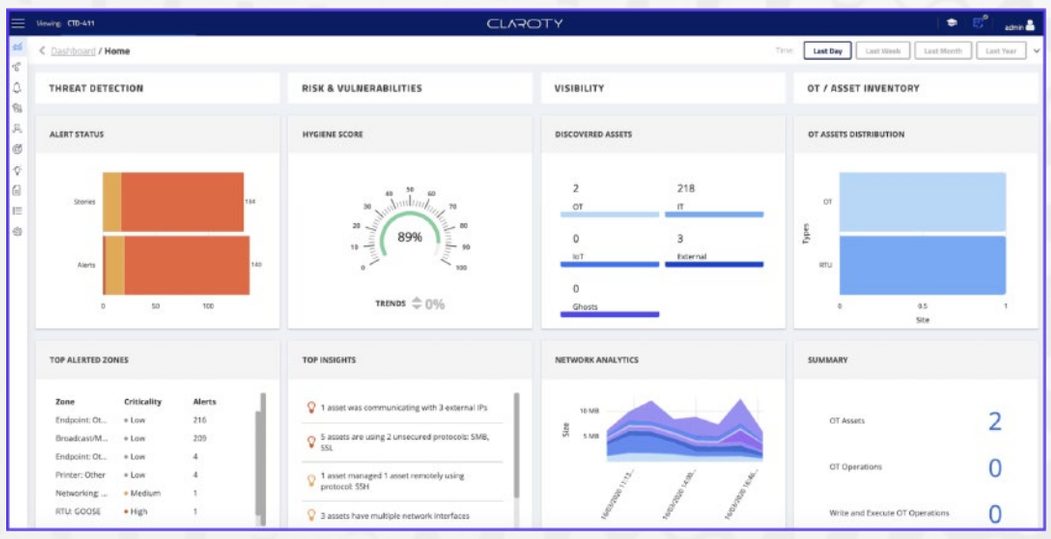
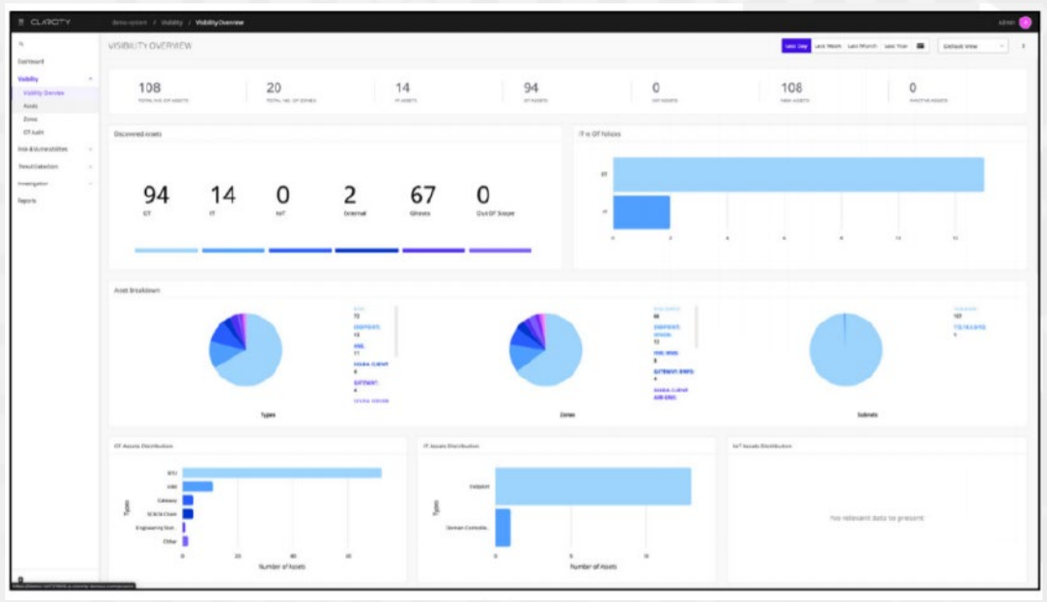
DETECCIÓN DE AMENAZA CONTINUA

Total visibilidad y controles fundamentales para redes industriales.





Resumen de visibilidad CTD

- Extiende los controles fundamentales de ciberseguridad a redes industriales.
- Ofrece una visibilidad completa de lo que antes era invisible en redes industriales.
- Monitorea continuamente para detectar anomalías, conocidas y amenazas emergentes y ataques de día cero.
- Proporciona análisis automático de causa raíz y puntuación basada en el riesgo para todas las alertas.
- Incluye actualizaciones de inteligencia de amenazas en tiempo real a través de la nube de Claroty.
- Revela la frecuencia y el impacto potencial de alertas recibidas por compañeros a través de Wisdom of the Crowd.
- Está completamente armonizado con todos los aspectos de la Plataforma Claroty, incluido el acceso remoto seguro.
- Se integra perfectamente con la seguridad de TI existente infraestructura y flujos de trabajo.

