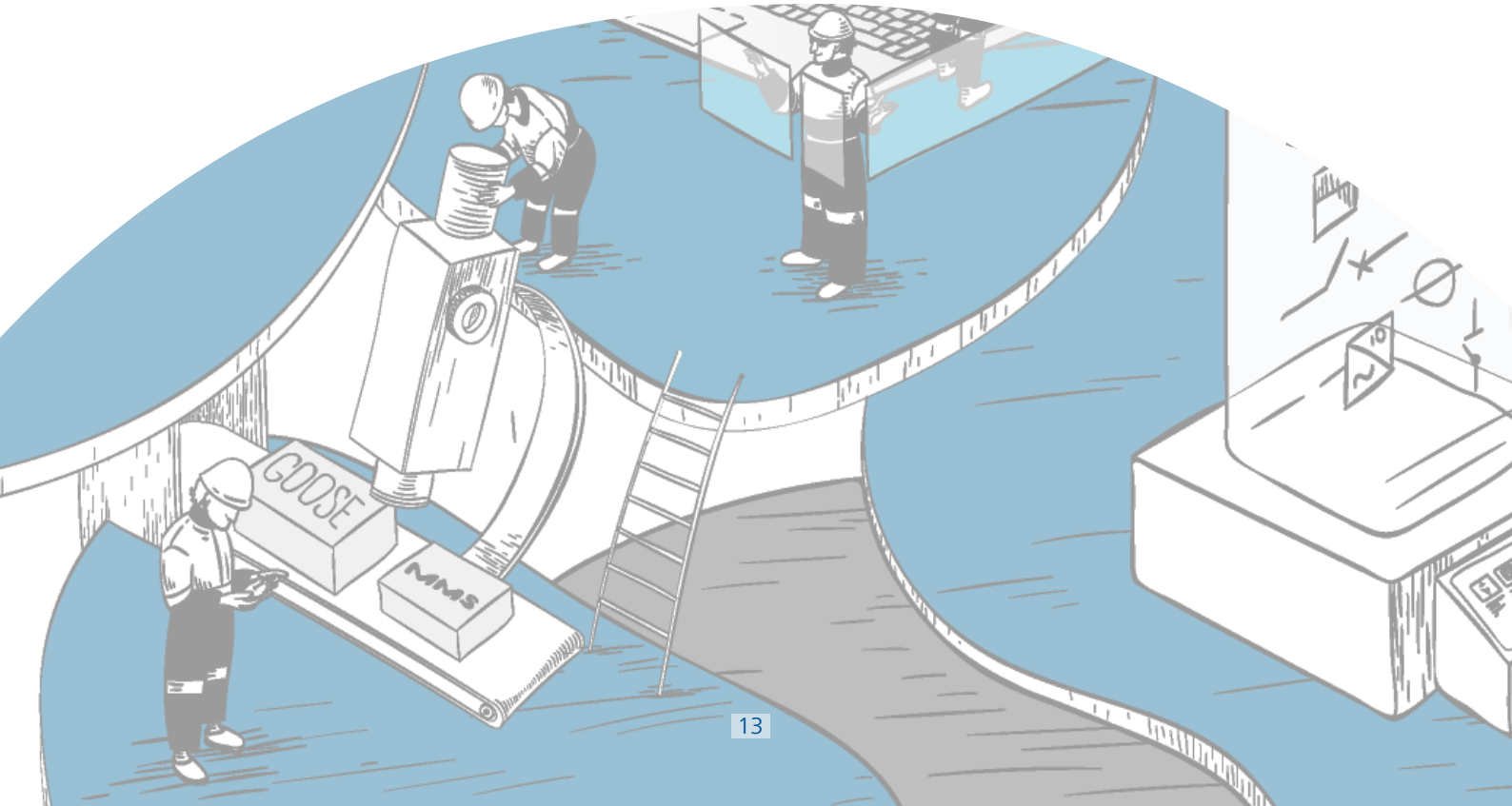
StationGuard detecta y registra los comandos de control fallidos y los problemas de interoperabilidad.

StationGuard registra todos los comandos de control IEC 60870-5-104 y MMS. Si un comando falla, crea avisos y registra los trazos de la red para su posterior análisis. Además, detecta problemas de protocolo e interoperabilidad en MMS, IEC 60870-5-104, DNP3, Modbus, Synchrophasor y muchos más.

Registro de las transferencias de archivos

StationGuard registra las descargas y subidas de archivos, tal como los registros de perturbaciones.

Todas las transferencias de archivos en IEC-104 y MMS se registran junto con los nombres de los archivos y un registro de la red. Podrá ver quién accedió a los archivos en los IED y cuándo se produjo el evento.



Análisis de alertas e investigación de amenazas

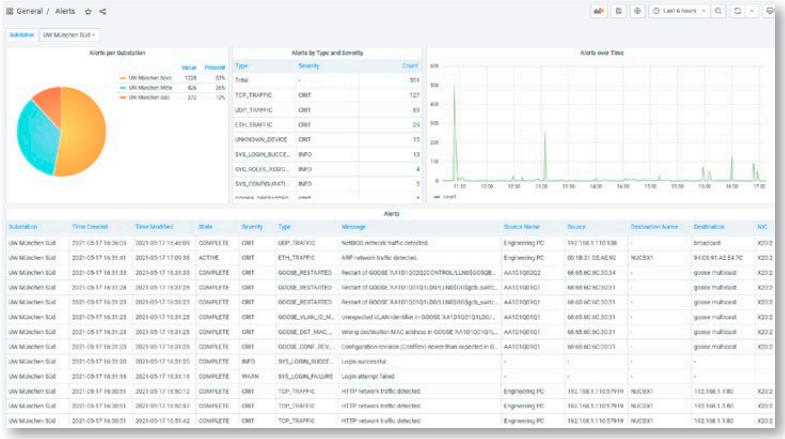
Investigación de alertas (GridOps)

El panel de control de alertas de GridOps se ha diseñado para ofrecer una imagen completa del estado de seguridad de la red eléctrica, al tener acceso a datos relacionados con la seguridad combinados con datos operativos que hacen más visibles las operaciones de la red y los problemas de seguridad.

