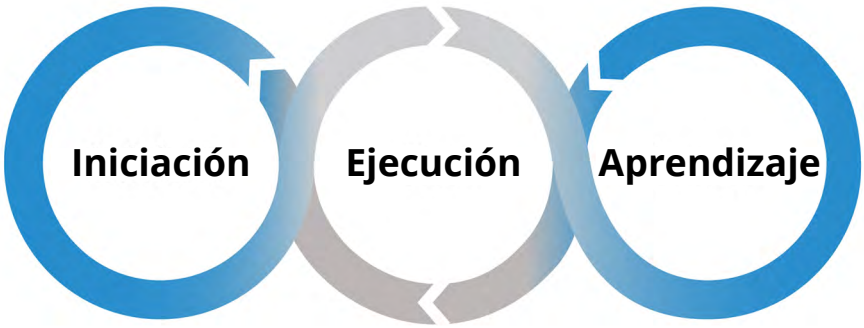
FICHA TÉCNICA

ThreatQ TDR Orchestrator

ThreatQ TDR Orchestrator es la primera solución de la industria que introduce un enfoque simplificado para SOAR, TIP y XDR basado en los datos, que acelera la detección y la respuesta a las amenazas en diferentes sistemas, mejorando la eficacia y la eficiencia de las operaciones de seguridad.

Ante la escasez de personal de seguridad, la automatización se ha convertido en una estrategia clave para liberar a los empleados de las tareas repetitivas de manera que puedan centrarse en las operaciones de seguridad avanzadas con mayor eficacia. Hasta ahora, la automatización se consideraba como definir un proceso y los pasos necesarios para completarlo. Sin embargo, se ignoraba el hecho de que la automatización implica mucho más que llevar a cabo el proceso. De hecho, requiere que se definan y aborden tres pasos fundamentales:



Iniciación: definir sobre qué hay que aplicar medidas y cuándo hacerlo.

Ejecución: aplicar las medidas necesarias o poner en práctica el proceso definido, de principio a fin.

Aprendizaje: grabar lo aprendido para usarlo en análisis y mejorar la respuesta en el futuro.

VENTAJAS Y CARACTERÍSTICAS DESTACADAS

Un enfoque basado en los datos es más fácil de establecer y mantener, emplea menos recursos y proporciona algunas otras ventajas:

Se reducen un 80 % las ejecuciones de playbooks

Se asegura un resultado relevante y prioritario

Se aprende de las medidas aplicadas, lo que permite mejorar con el tiempo

Es fácil realizar la configuración y la ejecución con las herramientas existentes

Con el uso de Smart Collections™ y playbooks basados en datos, ThreatQ TDR Orchestrator pone el énfasis en el aspecto "inteligente" de la plataforma, en lugar de en los playbooks individuales.
La aplicación de Smart Collections y playbooks basados en datos simplifica la configuración y el mantenimiento, y mejora la eficacia de la automatización. Este enfoque aborda los tres pasos de la automatización (iniciación, ejecución y aprendizaje), de manera sencilla y eficaz, ya que permite a los usuarios filtrar y priorizar los datos de antemano, automatizar solo cuando corresponda y simplificar las medidas adoptadas. Puede utilizarse para complementar otras funciones de playbooks a través del ecosistema de partners de ThreatQuotient y los usuarios pueden definir playbooks basados en datos en la plataforma ThreatQ. Para potenciar el aspecto "inteligente" de la plataforma, además, capturará lo que se ha aprendido para optimizar los análisis de datos lo que, a su vez, mejorará la fase de iniciación de la automatización.

THREATQ SMART COLLECTIONS™

Una ThreatQ Smart Collection es un conjunto dinámico de datos basado en criterios específicos que mejora la detección y la respuesta, ya que realiza lo siguiente automáticamente:

- Generar análisis de paneles
- Controlar los datos compartidos en los feeds de ThreatQ Data Exchange
- Compartir datos con determinadas integraciones de ThreatQ para dar respuesta a una amplia variedad de casos de uso
- Iniciar flujos de trabajo automatizados en ThreatQ Orchestrator

Por ejemplo, se puede definir una Smart Collection para los indicadores observados en la red con una puntuación de amenaza entre 6 y 10, y en relación con un atacante concreto, como APT28. La misma Smart Collection puede actualizar paneles, compartir datos en integraciones o plataformas e iniciar un enriquecimiento automático cada vez que se detecten nuevos indicadores que cumplan los criterios.

ThreatQuotient mejora las operaciones de seguridad fusionando diversas fuentes de datos, herramientas y equipos con el fin de agilizar la detección de amenazas y la respuesta que se les da. La plataforma de operaciones de seguridad de ThreatQuotient se basa en datos y ayuda a los equipos a priorizar los incidentes de seguridad, aplicar la automatización y colaborar en su resolución; permite tomar decisiones más fundamentadas; y optimiza el uso de recursos limitados integrando la tecnología y los procesos en un espacio de trabajo unificado. Lo que se logra de esta manera es reducir el ruido, determinar qué amenazas son prioritarias y poder automatizar los procesos con datos precisos. Las funciones líderes en el sector de ThreatQuotient para la gestión de datos, la orquestación y la automatización cubren diferentes casos de uso, como la respuesta a incidentes, la caza de amenazas, el phishing dirigido, la clasificación de alertas y la priorización de vulnerabilidades, y también pueden servir como plataforma para la inteligencia sobre amenazas. ThreatQuotient tiene su sede central en Virginia del Norte y centros de operaciones internacionales en Europa y Asia-Pacífico.

Para obtener más información, visite www.threatquotient.com.