RISOUL MX

Download on the App Store

GET IT ON Google Play

www.risoul.com.mx

VISIBILIDAD INDUSTRIAL Y GESTIÓN DE ACTIVOS

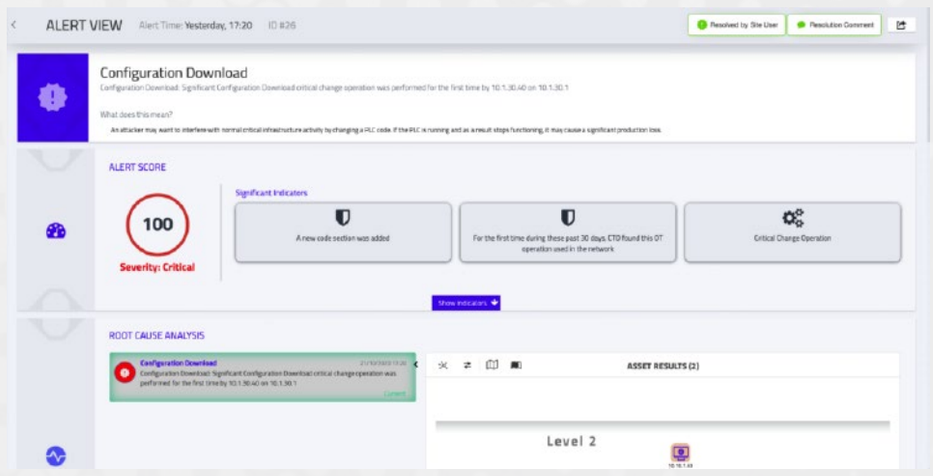
La ciberseguridad industrial eficaz comienza con saber qué se debe proteger. CTD aprovecha la más amplia y profunda cobertura de protocolo industrial en la industria y capacidades de escaneo pasivo, activo y AppDB incomparables para proporcionar controles integrales de visibilidad industrial y gestión de activos, lo que da como resultado un inventario centralizado y altamente detallado de todos Activos, procesos y conexiones de OT, IoT e IIoT. Claroty es el único proveedor que ofrece este calibre de visibilidad en las tres dimensiones integrales para el cálculo y la reducción de riesgos efectivos para redes industriales:

1 **Visibilidad de activos:** abarca todos los activos de OT, IoT e IIoT en una red industrial, incluidas las redes seriales, así como extensos atributos sobre cada activo, incluido el número de modelo, la versión del firewall y la ranura para tarjetas, entre otros.

2 **Visibilidad de la sesión:** esto incluye todas las sesiones de la red industrial junto con su ancho de banda, las acciones tomadas, los cambios realizados.

3 **Visibilidad del proceso:** esto incluye el seguimiento de todas las operaciones industriales, la sección de código y los valores de etiqueta de todos los procesos con qué activos de OT, IoT o IIoT están involucrados, y cualquier cambio anormal en los valores de proceso de estos activos que podría indicar amenazas a la integridad del proceso.

DETECCIÓN DE AMENAZAS Y ANOMALÍAS



Vista de alerta CTD con análisis de causa raíz

Las amenazas a las redes industriales son a menudo innovadoras pero engañosamente simples, explotando nuestra compulsión hacia el proceso para introducir riesgo. CTD utiliza cinco motores de detección para perfilar automáticamente todos los activos, comunicaciones y procesos en redes industriales, generar una línea de base de comportamiento que caracterice el tráfico legítimo para eliminar los falsos positivos, y alertar a los usuarios en tiempo real sobre anomalías y amenazas conocidas, desconocidas y emergentes. Reflejos:

Inteligencia de amenazas específicas de OT: CTD incluye inteligencia de amenazas específicas de la industria que se actualiza en tiempo real a través de Claroty Cloud para respaldar la detección rápida de amenazas.

Puntuación de riesgo de alerta contextual: esta única métrica se basa en el contexto único en el que se activa cada alerta, lo que permite a los usuarios filtrar fácilmente los falsos positivos y comprender y priorizar rápidamente las alertas para la clasificación y la mitigación.

Wisdom of the Crowd: La capacidad Wisdom of the Crowd de Claroty utiliza información anónima de similares eventos en la base de clientes de Claroty para proporcionar contexto sobre la frecuencia y el impacto potencial de la alerta, permitiendo a los usuarios responder de manera más eficaz y eficiente.