GridOps permite analizar el registro de eventos combinado de todas las ubicaciones de los sensores y visualiza todos los eventos desde diferentes perspectivas, observando varios indicadores. Permite ver los patrones de alerta y las tendencias para tipos de dispositivos o ubicaciones específicas.

Los registros de alerta pueden ser revisados y analizados, lo cual es esencial para identificar incidentes de seguridad, infracciones de políticas, problemas operativos y más. Sus capacidades de análisis también pueden utilizarse para ayudar en las auditorías y los análisis forenses y para identificar los problemas de funcionamiento actuales y a largo plazo.

La visión en tiempo real de todas las redes de explotación de la red asiste a los distintos equipos de personal; los responsables de seguridad pueden aplicar las políticas de seguridad que protegen las redes sin interrumpir el funcionamiento, y se benefician del monitoreo de las comunicaciones para impulsar la segmentación de la red.
Los ingenieros de protección y control obtendrán visibilidad y conocimientos que garantizan la disponibilidad de las redes de automatización de las compañías eléctricas.



Panel de control con estadísticas de alerta para múltiples sitios

Sistema de gestión centralizada - GridOps (componente de StationGuard)

Plataforma unificada

- Reduzca los falsos positivos y concéntrese en lo esencial
- Visibilidad total permanente en cuanto a incidencias de seguridad, problemas funcionales, etc.
- Acelera y simplifica las respuestas a los incidentes.

Con GridOps puede...

... comprender cómo ha aparecido una amenaza,
qué la ha creado, si ha establecido una conexión, y mucho más.

... colaborar sin fisuras con los equipos de personal de seguridad informática y tecnología operativa para una gestión optimizada de los incidentes y las vulnerabilidades.

... reducir los riesgos operativos al estar preparado para manejar los incidentes de seguridad.

... buscar anomalías en el comportamiento típico de su red eléctrica para detectar todo tipo de amenazas.

... visualizar cada intento de ataque y desviación del comportamiento, por muy sutil que sea.

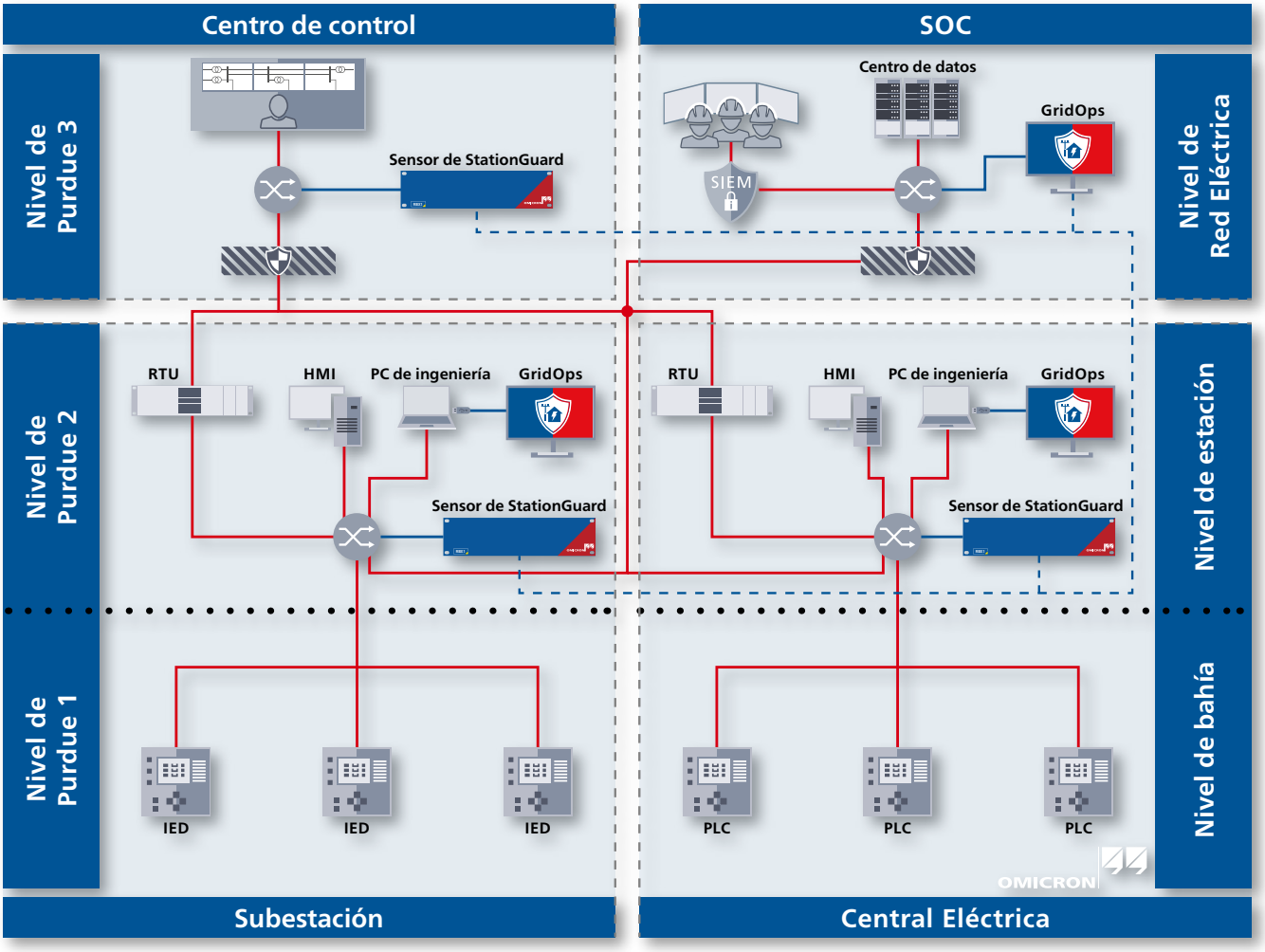


Diagrama de despliegue de StationGuard

¿De qué se compone nuestra solución StationGuard?

