NOZOMI NETWORKS

RESUMEN SECTORIAL

Minería: Protección de la resiliencia operativa a través de la visibilidad y seguridad de TO e IoT

Tabla de contenido

1. Introducción 1

2. Principales desafíos del sector de la minería 2

2.1 En defensa de un espacio cada vez más amenazado 2

2.2 Reducción de tiempos de inactividad no planificados y de las pérdidas resultantes 3

2.3 Protección de la propiedad intelectual y de los recursos del negocio contra el espionaje industrial y los activistas 4

3. La solución de Nozomi Networks 5

3.1 Cómo la solución de Nozomi Networks mejora la resiliencia operativa 5

3.2 Diagrama: Seguridad y visibilidad de TO e IoT 6

3.3 Arquitectura de implementación: Ejemplo de modelo Purdue 7

4. Mejora de la visibilidad operativa y de red 8

4.1 Caso de uso: Monitorización eficaz de la red SCADA 8

4.2 Caso de uso: Identificación proactiva del desgaste de los equipos 10

5. Detección de ciberriesgos y mejora de la resiliencia cibernética 12

5.1 Caso de uso: Segmentación de la red de TO para lograr resiliencia cibernética 12

5.2 Caso de uso: Defensa de la mina contra el robo malicioso de datos 14

6. Conclusión 16

7. Opiniones del cliente 17

Qué buscamos en una solución de seguridad y visibilidad de TO e IoT 18

Vea en acción la solución de Nozomi Networks 18

¿Desea obtenermás información? 18

8. Referencias 19

1. Introducción

Proteger la resiliencia operativa de los operadores de minas a través de la visibilidad y seguridad de TO e IoT

Las empresas de minería están trabajando diligentemente para mantener la competitividad y rentabilidad en un entorno empresarial complicado. La baja en los precios de las materias primas y los limitados recursos naturales no explotados obligan a estas empresas a mejorar la eficiencia operativa.

A medida que los operadores de minas comienzan a integrar sistemas en toda la empresa para obtener eficiencias, también aumentan los riesgos de ciberseguridad. Para hacerles frente, las minas deben implementar soluciones de ciberseguridad y visibilidad en tiempo real diseñadas para reducir el riesgo y lograr la resiliencia operativa.

En su camino hacia la eficiencia operativa, las empresas de minería han adoptado la digitalización, la automatización e Internet de las cosas industrial (IIoT). Sin embargo, la integración de sistemas operativos con sistemas empresariales más amplios resalta desafíos para la visibilidad de la tecnología operativa (TO) y ha aumentado la exposición a ciberamenazas. La protección de beneficios, personal y propiedad intelectual (IP), pese a sistemas preexistentes poco seguros, requiere un delicado equilibrio.

Afortunadamente, la industria de la minería ha eludido los ciberataques a gran escala que se han experimentado en el sector de las infraestructuras críticas. Aún así, un estudio de Ernst & Young de 2019 informó que el 54 % de las empresas de minería y metalurgia han sufrido algún incidente de ciberseguridad significativo en el último año.[1]

Los operadores de minas deben asegurarse de poder detectar y contener los incidentes y ciberamenazas, independientemente de la causa, antes de que interrumpan la producción, comprometan la seguridad del personal y los equipos, o provoquen la pérdida de propiedad intelectual. Esto incluye combatir errores internos o ataques deliberados de gobiernos extranjeros, hackers, otros proveedores o activistas.

Aunque los líderes del sector minero han sido, con frecuencia, los últimos en adoptar las mejores prácticas en materia de ciberseguridad, están empezando a reconocer la gravedad de las ciberamenazas potenciales y trabajando para generar resiliencia. En 2017, un grupo canadiense de empresas de minería formaron el Centro de Análisis de Información Compartida sobre Minería y Metalurgia para proteger a los miembros contra incidentes cibernéticos.[2] Otros países están aplicando reglamentos en materia de protección de los datos, e investigadores de ciberseguridad a nivel global también están colaborando con la industria e instituciones para proteger los sistemas industriales contra el riesgo cibernético.

EL CAMINO HACIA LA RESILIENCIA OPERATIVA

Lea este documento para descubrir cómo se puede utilizar la solución unificada de detección de amenazas y monitorización de TO e IoT para **lograr disponibilidad, visibilidad y seguridad operativas.**

Para adelantarse a los inminentes reglamentos y prosperar durante la volatilidad del mercado, los operadores de minería necesitan dar pasos proactivos para proteger sus operaciones. Afortunadamente, es posible utilizar tecnologías como la solución de ciberseguridad y visibilidad en tiempo real de Nozomi Networks para generar resiliencia operativa de forma rápida y fácil.

2. Principales desafíos del sector de la minería

A medida que los operadores de minas adoptan prácticas inteligentes de minería, se enfrentan a desafíos que, si no se abordan convenientemente, podrían exponerlos a importantes riesgos empresariales.

2.1 En defensa de un espacio cada vez más amenazado

Para mejorar la rentabilidad y reducir los costes, las empresas de minería están incorporando nuevas aplicaciones de IIoT en su entorno operativo. Estas aplicaciones emplean procesadores y sensores para recopilar y compartir datos de forma inalámbrica. No obstante, también crean interconectividad entre sistemas anteriores de TO e IoT y el sistema de TI corporativo, un cambio que aumenta la vulnerabilidad de la mina ante los ciberataques a través de toda la red.

Los sistemas heredados de TO e IoT no se diseñaron originalmente para conectarse en red. Con frecuencia, carecen de estándares de seguridad básicos como, por ejemplo, firewalls, restricciones de usuarios o mecanismos de autenticación. Estas deficiencias en seguridad exponen a las empresas de minería a riesgos cibernéticos en toda la organización, de origen tanto externo como interno, incluyendo atacantes con motivaciones económicas o políticas.

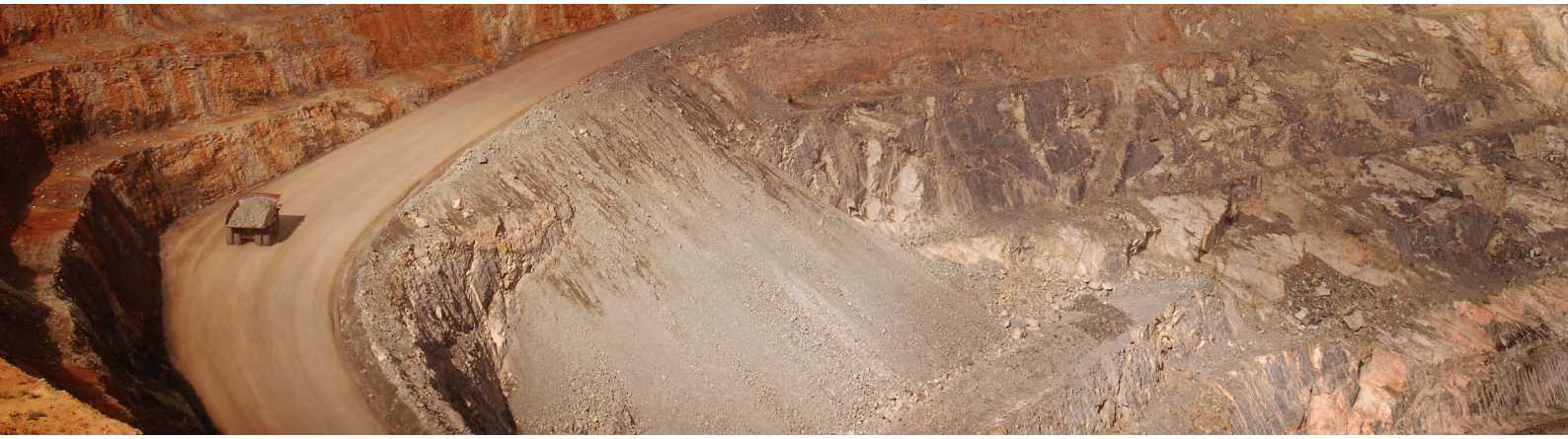
En la filtración de datos de 2016 de una empresa de minería canadiense, los hackers fueron capaces de acceder a la red interna de la organización durante meses sin ser detectados, obteniendo acceso a 15 GB de datos personales y de clientes.[3] Aunque es uno de los productores de extracción de oro más importantes del mundo, la organización no disponía de ningún sistema para monitorizar satisfactoriamente las posibles brechas de seguridad.