Análisis de causa raíz: esta función agrupa todos los eventos relacionados con el mismo ataque o incidente en una sola alerta, proporcionando una visión consolidada de la cadena de eventos, así como un análisis de la causa raíz. El resultado es una relación señal-ruido más alta, menos falsos positivos, menor fatiga de alerta y, por lo tanto, una clasificación y mitigación más eficientes y efectivas.

SEGMENTACIÓN DE LA RED

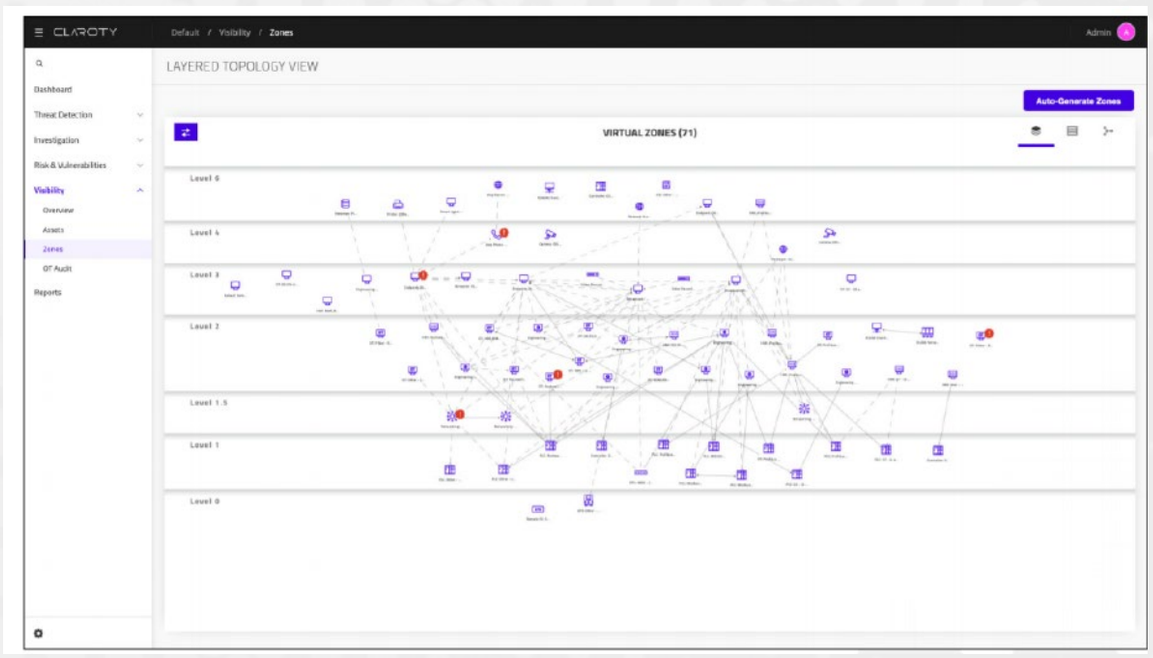
La amplia visibilidad que proporciona CTD le permite mapear automáticamente y segmentar virtualmente redes industriales en Virtual Zonas, que son grupos lógicos de activos que se comunican entre sí en circunstancias normales. Beneficios clave:

Rendimiento de las infracciones entre zonas alertas en tiempo real que son puntuado automáticamente basado sobre el riesgo para ayudar a la seguridad los equipos priorizan.

Clientes sin existente físico o lógico la segmentación puede usar Zonas virtuales como alternativa rentable.

Clientes que buscan implementar físico o lógico la segmentación se acelera tales iniciativas usando Virtual Zonas como modelo.

Los clientes pueden integrar CTD con sus cortafuegos y red productos de control de acceso a hacer cumplir proactivamente la segmentación basada en políticas y mitigar ataques activos.



Zonas virtuales CTD en vista en capas

GESTIÓN DE VULNERABILIDADES

CTD compara automáticamente cada activo en un entorno OT con una extensa base de datos de protocolos inseguros, configuraciones, prácticas de seguridad deficientes y otras vulnerabilidades rastreadas por Claroty, así como a las últimas datos de vulnerabilidades y exposiciones comunes (CVE) de la base de datos de vulnerabilidades. Como resultado, los usuarios pueden identificar, priorizar y remediar las vulnerabilidades en las redes industriales de forma más eficaz.

Vulnerabilidades de coincidencia exacta: la visibilidad completa, incluidos los detalles granulares sobre cada activo de OT, IoT e IIoT, proporcionado por CTD facilita la identificación fácil y precisa de vulnerabilidades de coincidencia exacta.