Los sensores de StationGuard pueden instalarse en centros de control, centrales eléctricas y subestaciones para implementar la detección de intrusión, la visualización de la red, el descubrimiento de activos y monitorear el correcto funcionamiento de los sistemas de automatización de las empresas eléctricas. El sensor de StationGuard permite un despliegue flexible:

- RBX1 para una instalación permanente
- VBX1 para una plataforma virtual
- MBX1 para un uso móvil y temporal

El componente GridOps es el sistema de gestión centralizada de StationGuard. Proporciona funciones para la gestión de activos, la gestión de vulnerabilidades, el análisis de eventos y alertas, así como la gestión de los sensores. Su principal característica es una plataforma única para visualizar los riesgos de ciberseguridad, las amenazas y monitorear activos y eventos (tanto de ciberseguridad como funcionales) en toda la red eléctrica.

GridOps puede instalarse en un centro de control o en un SOC (Security Operations Center, centro de operaciones de seguridad) para gestionar de forma centralizada todos los sensores IDS de StationGuard desde una única ubicación.

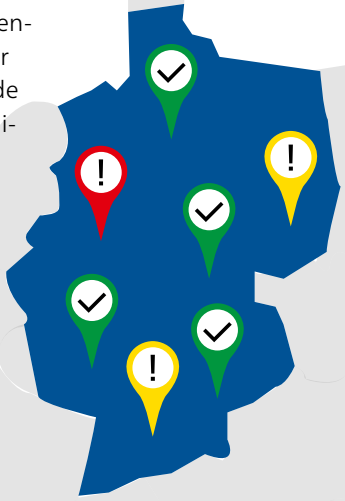
Visibilidad de la red

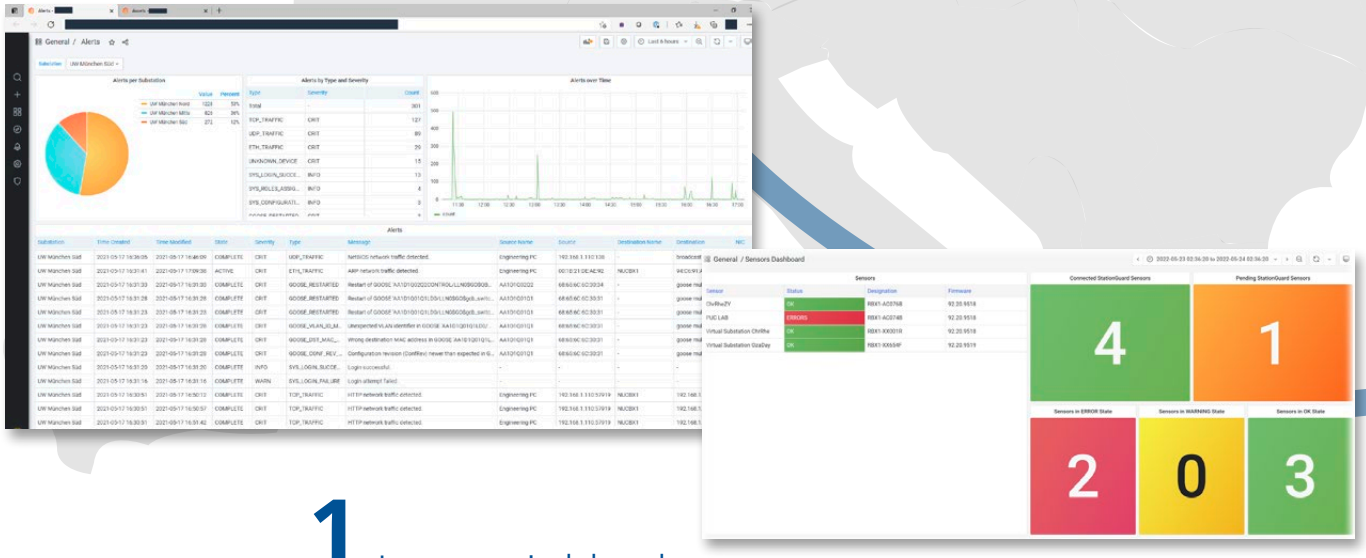
Visibilidad de la red desde la red eléctrica hasta la estación

Hay preguntas apremiantes a las que se enfrentan los responsables de seguridad informática y los ingenieros de redes SCADA y tecnología operativa: ¿Cuál es el estado general de amenaza y riesgo de nuestras redes OT críticas en este momento? ¿Cuál es la estructura de estas zonas de la red y cómo están interconectadas? ¿Cómo se comunican los dispositivos dentro y entre estos límites?

Estas preguntas y otras más exigen una herramienta versátil que permita a los usuarios profundizar con una vista global en la perspectiva de la red de la planta, y aún más en los detalles de las comunicaciones entre activos individuales.

Nuestra solución StationGuard ofrece este alto nivel de transparencia del sistema.





