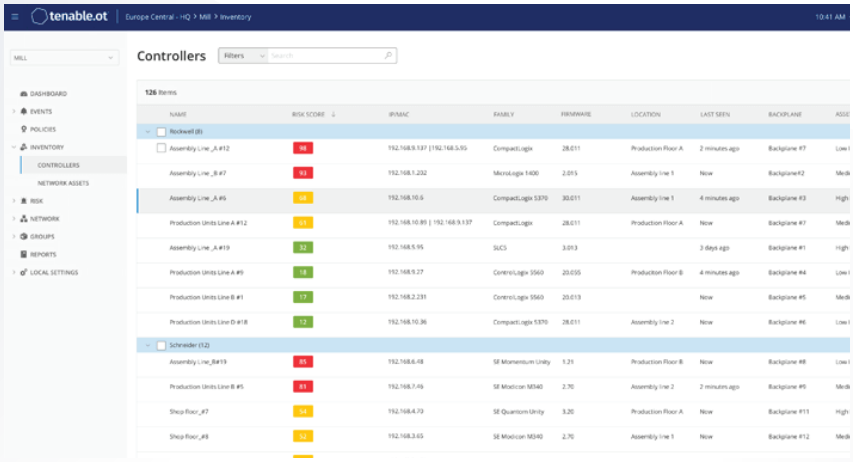
TENABLE.OT™

DESCRIPCIÓN GENERAL DEL PRODUCTO

La esencia de toda planta industrial es una red de sistemas de control industrial, la cual está compuesta por controladores especialmente diseñados para tal fin. Denominados a veces controladores lógicos programables (PLC) y unidades terminales remotas (RTU), estos controladores son dispositivos industriales dedicados que sirven de base para todos los procesos industriales. Los sofisticados entornos actuales de las tecnologías operativas (TO) tienen una amplia superficie de ataque con múltiples vectores de ataque. Sin una visibilidad, seguridad y control completos a lo largo de la TI y la TO convergentes, la probabilidad de sufrir un ataque no es una cuestión de "si ocurrirá", sino de "cuándo ocurrirá".

Tenable.ot™ protege las redes industriales contra las amenazas cibernéticas, los agentes maliciosos con acceso a información privilegiada y los errores humanos. Desde la visibilidad completa a lo largo de toda la superficie de ataque hasta la detección de amenazas y el seguimiento de activos, la gestión de vulnerabilidades y el control de configuración, nuestras capacidades de seguridad del sistema de control industrial (ICS) maximizan la seguridad y la confiabilidad de los entornos de TO. La solución ofrece un conocimiento situacional a profundidad a lo largo de todas las entidades y sus respectivos entornos de TI y TO.

Los controladores lógicos programables (PLC) son fundamentales para las operaciones de la infraestructura crítica. La infraestructura crítica continúa expandiéndose hacia nuevos negocios y disciplinas.



BENEFICIOS PRINCIPALES

- **Obtener una visibilidad total** a lo largo de las operaciones convergentes de TI/TO. Eliminar los puntos ciegos que pueden esconder amenazas laterales que serían capaces de atravesar la TI y la TO.
- **Detectar las amenazas a redes y dispositivos** que afectan a las operaciones industriales y críticas mediante el uso de diversas metodologías de detección. Realizar proactivamente una investigación sobre amenazas con la tecnología de "Vector de ataque".
- **Identificar y dar seguimiento a los activos de TI y de TO** Obtener un conocimiento situacional a profundidad sobre el funcionamiento y el estado de todos los dispositivos.
- **Reducir el riesgo** mediante la identificación y clasificación de vulnerabilidades y posibles amenazas antes de que se conviertan en exploits y tengan un impacto en las operaciones industriales.
- **Dar seguimiento a los cambios de configuración** con capacidades completas de registro de auditoría. Determinar quién hizo cambios, qué cambios se hicieron y por qué se hicieron, así como también su resultado.

BLUEHat Corporation

CAPACIDADES PRINCIPALES

Visibilidad convergente

Tenable.ot proporciona una visibilidad empresarial completa mediante la integración con el resto de la cartera de productos de Tenable.sc y con las herramientas líderes de seguridad de TI, tales como SIEM, SOAR, firewalls de próxima generación, firewalls basados en diodos y mucho más. La plataforma también comparte información con CMDB, plataformas de inventario de activos, herramientas de gestión del cambio y más. Nuestra API RESTful está diseñada para facilitar la extracción de datos incluso hacia herramientas de propiedad exclusiva, lo cual ofrece una visión más coherente de los entornos de TI y TO en un tablero de control único.