Sin embargo, no todas las ciberamenazas son intencionadas. Una red puede verse expuesta a amenazas por diversas causas: desde contraseñas débiles a dispositivos personales infectados con malware y errores de configuración accidentales. Incluso empleados que no quieren provocar daños pueden representar un peligro.

SER PROACTIVO ES UNA DE LAS MEJORES PRÁCTICAS RECOMENDADAS

La digitalización de recursos preexistentes de TO e IoT está generando interconectividad entre los sistemas de TI y TO de una mina, lo que aumenta su vulnerabilidad ante los ciberataques. Los operadores de minas deben dar pasos para mitigar esta exposición a través de la implementación de **procesos de seguridad diseñados específicamente para proteger el entorno de TO e IoT.**

La defensa de este espacio cada vez más amenazado requiere avanzadas soluciones de seguridad capaces de proporcionar visibilidad operativa y detección de amenazas, y soluciones específicamente adaptadas para defender el entorno de TO e IoT.



2.2 Reducción de tiempos de inactividad no planificados y de las pérdidas resultantes

Con precios de las materias primas en constante cambio y los depósitos naturales en descenso, las operaciones en las minas se esfuerzan por alcanzar la rentabilidad a través de eficiencias operativas. Un obstáculo común, aunque costoso, para la productividad es el tiempo de inactividad no planificado y las pérdidas resultantes.

Caterpillar, la empresa de maquinaria y equipos de construcción, estima que "el coste total de los tiempos de inactividad no planificados en minería puede llegar a ser 15 veces el coste de un evento planificado". [4]

Incluso las operaciones que se llevan a cabo con éxito pueden desviarse por averías y fallos en los equipos. Además, puesto que procesos de producción se basan en la automatización, una avería en un único dispositivo puede tener repercusiones en todo el sistema.

Los tiempos de inactividad no planificados se producen por una variedad de motivos, desde desgaste no detectado de equipos hasta sofisticados ciberataques. La monitorización en tiempo real del estado de todos los equipos de una mina es una tarea compleja. Normalmente, los operadores realizan evaluaciones mensuales de las operaciones del sistema de producción. Sin embargo, este ritmo no permite al personal detectar problemas a medida que se desarrollan ni reaccionar a cambios invisibles en el comportamiento.

Estos procesos de revisión de equipos tampoco abordan adecuadamente la creciente amenaza de malware diseñado para hacer que los sistemas de TO se detengan. Aunque la mayoría de ciberataques de mayor escala se han dirigido a sistemas de TI, las operaciones mineras son un objetivo en crecimiento.

De hecho, en marzo de 2019, uno de los productores de aluminio más importantes del mundo experimentó un ciberataque devastador. El ataque paralizó las redes de ordenadores de la empresa, lo que forzó el aislamiento de algunas plantas y el cambio de operaciones de minería al modo manual. En conjunto, se informó que el ataque tuvo un coste para la empresa de 70 millones de dólares.[5]

EL COSTE DEL TIEMPO DE INACTIVIDAD NO PLANIFICADO

Anticiparse al desgaste de los equipos y evitar el tiempo de inactividad no planificado son factores críticos.

Una estimación sitúa el coste total del tiempo de inactividad no programado en minería en 15 veces el coste de un evento programado.[4]

EL ALTO COSTE DE UN INCIDENTE CIBERNÉTICO

EMPRESA

Norsk Hydro

INCIDENTE CIBERNÉTICO

Ransomware: LockerGoga

IMPACTO

Se vio forzada a cambiar a operaciones manuales y soluciones alternativas

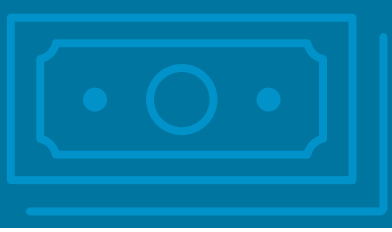
La salida de producto de una unidad de negocio se redujo en un 50%

Se retrasaron los sistemas de información, cobro, facturación y otros

Se perdieron márgenes y se redujeron los volúmenes de producción

COSTE

70 millones de $



2.3 Protección de la propiedad intelectual y de los recursos del negocio contra el espionaje industrial y los activistas

Las empresas de minería son un tesoro para recabar información: investigación sobre exploración geológica que contiene datos sobre la ubicación y el valor de depósitos naturales, o información sobre precios y tecnología propietaria de extracción y procesamiento, por nombrar solo algunos ejemplos.

Es conocido que ciertos grupos de interés corporativos y estados nación se han implicado en actividades de ciberespionaje para acceder a este tipo de datos y lograr ventajas competitivas a largo plazo. Por ejemplo, información sobre el valor y precios de la mina podría utilizarse en negociaciones sobre fusiones y adquisiciones para bajar el precio del objetivo de adquisición u ofrecer más que la competencia en un contrato de venta.

Los recursos de propiedad intelectual son otro atractivo objetivo de la ciberdelincuencia. El acceso a métodos de producción y procesamiento propietarios y al diseño de equipos de minería puede utilizarse para recortar costes de I+D y obtener acceso a lucrativos segmentos de mercado.

En 2015, por ejemplo, un fabricante australiano de tecnología minera reveló un golpe cibernético de hackers chinos: robaron el diseño de su detector de metales e inundaron el mercado con dispositivos falsificados baratos. La empresa tuvo que reducir el precio de su detector casi a la mitad para competir y perdió casi el 80 % de sus beneficios en un año.[6]

Por otra parte, debido a la naturaleza de sus operaciones, se ha investigado a las empresas de minería por su impacto en el medio ambiente. Hacktivistas con interés en exponer supuestos daños medioambientales en hábitats naturales y que buscan llamar la atención pública sobre sus causas, también representan una amenaza añadida de ciberseguridad.

DATOS CORPORATIVOS OBJETIVO DE CIBERAMENAZAS

Grupos de interés corporativos y estados nación tienen a las empresas de minería entre sus objetivos para obtener acceso a datos corporativos sensibles.