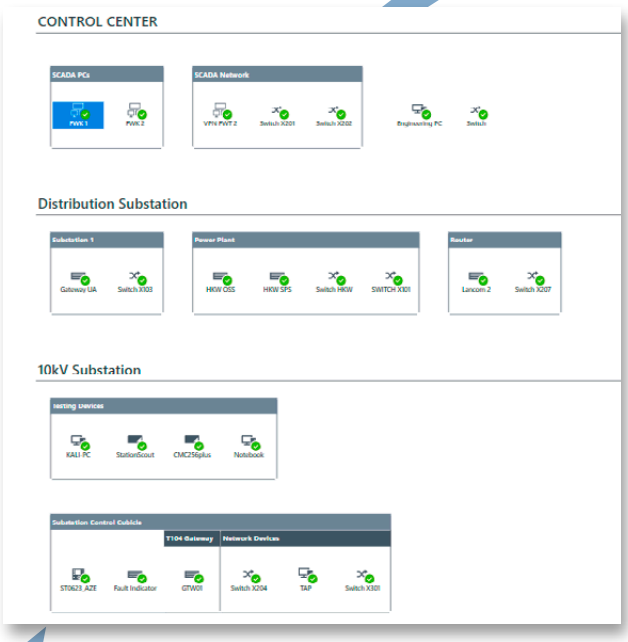
1 Imagen a nivel de red

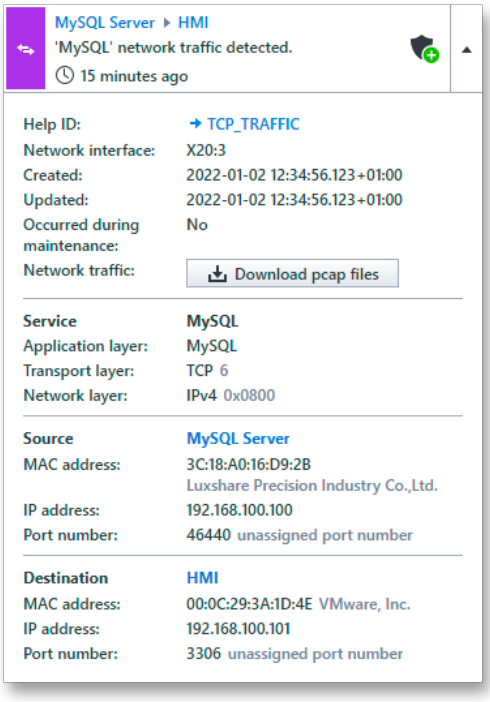
Diferentes paneles de control permiten supervisar el estado de todas las redes de automatización de la red a vista de pájaro. Las amenazas, los problemas de funcionamiento o las vulnerabilidades que requieren una acción inmediata pueden verse de un vistazo.

2 Diagrama de la red de la estación

Sumergirse un nivel más a fondo permite observar las redes utilizando nuestra vista única que combina aspectos del diagrama modelado de Purdue con diagramas unifilares bien conocidos por los ingenieros de protección y SCADA. Esta combinación permite una colaboración óptima entre ambos mundos.

Estos diagramas pueden generarse automáticamente a partir de archivos de ingeniería SCL. También pueden mejorarse manualmente e incluso pueden importarse hojas de cálculo de documentación de la planta para mejorar los nombres de los equipos.





3 Relaciones de comunicación entre dispositivos

Finalmente, la información de las comunicaciones y los protocolos entre dispositivos pasa a primer plano. Allí se pueden observar los detalles de los activos y la información de la placa de características. Los especialistas en informática pueden determinar la bahía y el nivel de tensión de cada activo y pueden deliberar eficazmente con los ingenieros de protección de tecnología operativa mediante una terminología compartida.

Recopilación automática de datos para mejorar la detección de vulner

Una base de datos de inventario de activos con detalles precisos sobre cada IED de protección y control es crucial para el éxito de la gestión de vulnerabilidades y riesgos. Cuanta más información se tenga sobre cada activo, más precisos serán su análisis de vulnerabilidad y su priorización. Nuestra solución StationGuard le atiende durante todo el flujo de trabajo, desde la creación y actualización del inventario de activos hasta la gestión de vulnerabilidades y riesgos.

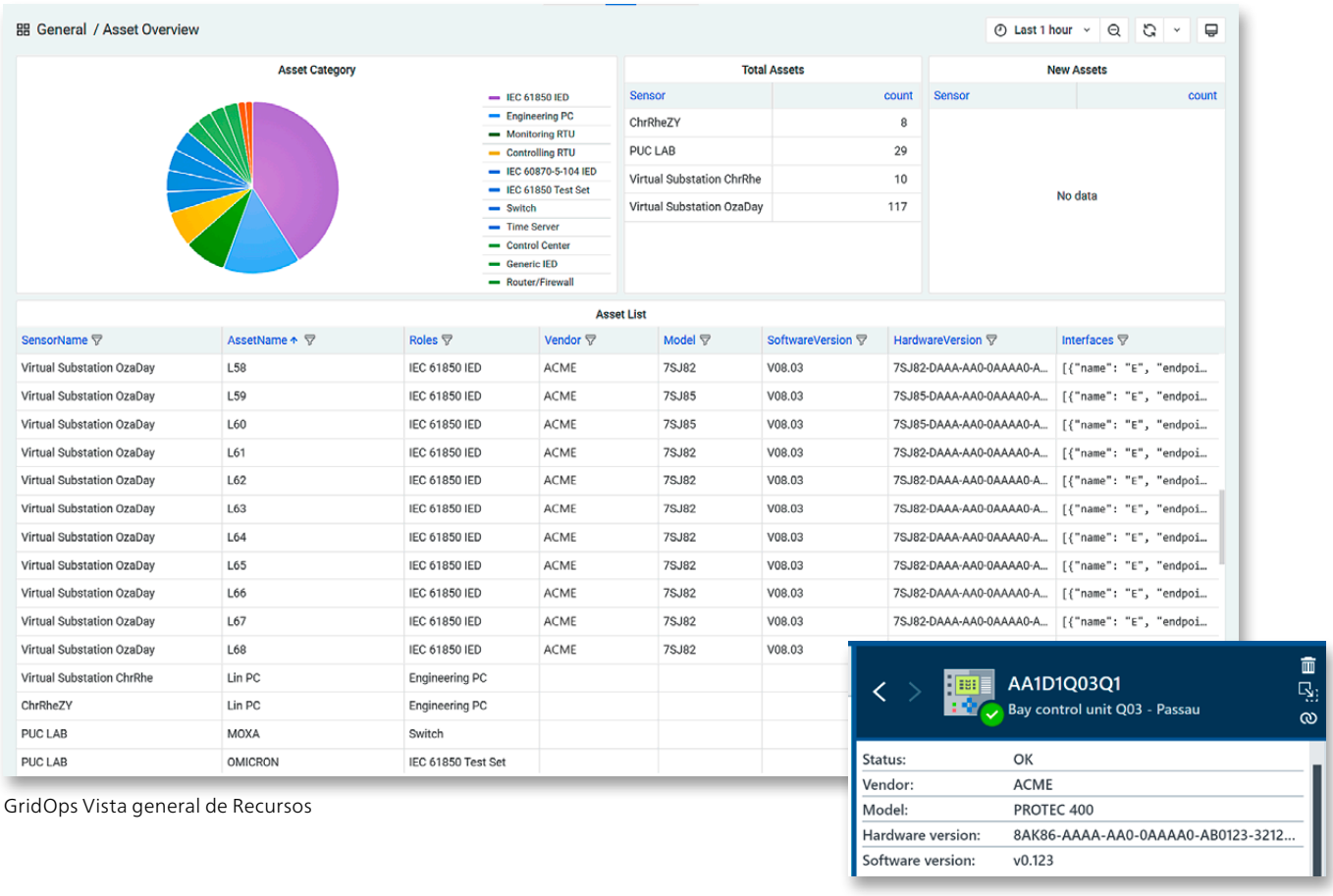
StationGuard descubre automáticamente todos los activos de la red, crea una base de datos de inventario de activos global y le avisa de los nuevos activos en sus redes. Recoge información precisa de cada activo combinando el análisis de la red con archivos de ingeniería SCL importados y hojas de cálculo de documentación de la planta. El inventario de activos puede actualizarse importando información de fuentes externas.