Mapeo de vectores de ataque: esta función identifica y analiza todas las vulnerabilidades y riesgos en un entorno OT para Calcule automáticamente los escenarios más probables en los que un atacante podría comprometer el medio ambiente. También proporciona recomendaciones de mitigación para cada escenario.

Priorización basada en riesgos: todas las vulnerabilidades se evalúan y puntúan automáticamente en función del riesgo único que representan a cada entorno de TO, lo que permite una priorización más eficiente y eficaz.

GESTIÓN REMOTA DE INCIDENTES

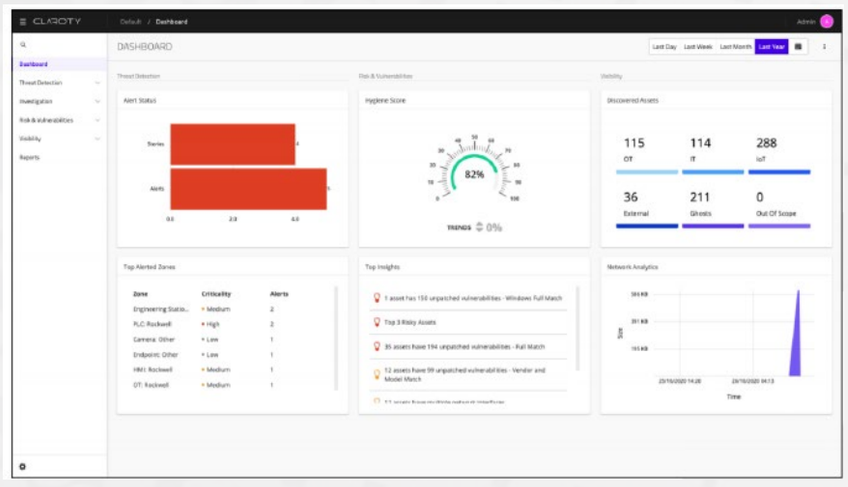
Como parte de un enfoque holístico de la ciberseguridad industrial, CTD y Claroty Secure Remote Access (SRA) unen fuerzas para distinguir a The Claroty Platform como la primera solución de ciberseguridad industrial de la industria que ofrece servicios remotos totalmente integrados capacidades de gestión de incidentes. Estas capacidades abarcan todo el ciclo de vida del incidente, lo que permite a los usuarios detectar, investigar y responder a los incidentes de ciberseguridad industrial en la superficie de ataque más amplia posible desde cualquier ubicación. Como resultado, Las organizaciones pueden evolucionar y adaptar fácilmente su postura de seguridad general y sus flujos de trabajo para un control remoto, distribuido y / o entorno de trabajo muy variable.

Recibir alertas relacionadas con la actividad de usuarios remotos de OT: CTD activa alertas cuando los usuarios remotos participan en actividades no autorizadas o actividades anormales, como descargas de configuración o activos de servicio fuera de las ventanas de mantenimiento predeterminadas - mientras está conectado al entorno de OT a través de SRA Estas alertas contienen información contextual, incluido el usuario de SRA, intención de la sesión, indicadores asociados, activos involucrados y un análisis de la causa raíz para respaldar los esfuerzos de priorización y clasificacion.

Investigar la actividad del usuario remoto de OT: todas las alertas de CTD relacionadas con la actividad del usuario remoto de OT incluyen un enlace directo a la sesión SRA asociada y la capacidad de monitorear esa sesión en vivo. Si la sesión ya no está activa, la alerta se vinculará directamente a una grabación de video de larga duración que se puede ver con fines de investigación.

Responder a la actividad del usuario remoto de OT: todas las alertas de CTD relacionadas con la actividad del usuario remoto de OT también permiten a los administradores desconecte inmediatamente la sesión SRA asociada si se considera necesario como acción de respuesta para prevenir, contener, y / o remediar cualquier daño causado por cambios no autorizados u otras actividades realizadas por usuarios remotos de OT.

CLAROTY Y ROCKWELL AUTOMATION: UN SÓLIDO EQUIPO DE CIBERSEGURIDAD



Vista del panel de CTD

Hace unos años, Rockwell Automation seleccionó a Claroty, líder en software de detección de amenazas y anomalías para redes industriales, como socio de Encompass. Asimismo, Claroty ha designado a Rockwell Automation como socio de élite. Juntos, Rockwell Automation y Claroty se unen para proporcionar productos y servicios de ciberseguridad integrales y líderes en la industria para clientes de todo el mundo.

El software de detección de amenazas de Claroty es una pieza fundamental de la cobertura que ofrecemos como soluciones en ciberataques.