Dicha información puede utilizarse en negociaciones de fusiones y adquisiciones, I+D y otras situaciones empresariales para ganar ventajas competitivas o interrumpir las operaciones.

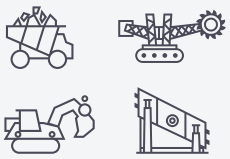
3. La solución de Nozomi Networks

3.1 Cómo la solución de Nozomi Networks mejora la resiliencia operativa

Nozomi Networks ayuda a las empresas de minería a acelerar el ritmo de la transformación digital. Nuestra solución unifica visibilidad y detección de amenazas a través de sistemas de TO, IoT, TI y ciberfísicos.

Hacemos posible que las organizaciones enfrenten la escalada de riesgos cibernéticos en redes operativas y puedan modernizar sus negocios para tener éxito en el futuro.

LIDERAZGO EN LA INDUSTRIA DE LA MINERÍA



Implementado en
5 de las 10 más importantes empresas de minería globales

Nozomi Networks ofrece visibilidad de red, detección de amenazas e información operativa a miles de grandes centros industriales de todo el mundo. A través del uso innovador de la inteligencia artificial, nuestra solución automatiza el duro trabajo de inventariado, visualización y monitorización de redes de TO e IoT.

Los operadores de minas se benefician de la visibilidad y la detección de amenazas en tiempo real necesarias para garantizar una alta resiliencia y fiabilidad cibernéticas.

A continuación se incluye una breve descripción de nuestra línea de productos. Para ampliar la información, visite **nuestro sitio web**.

SAAS

Vantage

Vantage acelera la respuesta en materia de seguridad con visibilidad y detección de amenazas incomparables a través de las redes de TO, IoT y TI. Su plataforma SaaS escalable permite proteger cualquier número de recursos, en cualquier lugar. Podrá responder con mayor rapidez y eficacia a las ciberamenazas, garantizando la resiliencia operativa.

Requiere sensores Guardian.

PERÍMETRO O NUBE PÚBLICA

Guardian

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

PERÍMETRO O NUBE PÚBLICA

Central Management Console

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

SUSCRIPCIÓN

Threat Intelligence

El servicio Threat Intelligence ofrece inteligencia continua de amenazas y vulnerabilidades de TO e IoT. Le ayuda a mantenerse al día de las amenazas emergentes y las nuevas vulnerabilidades, y a reducir el tiempo promedio de detección (MTTD).

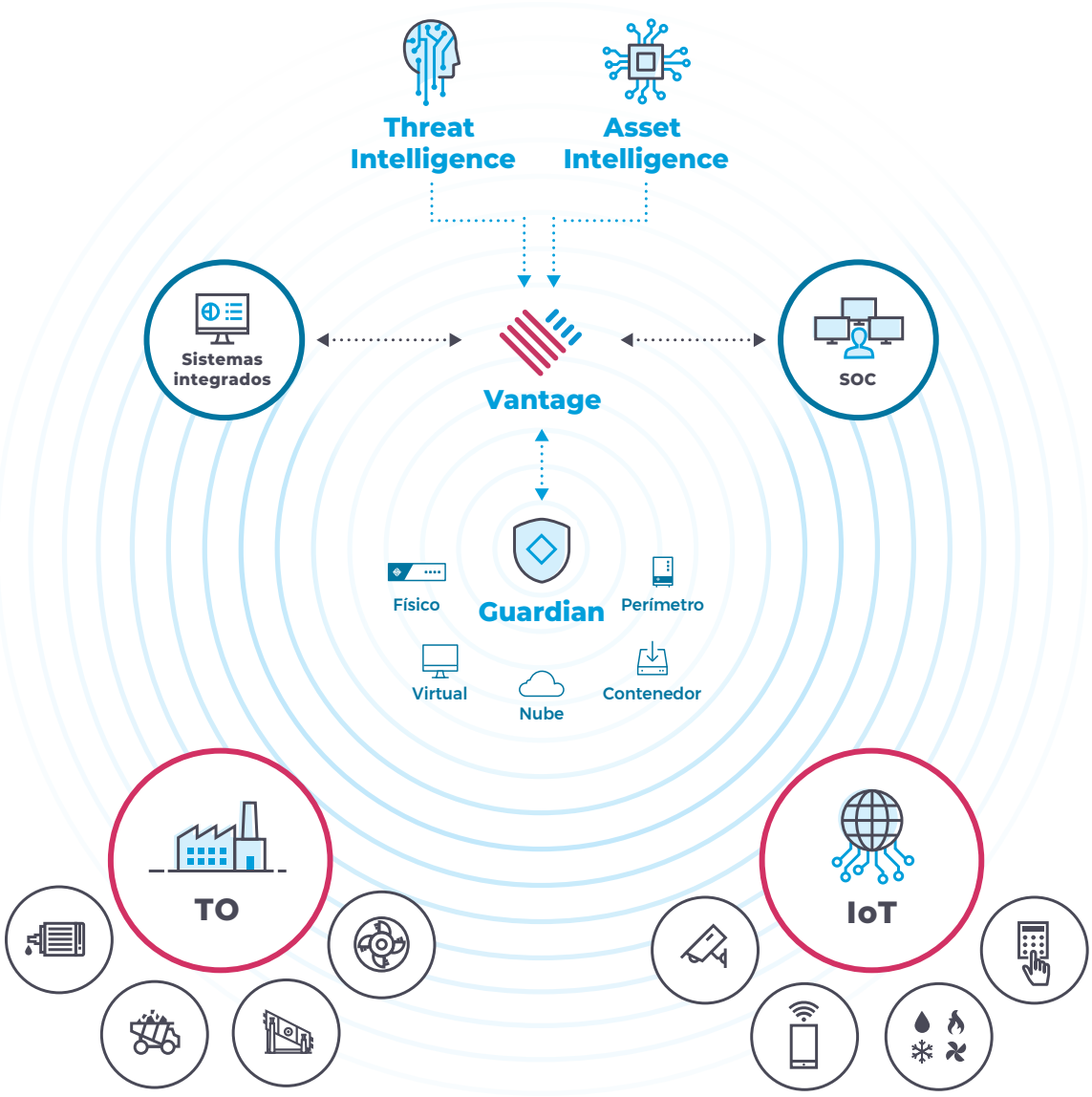
SUSCRIPCIÓN

Asset Intelligence

El servicio Asset Intelligence ofrece actualizaciones periódicas de perfiles para lograr una detección más rápida y precisa de las anomalías. Ayuda a focalizar los esfuerzos y a reducir el tiempo promedio de respuesta (MTTR).

