FICHA TÉCNICA

THREATQ DATA EXCHANGE

Cómo pueden ayudar la plataforma de ThreatQ y ThreatQ Data Exchange a las empresas a compartir con eficacia inteligencia de amenazas relevante y filtrada

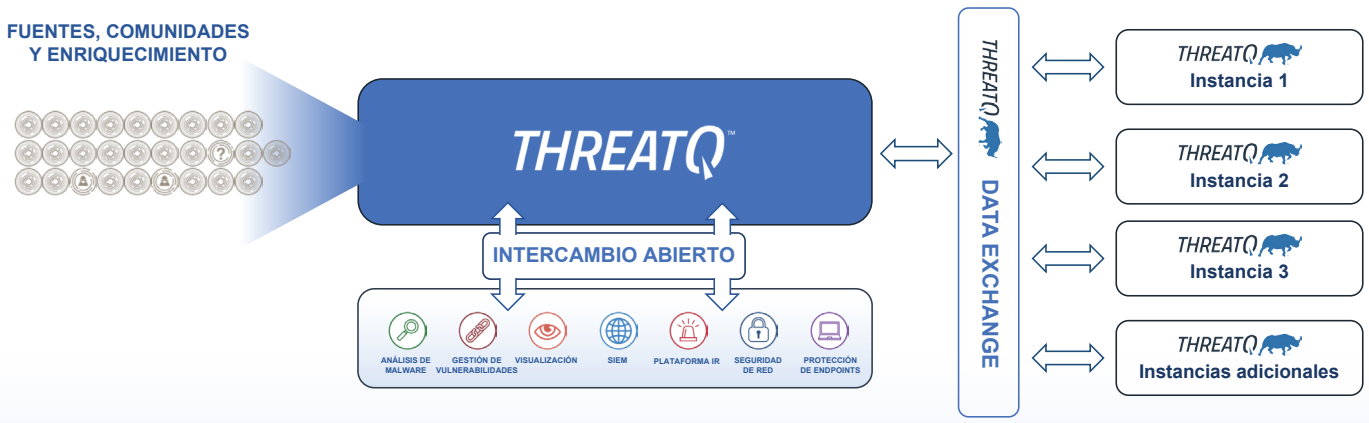
ThreatQ Data Exchange ofrece la mejor forma de facilitar y gestionar la colaboración en asuntos de inteligencia entre varias organizaciones incluso si tienen distinto tamaño y nivel de complejidad. Con ThreatQ Data Exchange es fácil configurar el uso compartido bidireccional de todos los datos de inteligencia en la plataforma de ThreatQ y adaptar dicho uso para numerosos equipos y empresas de todos los tamaños.

La solución, basada en el modelo de datos flexible de ThreatQuotient y compatible con los estándares abiertos de uso compartido de inteligencia, ha sido diseñada para fomentar la personalización y la colaboración. Esto permite a los equipos trabajar según sus propios requisitos y misiones, así como colaborar con sus partners sin limitar la cantidad de datos que desean compartir y sin riesgos de filtrar información que quieren que siga siendo privada.

Características principales

- Una intuitiva interfaz de usuario para establecer con facilidad conexiones bidireccionales o unidireccionales con sistemas externos.
- Gráfico de topología interactiva que representa todos los sistemas conectados y simplifica la administración y la supervisión, aportando escalabilidad.
- Los sencillos flujos de trabajo de instalación aprovechan los paquetes de configuración de conexiones, lo que facilita y permite repetir la tarea de añadir varios nodos conectados.
- Un completo registro de actividad incluye el estado de las conexiones, así como detalles de los datos intercambiados para su seguimiento y la generación de informes.

TRANSFERENCIA DE DATOS CON THREATQ DATA EXCHANGE



¿Quién puede beneficiarse del empleo de ThreatQ Data Exchange?

Toda red multicapa de uso compartido de inteligencia sobre amenazas en la que un administrador global debe tener acceso al control y la supervisión observará que con ThreatQ Data Exchange utilizar la inteligencia sobre amenazas es más rápido y fácil. Por ejemplo:

- Entidades públicas con misiones y equipos concretos de inteligencia que colaboran continuamente y comparten información relevante.
- Los proveedores de servicios de seguridad gestionados (o MSSP) que ofrecen cobertura en varios sectores o áreas geográficas a los clientes finales.
- Medianas o grandes empresas comerciales con presencia internacional o unidades empresariales segmentadas (multinacionales, conglomerados, entidades con influencia en varias áreas geográficas y con requisitos de segregación de datos de inteligencia).

CASO DE USO

Una empresa centraliza las operaciones de seguridad en su sede. Debido a la naturaleza de su actividad empresarial, tiene varias filiales por todo el mundo y necesita compartir inteligencia sobre amenazas filtrada con los equipos de seguridad de dichas oficinas. El equipo de inteligencia sobre ciberamenazas (CTI) en su sede es responsable de recopilar, analizar y priorizar la inteligencia de las amenazas relevantes para su sector. Se debe enviar un subconjunto de esta inteligencia a cada filial con el fin de facilitar una detección coherente en todo el mundo y garantizar la protección contra riesgos para la seguridad global.

Con ThreatQ Data Exchange, el equipo central puede configurar su plataforma de ThreatQ como fuente principal de inteligencia de amenazas en su entorno. Las entidades reciben los datos de esta fuente principal fácilmente. Basta con que generen un paquete de conexiones en la plataforma de ThreatQ principal y lo exporten a cada nodo de las filiales. Una vez que se han implementado estos nodos, se puede iniciar la comunicación.

Los analistas que utilizan la plataforma de ThreatQ principal pueden filtrar la inteligencia sobre amenazas con el fin de que los datos recopilados que reciban y consuman las filiales sean relevantes y prioritarios para sus entornos. El equipo de CTI central puede guardar la búsqueda para que cada vez que creen un grupo de datos y lo compartan para consumo local, esté ya filtrado según los parámetros definidos. Los grupos de datos no se limitan a indicadores técnicos, sino que pueden incluir contexto, así como información sobre malware, campañas específicas y las tácticas, técnicas y procedimientos (TTP) empleados por los ciberdelincuentes, así como sus motivaciones. Al iniciar la transferencia de datos se transmite inteligencia sobre amenazas filtrada a cada filial.

Intercambio bidireccional

También es importante para el equipo de CTI central poder recopilar los comentarios sobre la inteligencia difundida de las filiales en todo el mundo. ThreatQ Data Exchange ofrece integración bidireccional para que se pueda configurar exactamente la misma capa de transporte para que cada filial proporcione sus comentarios al equipo de CTI central. De esta forma, este equipo puede conocer mejor el estado de seguridad de la organización en su conjunto en relación a amenazas específicas que se estén supervisando, con especial atención a las tendencias de los datos e identificando las deficiencias de cobertura.

Además, la comunicación bidireccional puede utilizarse también para generar una memoria global centralizada de amenazas. Cuando cada filial gestione los incidentes de seguridad, descubra nuevas amenazas o encuentre contexto adicional sobre amenazas conocidas, estos datos se pueden almacenar en el repositorio central. Basta con configurar la capa de transporte para que se envíe a la plataforma de ThreatQ principal de forma automática toda la información relacionada con incidentes o la inteligencia creada localmente con el fin de generar una única fuente de verdad que pueda compartirse con los equipos distribuidos por todo el mundo.