THREATQUOTIENT

**DESCRIPCIÓN GENERAL DEL PRODUCTO**

# THREATQ™

## Una plataforma diseñada para las operaciones de seguridad centradas en las amenazas

Para detener las amenazas con más eficacia y eficiencia, no es preciso que su infraestructura de seguridad actual ni sus empleados trabajen más, sino que deben funcionar de forma más inteligente. ThreatQ actúa como una plataforma de inteligencia sobre amenazas ampliable y abierta que acelera las operaciones de seguridad. Los componentes integrados y autoajustables (Threat Library, Adaptive Workbench, ThreatQ Investigations y Open Exchange) permiten comprender rápidamente las amenazas, tomar mejores decisiones, y acelerar la detección y la respuesta.

**PRIORIZAR**

**INTEGRAR**

**AUTOMATIZAR**

**COLABORAR**

**"La plataforma ThreatQ de ThreatQuotient se integra sin problemas con las tecnologías y herramientas que ya tienen sus clientes, por lo que puede autoajustar rápidamente su biblioteca de amenazas en función de las necesidades de los clientes. De esta forma, ThreatQ se convierte en la plataforma perfecta para los clientes que desean supervisar y bloquear amenazas, aunque cambien las circunstancias en la empresa".**

*~ Mohammed Riyaz Ahmed, analista industrial, Frost & Sullivan ~*

## THREAT LIBRARY

### Inteligencia relevante y contextualizada compartida entre sistemas y equipos

La biblioteca de amenazas puntúa y prioriza automáticamente la inteligencia sobre amenazas en función de los parámetros que se definan. La priorización se calcula entre muchas fuentes distintas, tanto externas como internas, para ofrecer mediante el contexto acumulado una única fuente de verdad. De esta forma, se eliminan los resultados irrelevantes y se reduce el riesgo de falsos positivos.

- Ajuste automático
- Contexto de datos externos + internos
- Importación de datos estructurados y no estructurados
- Priorización automática basada en todas las fuentes
- Fuente de enriquecimiento personalizado para los sistemas existentes

## OPEN EXCHANGE

### Arquitectura abierta y ampliable para tener un ecosistema robusto

Importe y agregue fuentes de datos externos e internos, integre la información con herramientas de enriquecimiento y análisis existentes, y exporte la inteligencia adecuada a las herramientas apropiadas, en el momento justo, para acelerar la detección y la respuesta. Saque más partido a sus inversiones en seguridad actuales integrando herramientas, equipos y flujos de trabajo a través de interfaces estándar y una SDK/API que permite la personalización.

- Incorporación de sus propios conectores y herramientas
- Apps comerciales para integraciones sencillas
- SDK/API para la personalización
- Compatibilidad con STIX/TAXII estándar

## ADAPTIVE WORKBENCH

### Combinación de automatización e inteligencia humana para disfrutar de detección y respuesta proactivas

La configuración definida por el cliente y las integraciones trabajan con sus procesos y herramientas para mejorar la eficacia de sus equipos. El flujo de trabajo personalizable y el enriquecimiento específico para el cliente permiten optimizar el análisis de los datos y eventos de las amenazas con el fin de agilizar la investigación y la automatización del ciclo de vida de la inteligencia.

- Vista consolidada, opinión unificada
- Evaluación continua de las amenazas
- Sencillas operaciones con las herramientas y procesos actuales
- Paneles personalizables, específicos para cada caso