3.2 Diagrama: Seguridad y visibilidad de TO e IoT

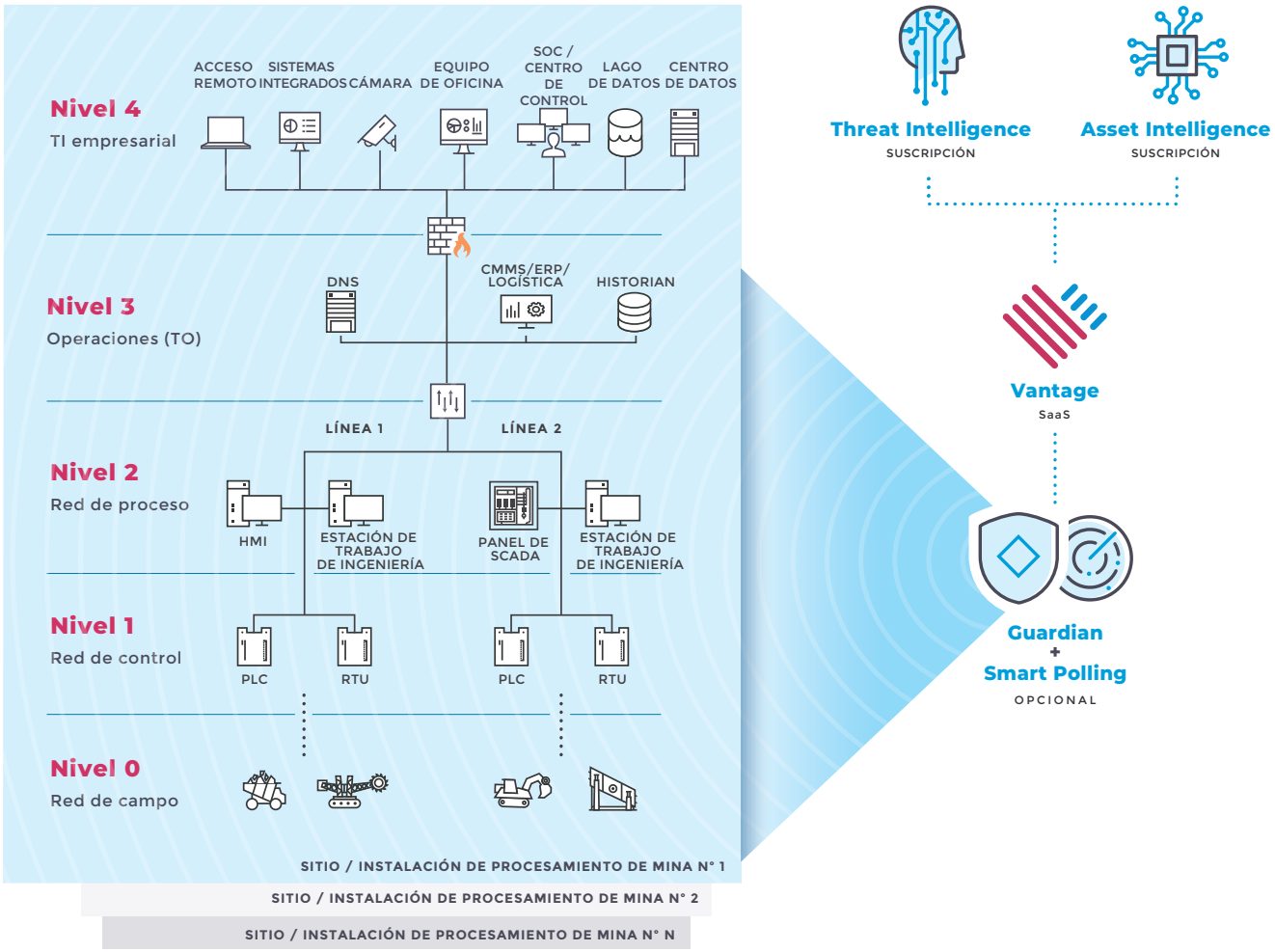
Es posible proteger una amplia variedad de entornos mixtos con una rápida detección de recursos, visualización de red en tiempo real e inteligencia actualizada sobre amenazas.



3.3 Arquitectura de implementación: Ejemplo de modelo Purdue

Puede adaptar la solución de Nozomi Networks para satisfacer sus necesidades aprovechando su arquitectura flexible y las integraciones con otros sistemas.

Adicionalmente, es posible agregar **Remote Collectors**™ a los sensores Guardian para capturar datos de ubicaciones remotas y fuera de la instalación.



4. Mejora de la visibilidad operativa y de red

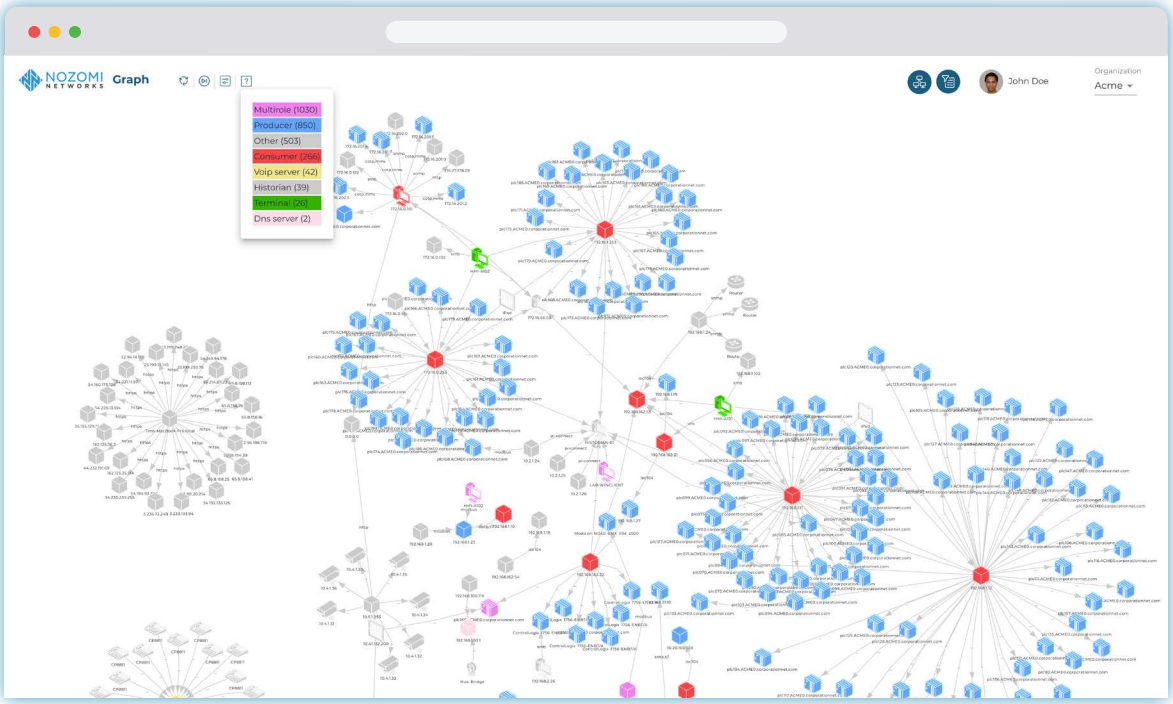
4.1 Caso de uso: Monitorización eficaz de la red SCADA

La naturaleza compleja de la industria minera implica que un pequeño cambio en el proceso puede tener un efecto significativo en equipos, seguridad y rentabilidad. Por lo tanto, mantenerse al tanto de lo que está pasando en la red de control industrial y responder rápidamente a los cambios, resulta crítico para la misión.

