CLAROTY

CLAROTY PLATFORM

Descripción general | Una solución de seguridad de TO completa

La plataforma Claroty Platform está compuesta por los sistemas Continuous Threat Detection (CTD), Enterprise Management Console (EMC) y Secure Remote Access (SRA) de Claroty. Esta solución única y sin agente se integra perfectamente con la infraestructura de seguridad de TI existente y proporciona la más amplia gama de controles de seguridad de TO de la industria, distribuidos en cuatro áreas: visibilidad, detección de amenazas, gestión de vulnerabilidades, y clasificación y mitigación.

Continuous Threat Detection (CTD):

- Descubre y administra automáticamente todos los activos para ofrecer una visibilidad de TO total.
- Detecta las amenazas conocidas y desconocidas en tiempo real.
- Monitoriza continuamente para detectar vulnerabilidades de coincidencia exacta.
- Proporciona segmentación y división en zonas de red, controladas por inteligencia artificial.

Secure Remote Access (SRA):

- Protege, controla y optimiza el acceso remoto al entorno de TO.
- Minimiza el riesgo que introducen los usuarios remotos y externos.
- Aplica las mejores prácticas de seguridad de TI/TO.
- Facilita una auditoría continua para ga rantizar el mantenimiento y el cumplimiento normativo

Enterprise Management Console (EMC):

- Se despliega rápidamente y de forma segura, con cero riesgo de inactividad.
- Proporciona una vista de TI-TO unificada para el centro de operaciones de seguridad (SOC).
- Consolida las alertas y análisis de riesgos entre centros.
- Se integra perfectamente con la infrae structura de seguridad de TI.

Una solución de seguridad de TO completa

VISIBILIDAD

Claroty Platform ofrece una compatibilidad inigualable con los protocolos y métodos de descubrimiento para ofrecer una visibilidad de TO total, que incluye:

- *Visibilidad de activos*, que incluye todos los dispositivos de una red de TO, incluidas las redes de serie, así como un gran número de atributos sobre cada dispositivo, como el número de modelo y la versión de firmware.
- *Visibilidad de redes*, que incluye información relativa a todas las sesiones de red, como su duración, las acciones realizadas, los cambios implementados y otros detalles relevantes.
- *Visibilidad de procesos*, que facilita un seguimiento de todas las operaciones de TO, examinando en algunos casos hasta el nivel del código, con el fin de detectar desviaciones en los procesos y cambios clave.

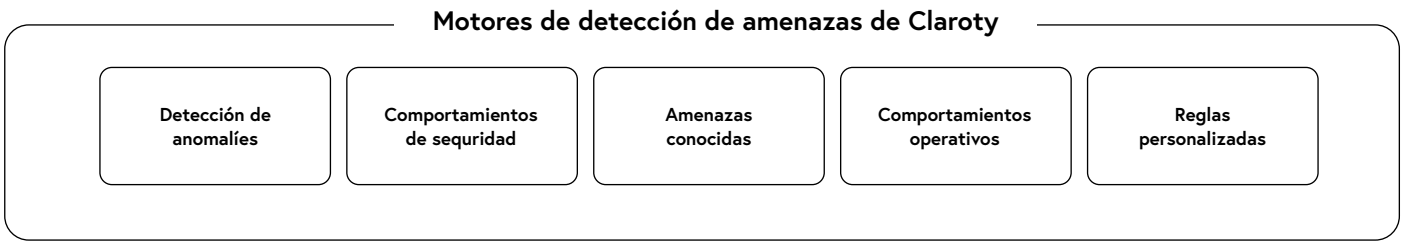
GESTIÓN DE VULNERABILIDADES

La visibilidad que ofrece la plataforma Claroty Platform se extiende a las vulnerabilidades y riesgos presentes en las redes de TO. Entre sus funciones y características principales se incluyen:

- Coincidencia con vulnerabilidades CVE: descubrimiento y evaluación en tiempo real de vulnerabilidades CVE de coincidencia exacta en los activos de red.
- Vectores de ataque: proporciona automáticamente el escenario más probable de compromiso de la red.
- Panel de riesgos: panel personalizable que ofrece una visión general del análisis de riesgos.

DETECCIÓN DE AMENAZAS

CTD utiliza cinco motores de detección para identificar automáticamente todos los activos, comunicaciones y procesos de su red de TO, con el fin de detectar en tiempo real anomalías y amenazas tanto conocidas como desconocidas.



Estas funciones se mejoran con las actualizaciones automáticas de la inteligencia sobre amenazas de Claroty Cloud, que incluyen:

- La investigación sobre amenazas y vulnerabilidades exclusiva del equipo de Claroty
- Indicadores de compromiso
- Los últimos datos de vulnerabilidades CVE de la NVD

CLASIFICACIÓN Y MITIGACIÓN

Todos los aspectos de Claroty Platform funcionan de forma conjunta con un amplio ecosistema de integraciones para optimizar y acelerar los procesos de clasificación y mitigación.

- *Puntuación del riesgo de alerta según el contexto:* indicador único generado por un algoritmo exclusivo para ofrecer contexto acerca de las circunstancias que desencadenan cada alerta.
- *Análisis de causas fundamentales:* las alertas sobre un evento específico se agrupan para proporcionar una vista consolidada de la cadena de eventos, así como un análisis de la causa raíz.
- *Auditoría de sesiones remotas:* se pueden auditar grabaciones de sesiones de red con el fin de investigar el origen de las alertas e identificar detalles fundamentales sobre ellas.

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.