Reciba información detallada sobre sus activos

El uso de esta agregación de información observada pasivamente con archivos de ingeniería y hojas de cálculo importados, proporciona la información más precisa posible sobre los activos. Incluye descripciones de ingeniería, tipo, configuración de hardware, códigos de pedido de productos y versión de firmware.

Puede exportarse el inventario e importarse en sistemas de gestión de activos y de configuración, sistemas ERP y hojas de cálculo. Al importar hojas de cálculo (archivos CSV) a StationGuard, puede cerrarse el bucle y sincronizarlo con cualquier otra fuente. Opcionalmente, puede habilitarse la identificación de activos de StationGuard para leer automáticamente la configuración de los dispositivos y la información de la versión del firmware en la red.

Como resultado, nuestra solución StationGuard compila un inventario de activos con información a fondo de múltiples fuentes que constituye la mejor base posible para la gestión de vulnerabilidades.



GridOps Vista general de Recursos

Gestión de vulnerabilidades

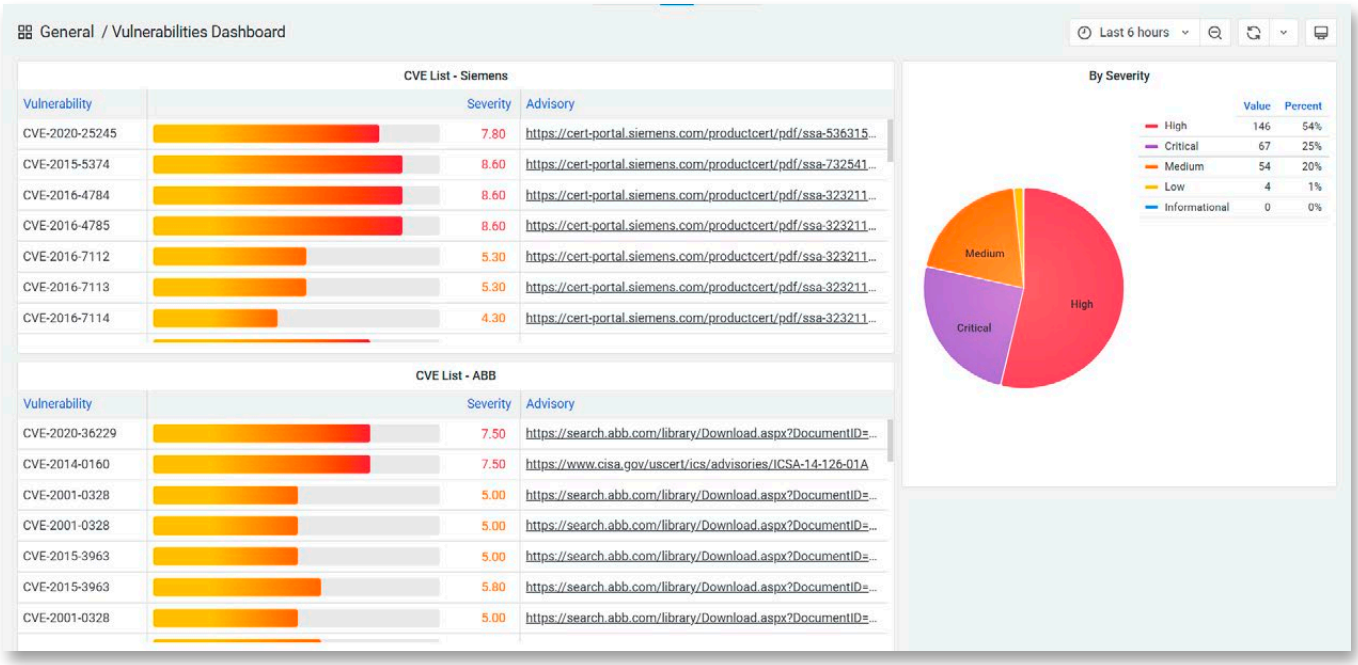
Los reglamentos de seguridad para sistemas críticos, como la directiva NIS de la UE y la NERC-CIP, estipulan que la gestión de la vulnerabilidad es un aspecto vital de cualquier programa de ciberseguridad para la red eléctrica. Puede determinar y aplicar una estrategia de mitigación adecuada asignando las vulnerabilidades conocidas oficialmente a la infraestructura de su sistema.

Sólo se puede proteger lo que se ve.

Nuestro panel de control de vulnerabilidades permite comprender mejor la exposición a las vulnerabilidades de seguridad generales de la red y los puntos críticos. También informa a los usuarios sobre las vulnerabilidades descubiertas recientemente, auditando continuamente estos activos para detectar cualquier amenaza potencial. Cuanta más información tengan los usuarios sobre cada activo, más precisos serán la detección, el análisis y la priorización.

Los usuarios sólo pueden consultar las vulnerabilidades que les resulten relevantes. Sólo se necesitan unos pocos clics, utilizando la base de datos de vulnerabilidades creada por OMICRON para la automatización de la red eléctrica y los dispositivos de red. Identifica rápidamente qué sistemas son vulnerables a un CVE (Common Vulnerability Exposure) concreto.

La elaboración de informes completos y significativos para la dirección, los proveedores y las autoridades reguladoras, para ayudar a priorizar y mitigar los riesgos, es más sencilla que nunca. Las partes interesadas agradecerán la mayor visibilidad y la postura de seguridad y riesgo destacada del sistema.