Sin embargo, los operadores de minas no pueden monitorizar ni gestionar un panorama tecnológico que no sea visible o no esté documentado. Para detectar y solucionar problemas de conexión de red y comunicación que amenacen la fiabilidad, los operadores industriales necesitan visibilidad en tiempo real de sus recursos, conexiones, comunicaciones, protocolos y mucho más.

Muchos desafíos habituales de la visibilidad operativa pueden resolverse a través de la visualización y monitorización de red en tiempo real para generar información útil, por ejemplo:

- Una vista macro de toda la red de control industrial, incluyendo zonas, topología, nodos, enlaces, sesiones y tráfico
- Diferentes subredes y segmentos de red
- El rol de cada nodo y el tráfico entre nodos
- Los protocolos utilizados para las comunicaciones entre nodos y zonas
- Información sobre el tráfico de red, como rendimiento, protocolos y conexiones TCP abiertas
- Los atributos detallados de los dispositivos terminales y de las conexiones



Solución de Nozomi Networks: Vista gráfica de red
Esta visualización muestra todos los recursos de la red para obtener información en tiempo real.

EL DESAFÍO:

- Mantenerse al tanto de la monitorización de la red SCADA

LA SOLUCIÓN

Utilizar la visualización de red en tiempo real para mejorar el conocimiento del proceso de minería

- La solución de Nozomi Networks proporciona visibilidad integral de la red industrial de un operador y de los recursos de TO e IoT.
- Los fabricantes pueden monitorizar eficientemente redes industriales y resolver fácilmente los problemas antes de que impacten en las operaciones.

RESULTADOS

Conocimiento de la situación de toda la red

Mayor rapidez en la resolución de problemas y cambios en el sistema

Mejorar la información sobre vulnerabilidades y riesgos

Mayor fiabilidad operativa

4.2 Caso de uso: Identificación proactiva del desgaste de los equipos

El tiempo de inactividad no planificado se produce por varios motivos: la rotura de un componente por funcionamiento en condiciones adversas, un cambio en la conexión de red que impacta en procesos automatizados o un incidente cibernético que causa la paralización del negocio.

Aquí se incluye un ejemplo de cómo puede impactar el fallo de los equipos en las operaciones: El cubo de cada neumático de 60.000 $ en un camión minero de 5 millones de $ contiene un pequeño motor orbital. El funcionamiento sometido a 4.000 psi de presión constante puede provocar que el líquido del motor se sobrecaliente, lo que dañaría el sistema hidráulico y reduciría la vida útil del componente.

En la industria minera intensiva en recursos, el mantenimiento y las reparaciones de los equipos pueden reducir ampliamente la productividad y los márgenes. De acuerdo con Gartner, el coste del tiempo de inactividad de producción se sitúa entre 300.000 $ y 500.000 $ la hora.[7]

Imagine los beneficios de la identificación proactiva de anomalías en la temperatura y la presión (o de otros problemas de mantenimiento preventivo) antes de que se detengan las operaciones y la cuenta de resultados resulte perjudicada.

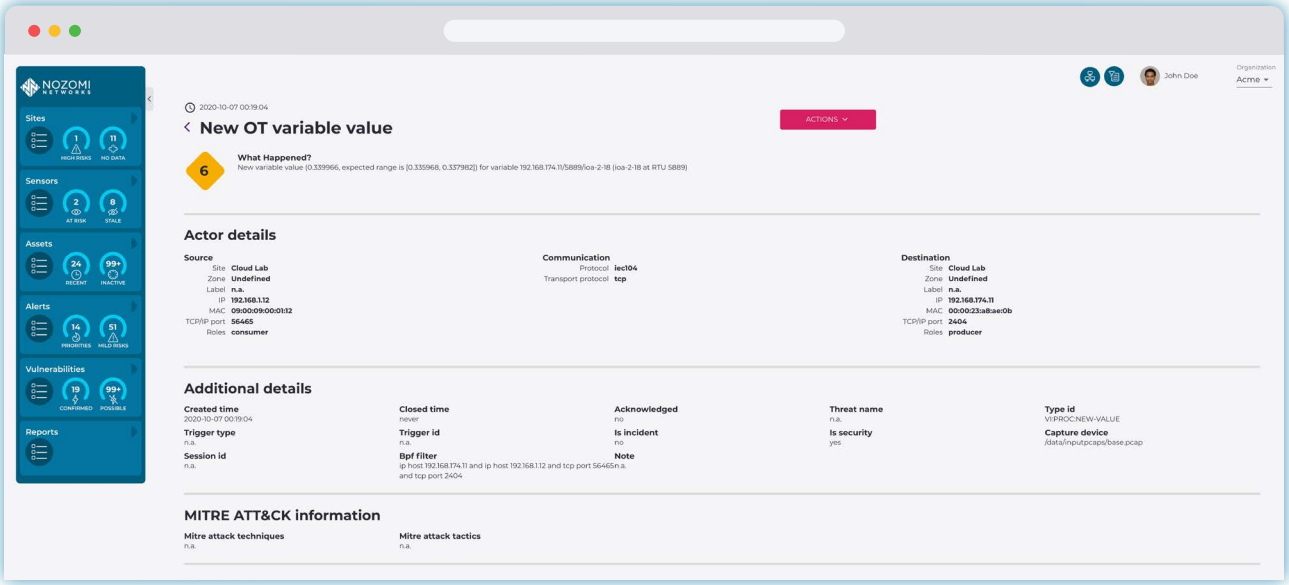
La solución de Nozomi Networks solventa directamente el mantenimiento preventivo mediante la monitorización de la red de TO e IoT y la detección de anomalías para identificar el comportamiento normal y alertar de desviaciones a los operadores industriales.

Variables de referencia

En la fase de aprendizaje dinámico inicial, la solución utiliza el aprendizaje automático y la inteligencia artificial para observar el tráfico de red de la mina y crear referencias de recursos y procesos. Modela el comportamiento y correlaciona varios tipos de datos, incluyendo información sobre recursos similares dentro de la mina, para determinar cómo se vería la actividad normal.

Eliminación de anomalías

En la segunda fase, monitorización, la solución detecta automáticamente cuándo un componente o proceso específico se está desviando de la referencia y pasando a un estado que podría interrumpir las operaciones de minería. Emplea la correlación avanzada y el contexto operativo para ofrecer una vista sencilla y consolidada de lo que está ocurriendo en la red, y alerta proactivamente a los operadores sobre las correcciones que podrían ser necesarias.



Solución de Nozomi Networks: Alerta de variables de TO
Un comportamiento inusual de dispositivos o del sistema podría conducir a la interrupción operativa y a incidentes graves para la seguridad.

EL DESAFÍO:

- Evitar la interrupción del proceso y costosas reparaciones

LA SOLUCIÓN

Uso de la detección de anomalías para identificar los equipos en riesgo antes de que fallen

- La solución de Nozomi Networks monitoriza la red de TO e IoT, determina las referencias de comportamiento, detecta anomalías y alerta de desviaciones a los operadores.
- Los operadores de las minas dedican menos tiempo a la resolución de problemas y pueden emprender acciones antes de que se produzca alguna incidencia de fallo en los componentes o procesos.