Detección de amenazas

Tenable.ot detecta amenazas provenientes de fuentes externas e internas, ya sean humanas o basadas en malware, y emite alertas sobre ellas. Al aprovechar las metodologías de detección múltiple, Tenable.ot identifica comportamientos anómalos de la red, aplica políticas de seguridad de red y da seguimiento a los cambios locales en los dispositivos. Además, Tenable.ot puede ejecutar una detección de amenazas basada en dispositivos que puede identificar problemas de seguridad en dispositivos inactivos que no se comunican por la red, antes de que prolifere el ataque. Esto permite a las organizaciones detectar y mitigar los eventos de riesgo en los entornos de TO. Las alertas, clasificadas en función del contexto, incluyen información ampliada y un registro de auditoría completo, a fin de brindar una rápida respuesta ante incidentes y realizar investigaciones forenses más ágiles.

Seguimiento de activos

Las capacidades de visualización y detección de activos automatizada de Tenable.ot proporcionan un inventario completo y actualizado de todos los activos de la red, incluyendo estaciones de trabajo, servidores, HMI, historiadores de proceso, PLC, RTU, IED y dispositivos de red. Las capacidades de escaneo activo de los dispositivos permiten detectar datos exclusivamente locales y dispositivos en la zona "ciega" de la red. El inventario contiene información profunda y sin precedentes sobre los activos: da seguimiento a las versiones del firmware y del sistema operativo, la configuración interna, el software en ejecución y los usuarios, así como también a los números de serie y la configuración de plano posterior tanto para equipos basados en TI como en TO.

Gestión de vulnerabilidades

Al aprovechar nuestras capacidades de seguimiento de activos, completas y detalladas, Tenable.ot genera niveles de riesgo para cada activo en su red de ICS. Estos informes incluyen la puntuación de riesgos e información detallada, además de sugerencias para la mitigación. Nuestra evaluación de vulnerabilidades se basa en parámetros tales como las versiones del firmware, las CVE relevantes, la investigación de propiedad exclusiva, las contraseñas predeterminadas, los puertos abiertos, las revisiones instaladas y más. Esto permite que el personal autorizado identifique rápidamente nuevas vulnerabilidades y mitigue de manera eficaz los factores de riesgo de la red.

Control de configuración

Tenable.ot da seguimiento a todos los cambios de configuración ejecutados por un usuario o por malware, ya sea a través de la red o directamente en el dispositivo, y los registra. Proporciona un historial completo de los cambios hechos a la configuración de los dispositivos a lo largo del tiempo, incluyendo la granularidad de segmentos de lenguaje ladder específicos, búferes de diagnóstico, tablas de etiquetas y más. Esto permite que los usuarios establezcan una snapshot de copia de seguridad con el "último estado aceptable" para una recuperación más rápida, y para demostrar el cumplimiento de las regulaciones de la industria.

BENEFÍCIESE CON EL "ECOSISTEMA DE CONFIANZA" DE TENABLE

Aproveche sus inversiones de seguridad existentes. Tenable.ot se integra por completo con Tenable.sc y Tenable.io para obtener visibilidad, seguridad y control completos a lo largo de todas sus operaciones convergentes. Tenable.ot trabaja junto con Tenable.ad para identificar errores de configuración y amenazas en Active Directory que puedan provocar ataques de ransomware en los entornos de TO. Tenable.ot también cuenta con una integración completa con las tecnologías de seguridad de TI que ya utiliza, tales como la gestión de servicios de TI, firewalls de próxima generación (NGFW) y proveedores de servicios de gestión de información y eventos de seguridad (SIEM).

Gracias a la integración y a la colaboración a lo largo de la línea de productos de Tenable, así como también de los sistemas líderes de seguridad de TI y de TO, obtendrá el conocimiento situacional que necesita para proteger sus operaciones contra las amenazas actuales de TI y de TO.

ACERCA DE TENABLE

Tenable®, Inc. es la compañía de Cyber Exposure. Más de 30 000 organizaciones de todo el mundo confían en Tenable para comprender y reducir el riesgo cibernético. Como creador de Nessus®, Tenable extendió su conocimiento sobre vulnerabilidades a fin de ofrecer la primera plataforma del mundo para ver y proteger los activos digitales en cualquier plataforma de cómputo. Entre los clientes de Tenable, se encuentran más del 50 % de las compañías de la lista Fortune 500, más del 30 % de las compañías de la lista Global 2000 y grandes instituciones gubernamentales. Obtenga más información en es-la.tenable.com.

LLámanos

+593 98 444 0111
+593 2 382 6909
+1 954 828 2333

Escríbenos

ventas@bluehatcorp.com

Visítanos

/bluehatcorp.com