CLAROTY

CLAROTY CONTINOUS THREAT DETECTION (CTD)

Ficha técnica | Visibilidad total y controles esenciales para los entornos de TO

EL DESAFÍO DE LA SEGURIDAD DE TO Y CLAROTY CTD

Las iniciativas de digitalización han transformado las empresas y ahora las redes de tecnología operativa (TO), que estaban aisladas, están interconectadas con sus equivalentes de tecnología de la información (TI). El resultado es una proliferación de redes empresariales de TI-TO convergentes de cuya protección se ocupan cada vez más los equipos seguridad de TI. El problema es que las partes de TO de dichas redes cuentan generalmente con protocolos propios y activos no conocidos, por lo que no son compatibles con las herramientas de seguridad de TI y, además, son invisibles para los equipos de seguridad de TI.

Claroty Continuous Threat Detection (CTD) fue diseñada para superar esta dificultad. Como base de la plataforma Claroty Platform, la solución CTD extiende a los entornos de TO los mismos controles que utilizan los equipos de seguridad informática para minimizar el riesgo en entornos de TI. Estos controles cubren:

- Administración de activos
- Segmentación de red
- Detección de amenazas y anomalías
- Gestión de vulnerabilidades

FUNCIONALIDADES Y CARACTERÍSTICAS PRINCIPALES:

- Extensión de los controles de seguridad de TI esenciales a los entornos de TO.
- Visibilidad completa de redes que antes eran invisibles.
- Detección continua de anomalías, amenazas conocidas y ataques desconocidos.
- Análisis de la causa fundamental y puntuación de todas las alertas en función de los riesgos.
- Actualizaciones de la inteligencia sobre amenazas en tiempo real a través de Claroty Cloud.
- Informes y paneles personalizados predefinidos.
- Perfecta integración con la infraestructura de seguridad de TI.

ADMINISTRACIÓN DE ACTIVOS

CTD aprovecha la compatibilidad con protocolos de TO más amplia y profunda de la industria y unas funciones inigualables de análisis pasivo, activo y de bases de datos de aplicaciones, para proporcionar visibilidad integral del entorno de TO y controles completos de administración de activos de TO. Claroty es el único proveedor que ofrece este grado de visibilidad en las tres dimensiones de TO fundamentales para el cálculo y la reducción efectiva del riesgo:

1. Visibilidad de activos: incluye todos los activos de una red de TO, como las redes de serie, así como atributos detallados sobre cada activo, incluido el número de modelo, la versión de firmware y la ranura de tarjeta, entre otros.

2. Visibilidad de sesiones: incluye información relativa a todas las sesiones de red, como su duración, las acciones realizadas, los cambios implementados y otros detalles relevantes.

3. Visibilidad de procesos: facilita el seguimiento de todas las operaciones de TO, en algunos casos hasta el nivel del código, con el fin de detectar desviaciones en los procesos y cambios clave

DETECCIÓN DE AMENAZAS Y ANOMALÍAS

CTD utiliza cinco motores de detección para identificar automáticamente todos los activos, comunicaciones y procesos en las redes de TO, generar una línea de base de comportamiento que caracteriza el tráfico legítimo y erradica los falsos positivos, y alertar a los usuarios en tiempo real de las anomalías y las amenazas conocidas y desconocidas. Características principales:

Inteligencia sobre amenazas específicas de TO: CTD incluye inteligencia sobre amenazas específicas de TO que se actualiza en tiempo real a través de Claroty Cloud para adaptarse a los cambios y la detección de amenazas relacionadas con malware.

Puntuación del riesgo de las alertas según el contexto: este indicador único se basa en el contexto concreto y específico en el que se activa cada alerta, y permite a los usuarios descartar fácilmente los falsos positivos, y comprender y priorizar rápidamente las alertas para su clasificación y mitigación.

Análisis de las causas fundamentales: esta función agrupa todas las alertas relacionadas con el mismo evento, ofreciendo para cada alerta unificada una vista consolidada de la cadena de eventos, así como un análisis de la causa fundamental. El resultado es una mejor relación señal-ruido, una reducción de falsos positivos y una disminución de la saturación de alertas, con la consiguiente mejora en la eficacia de la clasificación y la mitigación.

SEGMENTACIÓN DE LA RED

La amplia visibilidad de TO que proporciona CTD le permite asignar automáticamente y segmentar virtualmente las redes de TO en zonas virtuales, que son grupos lógicos de activos que se comunican entre sí en circunstancias normales. Ventajas principales:

Las violaciones de seguridad entre distintas zonas generan alertas en tiempo real que se puntúan automáticamente en función del riesgo, para ayudar a los equipos de seguridad a establecer prioridades.

Las zonas virtuales ofrecen a los clientes sin segmentación física o lógica existente una alternativa rentable.

Los clientes que tienen intención de implementar la segmentación física y lógica pueden acelerar esas iniciativas usando las zonas virtuales como modelo.

Los clientes pueden integrar CTD con sus firewalls y sus productos de control de acceso a la red (NAC) existentes para aplicar de manera proactiva una segmentación basada en políticas y mitigar los ataques activos.

GESTIÓN DE VULNERABILIDADES

CTD compara automáticamente cada activo de un entorno de TO con una completa base de datos de configuraciones, protocolos no seguros y otras vulnerabilidades detectadas por Claroty, así como con los últimos datos de vulnerabilidades y exposiciones conocidas (CVE) de la base de datos National Vulnerability Database. Esto permite a los usuarios identificar, priorizar y corregir las vulnerabilidades en los entornos de TO de forma más eficaz. Características principales:

- **Vulnerabilidades de coincidencia exacta:** la completa visibilidad de TO, con detalles concretos sobre cada activo, que ofrece CTD facilita una identificación fácil y precisa de las vulnerabilidades de coincidencia exacta.
- **Asignación de vectores de ataque:** esta función identifica y analiza todas las vulnerabilidades y riesgos en un entorno de TO para calcular automáticamente los escenarios más probables en los que el agresor podría comprometer el entorno. Además, ofrece recomendaciones de mitigación para cada escenario.
- **Priorización basada en el nivel de riesgo:** todas las vulnerabilidades se evalúan y puntúan automáticamente en función del riesgo específico que suponen para cada entorno de TO, lo que permite una clasificación por prioridades más eficaz y eficiente.

ACERCA DE CLAROTY

Claroty cierra la brecha de ciberseguridad industrial entre los entornos de tecnología de la información (TI) y de tecnología operativa (TO). Esto es particularmente importante para las organizaciones con fábricas y centros de producción muy automatizados, que se enfrentan a un importante riesgo financiero y de seguridad. Equipadas con las soluciones de TI/TO convergentes de Claroty, estas empresas y operadores de infraestructuras críticas pueden aprovechar sus procesos y tecnologías de seguridad de TI existentes para mejorar la disponibilidad, seguridad y fiabilidad de sus activos y redes de TO, sin necesidad de interrumpir la actividad ni disponer de equipos dedicados. El resultado es más tiempo de actividad y una mayor eficacia en las operaciones empresariales y de producción.

Gracias al respaldo y la confianza de los principales proveedores de automatización industrial, Claroty se despliega en los siete continentes a nivel mundial. La empresa tiene su sede central en Nueva York y desde que fue lanzada en 2015 por el reconocido grupo Team8 ha recibido 100 millones de dólares de financiación. Para obtener más información, visite www.claroty.com.