RESULTADOS

Detección proactiva de fallos potenciales en los equipos

Mayor rapidez en la resolución de problemas

Maximización del tiempo de actividad de la línea de producción

5. Detección de ciberriesgos y mejora de la resiliencia cibernética

5.1 Caso de uso: Segmentación de la red de TO para lograr resiliencia cibernética

A principios de este año, un ransomware denominado LockerGoga atacó a los productores de aluminio más importantes del mundo. De acuerdo con los medios de comunicación, el ataque de phishing malintencionado hizo que la organización tuviese que desconectar sistemas informáticos y cambiar a operaciones manuales, lo que provocó costosas interrupciones y la ralentización de la producción.

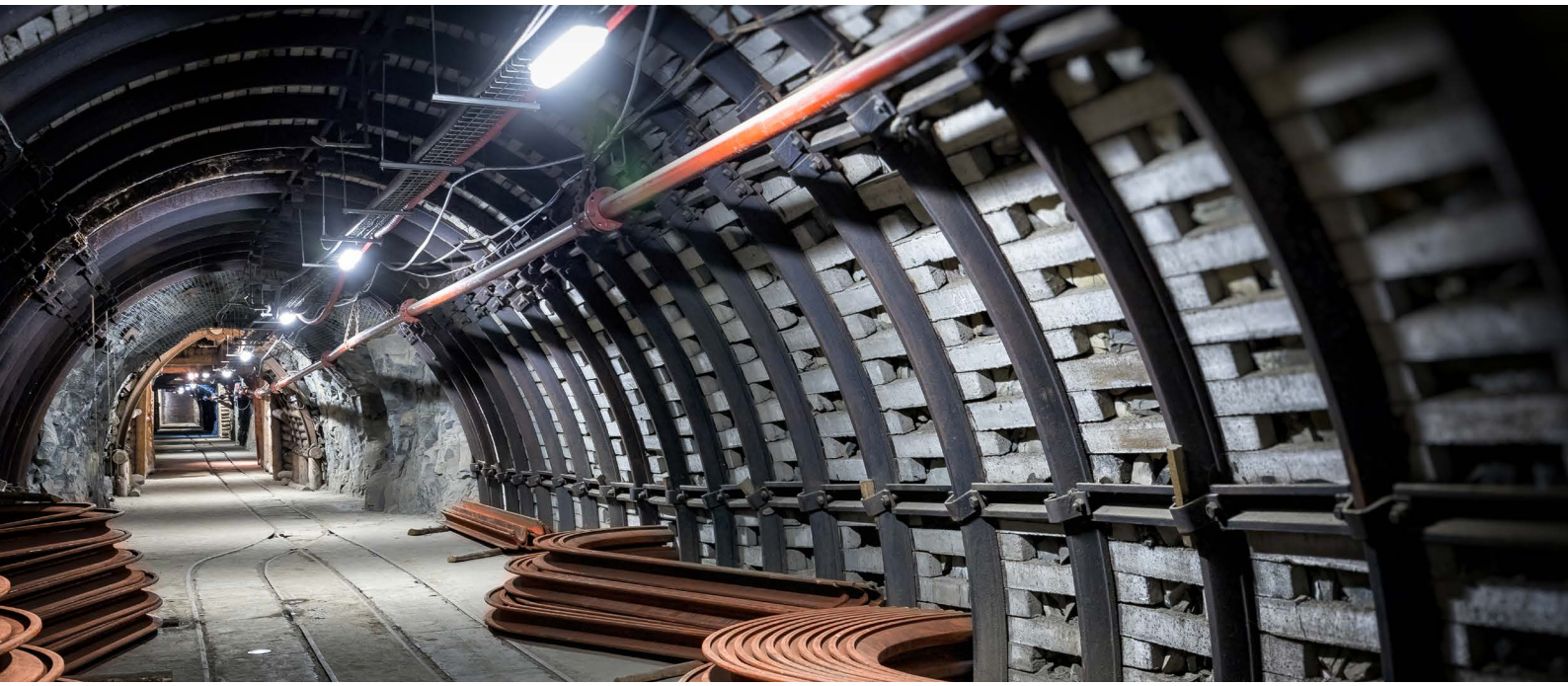
Sin embargo, LockerGoga no es la única ciberamenaza que repercute en las operaciones industriales. Un nuevo tipo de malware de TO e IoT denominado TRITON reprogramó recientemente los controladores del sistema de seguridad instrumentado (SIS) de la instalación y causó una parada automática del proceso industrial.

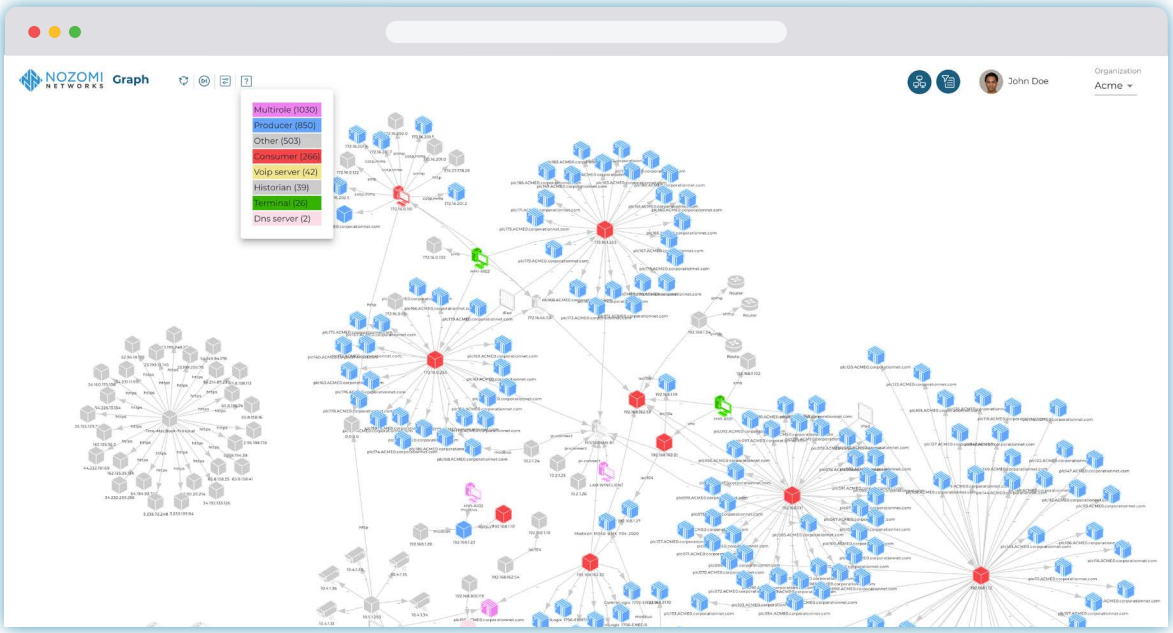
Independientemente de que el incidente cibernético se originara en el lado de TI del negocio o se introdujera intencionada o accidentalmente en el lado de TO, ya no será suficiente un único firewall que separe TI y TO.