GridOps Gestión de vulnerabilidades

Integraciones y asociaciones beneficiosas

La solución StationGuard ofrece complementos para sistemas de tickets, como ServiceNow, para crear automáticamente tickets de trabajo que respondan a las alertas de IDS. Al importar el inventario de activos de StationGuard, los tickets se asignan automáticamente al ingeniero responsable del activo o sitio afectado por la alerta.

Control de acceso para la protección de datos y redes

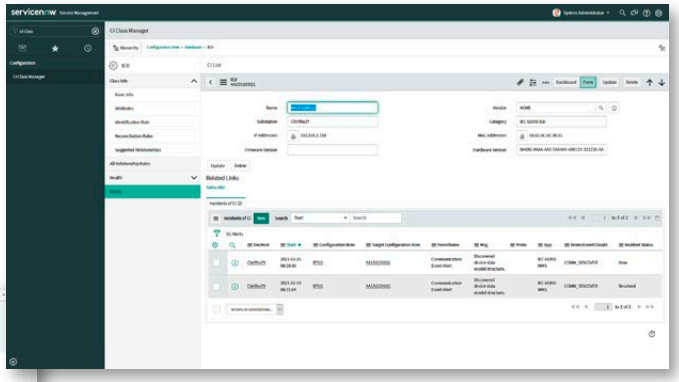
La integración en LDAP/ ActiveDirectory puede configurarse mediante el sistema de gestión centralizada. Dispone de diferentes roles de usuario para controlar el acceso a las distintas funciones de visualización y configuración de sus instancias de StationGuard. Por ejemplo, sólo los usuarios autorizados pueden cambiar la configuración o activar el modo de mantenimiento. Si todas las redes dejan de funcionar, también puede accederse a los sensores StationGuard de forma individual mediante la interfaz de usuario del cliente local de StationGuard.

Las amenazas internas pueden reducirse e incluso eliminarse utilizando RBAC (Role-Based Access Control, control de acceso basado en funciones). Mejora la seguridad del sistema y de las redes. También aumenta la eficiencia al minimizar la necesidad de cambiar las contraseñas y los errores humanos en la asignación de privilegios.

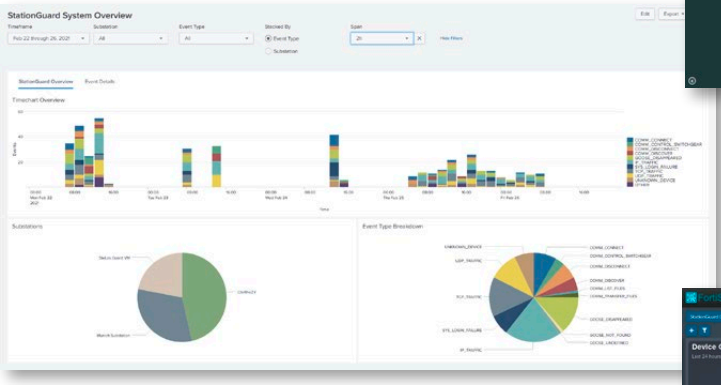
Integración sencilla en su red

Una forma sencilla de integrar los sensores StationGuard en los sistemas heredados es utilizar las salidas binarias de la plataforma RBX1. La presencia de una alarma no reconocida se señala en las salidas binarias, que pueden ser cableadas a una RTU (Remote Terminal Unit, unidad de terminal remota) e integradas en la lista de señales de SCADA.

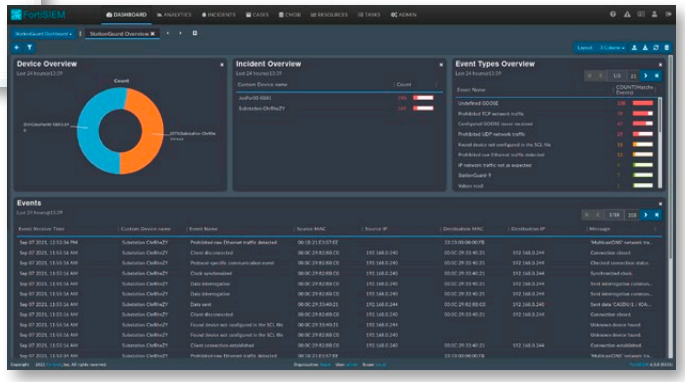
Alternativamente, nuestros mensajes de alerta, de fácil comprensión, también pueden reenviarse mediante el protocolo syslog. Existen varios complementos para integrar los sensores de StationGuard en los sistemas de gestión de la información y los eventos de seguridad (SIEM) y en los sistemas de tickets de diferentes proveedores.



Integración con ServiceNow



App StationGuard para Splunk



Integración con FortiSIEM

Nuestros socios para la seguridad de las redes eléctricas

Socios tecnológicos

Fortinet

El ecosistema Open Fabric de Fortinet ofrece soluciones integradas para una seguridad integral de extremo a extremo.

Integración de la solución StationGuard en FortiSIEM:

Mejora la seguridad, el cumplimiento normativo y la agilidad del negocio.

Splunk

Splunk captura, indexa y correlaciona datos en tiempo real en un repositorio con capacidad de búsqueda, a partir del cual se generan gráficos, informes, alertas, interfaces y visualizaciones.

Explore la aplicación StationGuard para Splunk en Splunkbase:

Informes a la carta con análisis estadísticos.

Contenido y sales partners

NTS

Junto con los fabricantes de gama alta, NTS asume la responsabilidad digital y crea soluciones informáticas con servicios fiables para las áreas de red, seguridad, colaboración, nube y centro de datos.

Combine la solución StationGuard con el servicio de detección de amenazas de NTS:

Ofrezca informes analíticos detallados que asisten en la identificación de riesgos y mejoran la postura de seguridad.

ALSEC

Sus expertos en ciberseguridad le apoyan con servicios competentes e individuales: Empezando por el aprendizaje, el desarrollo de procesos y la evaluación de productos hasta su implementación.

Conocimiento combinado de OMICRON y ALSEC:

Elaboración de informes de riesgo e inteligencia de seguridad empresarial para planificar y preparar el futuro.