Sin una segmentación eficaz de las redes de TO e IoT y SCADA, el ransomware y otras ciberamenazas tienen acceso lateral libre y fluido a los sistemas operativos, lo que provoca interrupciones o daños potencialmente peligrosos.

Como se describe en las normas IEC 62443, la segmentación de TO se considera una práctica recomendada en lo referente al control de las comunicaciones a través de los sistemas de TO, IoT y SCADA. La segmentación de zonas de TO es una forma eficaz de mitigar violaciones perimetrales y evita la propagación de incidentes cibernéticos de TO intencionados o accidentales. Aunque lograr una segmentación eficaz de la red requiere visibilidad de la estructura de red de TO y una perspectiva sobre dónde se encuentran las vulnerabilidades.

Las capacidades avanzadas de visualización de red y evaluación de vulnerabilidades de Nozomi Networks permiten identificar oportunidades para que los operadores de minería refuercen la resiliencia cibernética y eviten la propagación de una infección de la red.





Solución de Nozomi Networks: Topología de visualización de red
El panel de la vista de red permite a los usuarios desplazarse fácilmente y filtrar por diferentes subredes y segmentos de red. Las vistas de la derecha muestran detalles sobre el área de red seleccionada.

EL DESAFÍO:

- Mejora de la resiliencia cibernética con segmentación de la red TO

LA SOLUCIÓN

Visualización de red en tiempo real

- La solución de Nozomi Networks crea automáticamente un mapa de red que identifica oportunidades para generar resiliencia cibernética.
- A continuación, los operadores de minas pueden emplear la segmentación como una medida de mitigación de riesgos para grupos de dispositivos con las mismas vulnerabilidades o requisitos de seguridad.

RESULTADOS

Mayor facilidad de planificación y revisión de los proyectos de segmentación de red gracias a una visualización de red actualizada

Mejora de la toma de decisiones sobre la segmentación en función de evaluaciones fundamentadas sobre vulnerabilidades

Rápida identificación de tráfico inadecuado entre segmentos, mayor rapidez en la resolución de problemas y mitigación

5.2 Caso de uso: Defensa de la mina contra el robo malicioso de datos

En un mundo de intensa competencia sobre reservas cada vez más escasas, los datos corporativos pueden ser igual de valiosos que el oro o los diamantes. El ciberespionaje puede ser una amenaza potencial si el operador de una mina desea obtener una ventaja indebida en negociaciones de fusiones y adquisiciones o al licitar derechos de perforación.

En 2016, uno de los productores de oro más importantes de Norteamérica sufrió un ciberataque donde una considerable cantidad de información corporativa y personal, incluyendo datos de presupuestos y de nóminas, se retuvo a cambio de un rescate. Cuando los hackers no recibieron el pago, publicaron la información en línea para que todos pudieran verla.

Para proteger la posición competitiva y la reputación de la organización, resulta fundamental mantener la confidencialidad de la propiedad intelectual (IP), los planes de negocio, los resultados financieros y otros datos operativos.

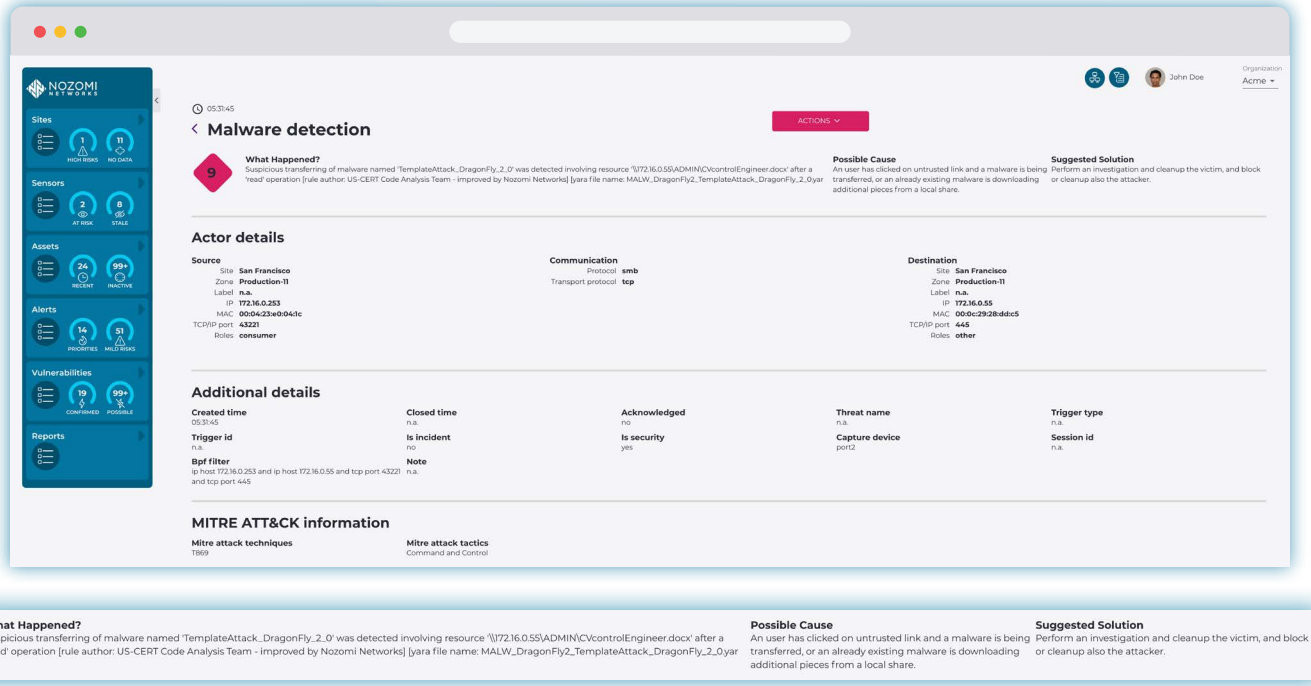
Nozomi Networks adopta un enfoque múltiple para identificar actividades sospechosas, ya sean accidentales o intencionadas.

A través de la detección de anomalías basada en comportamientos y diversos tipos de detección basada en firmas y reglas, la solución identifica actividades no autorizadas como:

- Acceso remoto
- Eliminación de archivos de registro
- Cambios en la configuración
- Descargas
- Cambios en la lógica de los controladores
- Cambios en proyectos de PLC y mucho más

Todos los resultados de la detección de amenazas se correlacionan con el contexto operativo para obtener información detallada. Por ejemplo, la solución comprueba las referencias para las particularidades de la red, por ejemplo, el acceso VPN y los rangos de IP asignados a proveedores de recursos conocidos. Si la actividad se produce fuera de dichos rangos, se activa una alerta.

Cuando se identifica alguna actividad sospechosa, la solución envía alertas de alta prioridad al personal de seguridad y operaciones de la mina que, a continuación, puede ejecutar el plan de respuesta ante incidentes para contener o erradicar la amenaza.



Solución de Nozomi Networks: Detalle de la alerta

La solución de Nozomi Networks adopta un enfoque multidimensional para detectar ciberriesgos y ciberamenazas. Utiliza firmas contra amenazas y detección de anomalías para identificar ataques en curso y proporcionar información clara y útil.