Explore más de nuestros socios y comunidades, como EE-ISAC, en nuestra página web:

https://www.omicronenergy.com/en/cybersecurity-partners/

Tres opciones de plataforma diferentes

Los sensores de StationGuard están disponibles en tres plataformas diferentes. Dependiendo de sus necesidades, puede elegir utilizar StationGuard en la plataforma de hardware RBX1 o MBX1 o en una máquina virtual (VBX1). Dado que toda la inteligencia de StationGuard está contenida en el sensor, los sensores funcionan de forma autónoma, por lo que no se requiere una conexión permanente a un servidor central.

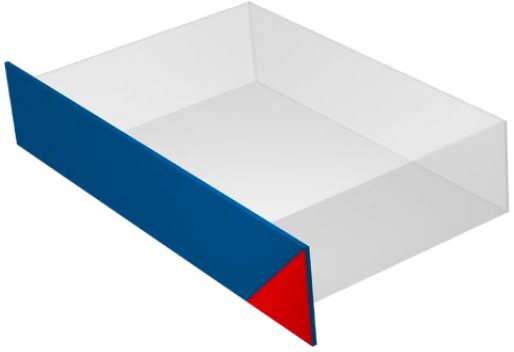
StationGuard en la plataforma RBX1

La ejecución de StationGuard en el hardware RBX1 es una solución IDS a medida para proteger los sistemas de automatización y SCADA de las compañías eléctricas frente a las ciberamenazas y los ataques de día cero. La plataforma RBX1, que puede montarse en un bastidor de 19 pulgadas, está hecha para entornos de red eléctrica difíciles. Tiene suficiente rendimiento y memoria para registrar todos los eventos y el tráfico asociado, aunque el evento haya ocurrido hace mucho tiempo.
La plataforma RBX1 viene con características de seguridad inigualables, como la encriptación completa del disco, un chip criptoprocesador compatible con la norma ISO/IEC 11889 y una seguridad personalizada (UEFI BIOS). También incluye salidas binarias que integran fácilmente las alertas IDS en la lista de señales SCADA.

StationGuard en la plataforma VBX1

Los sensores StationGuard también están disponibles como un dispositivo virtual que puede instalarse en plataformas informáticas existentes.
Al igual que las plataformas de hardware, la variante virtual también puede funcionar de forma completamente independiente, grabando y registrando eventos incluso sin una conexión permanente con el servidor central. Tenga en

cuenta que en las máquinas virtuales puede haber limitaciones técnicas a la hora de monitorear las funciones de las aplicaciones del bus de proceso, en comparación con StationGuard en las plataformas RBX1 y MBX1.



StationGuard en la plataforma MBX1

En la unidad de hardware MBX1 portátil, StationGuard proporciona el mismo nivel de seguridad que la solución montable en bastidor. Con la versión móvil de StationGuard puede realizarse una evaluación rápida de la seguridad de una red de plantas o generar rápidamente una lista de inventario de activos de todos los dispositivos de la red.

Durante las fases de puesta en servicio o mantenimiento, muchos ingenieros y proveedores de servicios externos conectan sus
equipos a la vulnerable red de la planta. StationGuard en MBX1 es perfectamente adecuado para monitorear temporalmente la red durante este período con el fin de alertar de comportamientos prohibidos y registrar acciones críticas durante la puesta en servicio y el mantenimiento.

Especificaciones técnicas de la plataforma RBX1

Condiciones ambientales

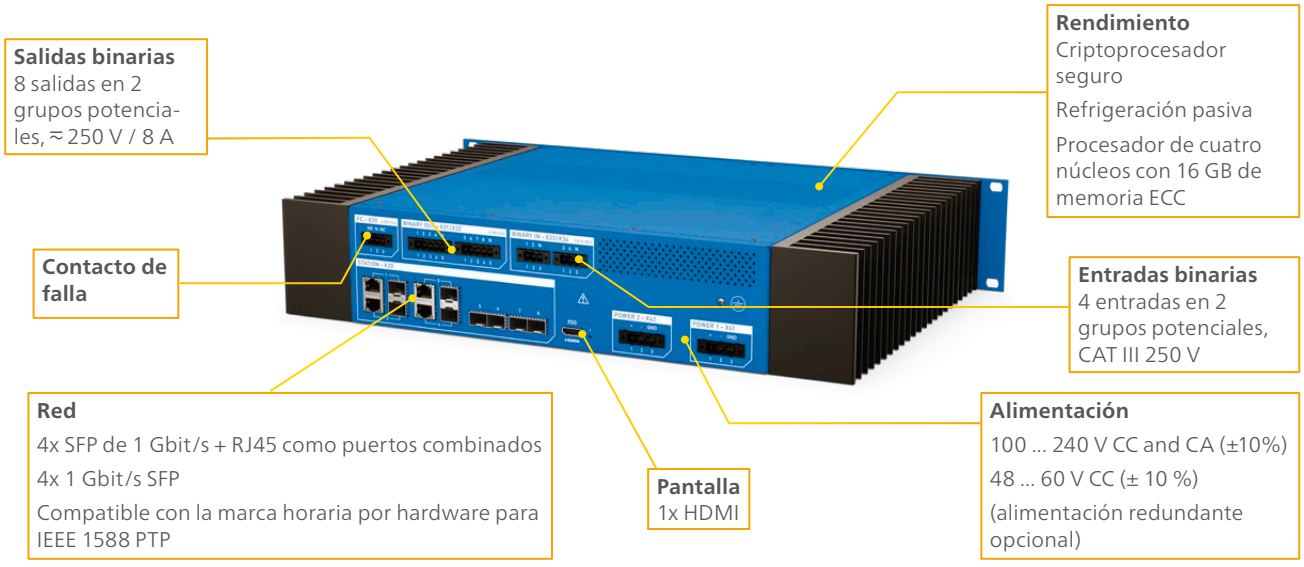
Temperatura de funcionamiento	-20 °C ... +55 °C ...
Temperatura de almacenamiento	-25 °C ... +70 °C ...
Humedad relativa	5 % ... 95 % (sin condensación)
La protección de penetración según la norma IEC 60529	IP30

Normas

Normas de productos	IEC 61850-3 IEEE 1613 Nivel de gseveridad:- Clase 1
Normas EMC	IEC 61326-1 IEC 60255-26 IEC 61000-6-5
Seguridad	EN 60255-27 EN 61010-1 EN 61010-2-030

Ver más detalles en la hoja de datos técnicos.