EL DESAFÍO:

- Mantener la confidencialidad de la información corporativa confidencial

LA SOLUCIÓN

Un método integral para detectar ciberriesgos y amenazas

- La solución de Nozomi Networks emplea detección de anomalías basada en comportamientos y diversos tipos de detección basada en firmas y reglas para identificar actividades no autorizadas.
- En función de los detalles de las alertas, los operadores de minas pueden ejecutar un plan de respuesta ante incidentes para contener o erradicar la amenaza.

RESULTADOS

Identificación proactiva de actividades no autorizadas

Mayor rapidez en la ejecución de planes de respuesta ante incidentes cibernéticos

Prevención o mitigación de robo de datos

6. Conclusión

Una mayor visibilidad en entornos de TO e IoT de minería genera resiliencia operativa

Las empresas de minería están adoptando rápidamente herramientas que les ayudan a lograr eficiencia operativa como, por ejemplo, digitalización, automatización e IIoT. No obstante, estos avances vienen acompañados por un aumento de la vulnerabilidad ante los riesgos informáticos debido a la conectividad entre el entorno de TO y los sistemas empresariales o externos.

Para combatir el aumento de las ciberamenazas, los operadores de minería necesitarán inevitablemente abordar desafíos operativos comunes en materia de ciberseguridad, por ejemplo, ganar visibilidad de sus redes de TO e IoT y la eliminación de ineficiencias en materia de seguridad.

LIDERAZGO EN LA INDUSTRIA DE LA MINERÍA

Implementado en

5 de las 10 más importantes empresas de minería

Sin visibilidad de TO e IoT, resulta difícil estar al tanto de los riesgos. Un pequeño cambio o problema en la conexión de red puede aumentar la exposición a ciberamenazas tener impactando la producción, los beneficios y la seguridad de la propiedad intelectual. Aunque una respuesta rápida ante las anomalías es algo crítico, la identificación de problemas antes de que afecten al negocio requiere visibilidad en tiempo real de los recursos de red, las conexiones, las comunicaciones, etc. Desafortunadamente, los operadores de minas suelen tener un déficit en dichas capacidades clave.

Las ineficiencias en materia de seguridad relacionadas con personas, procesos y tecnologías también pueden impactar en la resiliencia operativa. Por ejemplo, la falta de visibilidad de los recursos de TO e IoT puede conducir a puntos ciegos de ciberseguridad. Sin embargo, con la tecnología correcta y un enfoque en mejores prácticas, los operadores de minería pueden generar resiliencia.

Afortunadamente, gracias a tecnologías innovadoras, hoy en día es posible alcanzar una completa visibilidad del entorno de TO e IoT y la monitorización en tiempo real de los sistemas para la detección de amenazas.

La solución de Nozomi Networks mejora la visibilidad de TO e IoT al crear automáticamente un inventario actualizado de todos los recursos de la red. Posteriormente, monitoriza el comportamiento de los dispositivos para detectar anomalías y alerta a los operadores de cambios que podrían indicar problemas potenciales. La solución también proporciona detección avanzada de vulnerabilidades y amenazas, junto con información detallada que permite acelerar la priorización y resolución.

Adaptada para hacer frente a los desafíos específicos de las operaciones de minería, la solución de Nozomi Networks ofrece a los operadores una mayor visibilidad de TO e IoT, minimiza los tiempos de inactividad de la producción, les permite defenderse contra el robo de datos y mejora la resiliencia operativa.

MÁS INFORMACIÓN

Las principales empresas de minería del mundo obtienen considerables beneficios de su inversión en nuestra innovadora solución de visibilidad, monitorización y seguridad de red.

Descubra la rapidez con la que la solución de Nozomi Networks puede generar resiliencia en sus operaciones industriales.

Contacte con nosotros en **nozominetworks.com/contact**

7. Opiniones del cliente

Los clientes dan a Nozomi Networks la máxima puntuación

★★★★★

“Se superaron las expectativas. Mayor visibilidad de la esperada.

Nos aseguramos de que los proveedores con los que trabajamos entiendan que no aplicamos un tipo de solución “fabricada de serie”. Normalmente eso suele ser una complicación para la mayoría, si no para todos los proveedores. Y, como pensaba, la única excepción ha sido Nozomi. Ha superado con creces lo que prometían.

Director senior de seguridad industrial ›

“Una vez que se prueba Nozomi y su potente conjunto de funciones, resulta muy difícil prescindir de esta solución.

Comparamos a Nozomi con otros productos similares y la plataforma de Nozomi fue capaz de seleccionar y categorizar correctamente más dispositivos de L2 que cualquier otra herramienta del mercado en el momento de la prueba.

Analista de seguridad ›

“Grandes soluciones para ICS.

La solución aún dispone de muchas características que gestionan el entorno de TO como, por ejemplo, capacidades de inventario y análisis de vulnerabilidades. Un punto a favor de la solución es el mapa de flujo de comunicación de la red neuronal, que contiene información de gran relevancia para dar una respuesta ante incidentes.

Analista de TI ›

Para obtener más opiniones, visite nuestro sitio web.

Ver todas las opiniones

Qué buscamos en una solución de seguridad y visibilidad de TO e IoT

Los avances tecnológicos, como los que ofrece la solución de Nozomi Networks, pueden mejorar ampliamente la seguridad y fiabilidad.

Al elegir una solución, busque las siguientes características:

- Visibilidad integral de TO e IoT
- Detección avanzada de amenazas
- Alertas precisas de anomalías
- Escalabilidad demostrada en miles de sitios
- Facilidad de integración de TI/TO
- Ecosistema global de socios
- Compromiso y atención al cliente excepcionales

Vea en acción la solución de Nozomi Networks

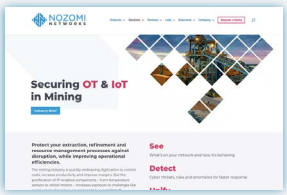
Si desea ver en acción nuestra solución y experimentar lo fácil que resulta trabajar con Nozomi Networks, contacte con nosotros en **nozominetworks.com/contact**

Contacto

¿Desea obtener más información?

RESUMEN DE LA SOLUCIÓN
Nozomi Networks

DESCARGAR



PÁGINA WEB
Solución: Minería

VISITAR

HOJA DE DATOS
Vantage

DESCARGAR

HOJA DE DATOS
Threat Intelligence

DESCARGAR

8. Referencias

1. **"Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19,"** EY, 2018.
2. **"Mining and Metals Information Sharing Analysis Center,"** MMISAC, 2019.
3. **"Hackers target Goldcorp Inc, release reams of private data online including payroll and passports,"** Financial Post, 2016.
4. **"Move to Zero Unplanned Downtime,"** Emmerson, 2012.
5. **"Hydro First Quarter 2019 Report,"** Hydro, 2019.
6. **"Australian metal detector company counts cost of Chinese hacking,"** Reuters, 2015.
7. **"The Cost of Downtime,"** Gartner, 2014.

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 TO e IoT. Los clientes confían en nosotros para minimizar el riesgo y la complejidad al tiempo que maximizan la resiliencia operativa.

© 2022 Nozomi Networks, Inc.
Todos los derechos reservados.

IB-MNG-A4-005

nozominetworks.com