Vista trasera de la plataforma RBX1



Vista frontal de la plataforma RBX1

Creamos valor para a nuestros clientes con...

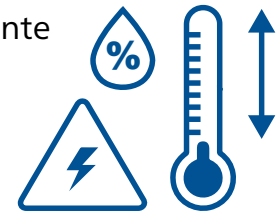
Calidad

Queremos que siempre pueda contar con nuestras soluciones de prueba. Por eso hemos desarrollado nuestros productos con experiencia, pasión y cuidado, estableciendo estos continuamente estándares innovadores en nuestro sector.

Puede contar con los más altos niveles de seguridad y protección

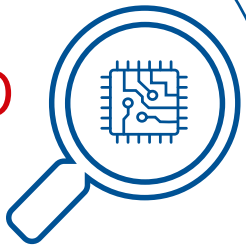
Confiabilidad superior mediante

72



horas de pruebas de rodaje antes de la entrega

100%



de pruebas de rutina de todos los componentes de los equipos de prueba

ISO 9001
TÜV & EMAS
ISO 14001
OHSAS 18001

Conformidad con las normas internacionales

Innovación

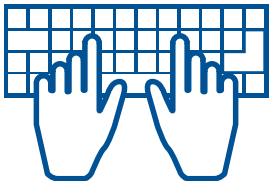
Pensar y actuar de forma innovadora es algo que está profundamente arraigado en nuestros genes. Nuestro amplio concepto del cuidado del producto también garantiza que la inversión rinda beneficios a largo plazo, por ejemplo, con actualizaciones de software gratuitas.

Necesito...

... una cartera de productos previstos para sus necesidades

Más de

200



desarrolladores mantienen actualizadas nuestras soluciones

Más del

15%

de nuestros ingresos anuales se reinvierte en investigación y desarrollo

Ahorre hasta el

70%

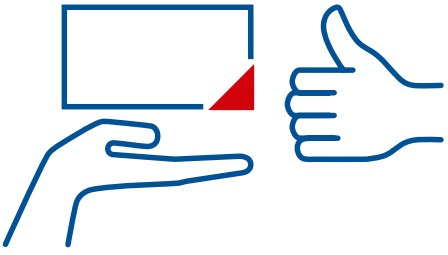
del tiempo de prueba mediante plantillas y automatización

Creamos valor para a nuestros clientes con...

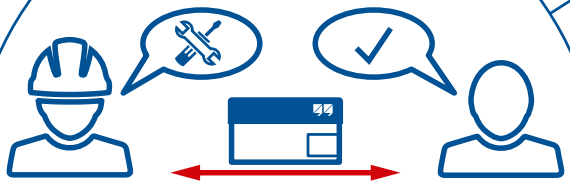
Asistencia

Cuando se requiere una asistencia rápida, siempre estamos a su lado. Nuestros técnicos altamente cualificados están siempre localizables. Además, le ayudamos a minimizar los tiempos fuera de servicio, prestándole equipos de prueba de uno de nuestros centros de servicio.

Asistencia técnica profesional en todo momento



Dispositivos en préstamo ayudan a reducir el tiempo fuera de servicio



Reparación y calibración económicas y sin complicaciones

oficinas en todo el mundo para contacto y asistencia locales

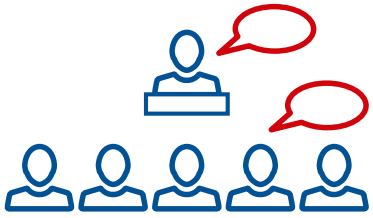
Conocimientos

Mantenemos un diálogo continuo con los usuarios y expertos. Los clientes pueden beneficiarse de nuestra experiencia con acceso gratuito a notas de aplicación y artículos profesionales. Además, la OMICRON Academy ofrece un amplio espectro de cursos de capacitación y seminarios web.

Más de

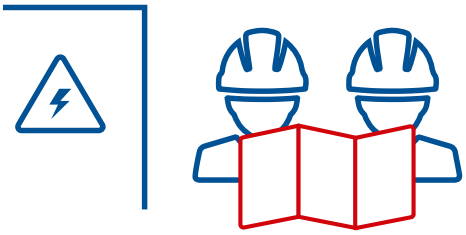
300

cursos prácticos y teóricos al año



OMICRON organiza frecuentes reuniones, seminarios y conferencias de usuarios

a miles de artículos técnicos y notas de aplicación



Expertos en asesoramiento, pruebas y diagnóstico

OMICRON es una empresa internacional que trabaja con pasión en ideas para que los sistemas eléctricos sean seguros y confiables. Nuestras soluciones pioneras están diseñadas para responder a los retos actuales y futuros de nuestro sector. Nos esforzamos constantemente para empoderar a nuestros clientes: reaccionamos ante sus necesidades, facilitamos una extraordinaria asistencia local y compartimos nuestros conocimientos expertos.

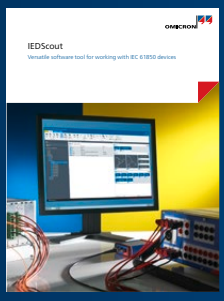
Dentro del grupo OMICRON, investigamos y desarrollamos tecnologías innovadoras para todos los campos de los sistemas eléctricos. Cuando se trata de las pruebas eléctricas de los equipos de media y alta tensión, pruebas de protección, soluciones de pruebas para subestaciones digitales y soluciones de ciberseguridad, clientes de todo el mundo confían en la precisión, velocidad y calidad de nuestras soluciones de fácil uso.

Fundada en 1984, OMICRON cuenta con décadas de amplia experiencia en el terreno de la ingeniería de la potencia eléctrica. Un equipo especializado de más de 900 empleados proporciona soluciones con asistencia permanente en 25 emplazamientos de todo el mundo y atiende a clientes de más de 160 países.

Las siguientes publicaciones ofrecen información adicional sobre las soluciones que se describen en este folleto:

Folleto de IEC 61850

Folleto de StationScout



Folleto de StationScout

Para obtener más información, documentación adicional e información de contacto detallada de nuestras oficinas en todo el mundo, visite nuestro sitio web.

www.omicronenergy.com

L4297