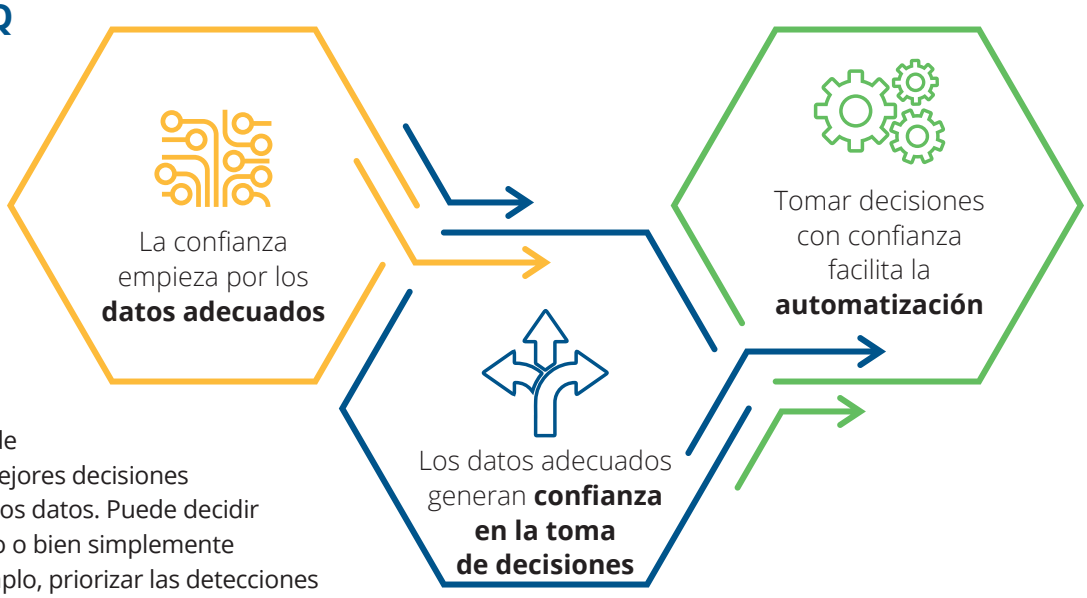
## THREATQ INVESTIGATIONS

### La primera sala de análisis de ciberseguridad del sector

ThreatQ Investigations resuelve el problema de la descoordinación y las ineficiencias en las operaciones de seguridad con el fin de acelerar la detección y la respuesta. Esta solución, que es la primera sala de análisis de ciberseguridad, optimiza las investigaciones y mejora la colaboración activa entre los equipos.

- Fusión de datos de amenazas, pruebas y usuarios.
- Aceleración de las investigaciones, análisis y comprensión de las amenazas para actualizar su nivel de defensa de manera proactiva.
- Reducción del tiempo medio hasta la detección (MTTD) y el tiempo medio hasta la respuesta (MTTR).
- Creación de cronologías de incidentes, adversarios y campañas.
- Aplicación de medidas y respuestas estándar en toda la infraestructura de seguridad desde la interfaz de investigación.

## El enfoque de ThreatQ para implementar la estrategia SOAR




En ThreatQuotient pensamos que un enfoque de SOAR y de las operaciones de seguridad centrado en las amenazas mejora la eficiencia, la coherencia y la eficacia a nivel global. Si empieza por conocer la amenaza y la situación concreta de riesgo del cliente, podrá tomar mejores decisiones automatizadas con confianza en los datos. Puede decidir automatizar un proceso completo o bien simplemente determinados aspectos, por ejemplo, priorizar las detecciones reales frente a las irrelevantes, determinando de qué alertas ocuparse primero, e implementar las mejores respuestas y medidas.

### Cómo lo hacemos:

- Evaluación y priorización continuas de datos, eventos y alertas de amenazas.
- Calificación específica de cada cliente, lo que se traduce en una inteligencia y un contexto muy fiables y relevantes.
- Priorización dinámica para comparar eventos y alertas.
- Recopilación de las opiniones en una base de datos central para un intercambio instantáneo del conocimiento.
- Optimización automática a medida que se conocen más datos y más contexto.
- Mayor eficiencia y eficacia de los procesos *downstream*.

**"Con ThreatQ, nuestro tiempo de investigación se redujo un 80 % y nuestra tasa de falsos positivos y falsos negativos, un 50 %".**

*~ Antonin Hilly, director ejecutivo de MSSP, COO y CTSO, Sopra Steria ~*

# EL PODER DE THREATQ

La plataforma ThreatQ ofrece las siguientes ventajas:

## ADMINISTRACIÓN DE INTELIGENCIA SOBRE AMENAZAS

Convierta los datos en inteligencia sobre amenazas gracias a la aportación del contexto y priorice automáticamente la información en función de las puntuaciones y la relevancia definidas por el usuario.

## CAZA DE AMENAZAS

Permite a los equipos buscar de manera proactiva actividad maliciosa no detectada aún por la red de sensores.

## RESPUESTA A INCIDENTES

Consiga una visibilidad global de las tácticas, técnicas y procedimientos empleados por los adversarios, con el fin de mejorar la calidad, la cobertura y la velocidad de las medidas correctivas.

## PHISHING DIRIGIDO

Simplifique el proceso de análisis y examen de los mensajes de correo electrónico de phishing dirigido, para mejorar la prevención y la respuesta.

## CLASIFICACIÓN DE ALERTAS

Envíe solamente inteligencia sobre amenazas relevante para limitar la cantidad de alertas que deben investigarse.

## GESTIÓN DE VULNERABILIDADES

Centre los recursos en las áreas de mayor riesgo y priorice las vulnerabilidades gracias a que se sabe cómo se están aprovechando.

### FUNCIONES DE THREATQ:

- Ingestión de datos de amenazas procedentes de fuentes internas y externas
- Ingestión de inteligencia estructurada (XML, JSON, CSV, etc.) y no estructurada
- Integración con fuentes comerciales, OSINT e ISAC
- Agregación, desduplicación, normalización y enriquecimiento de datos sobre amenazas
- STIX 1.1, STIX 1.2, STIX 2.0, TAXII
- Almacenamiento de muestras, informes e incidentes de malware
- Puntuaciones definidas por el cliente
- Paneles personalizables
- Listas de seguimiento
- Administración de firmas y reglas (YARA, OpenIOC, Bro/Zeek, Surricata, Snort)
- Operaciones integradas para automatizar las tareas manuales
- Acciones de conjuntos masivos de datos
- Caducidad automatizada
- Intercambio de datos personalizable
- Distribución de tareas en el equipo
- Generación de informes definidos por el usuario (PDF y JSON)
- TLP
- Marcados TLP detallados
- Modelos/objetos de datos personalizados
- API/SDK abiertos
- Integración bidireccional con SIEM, EDR, respuesta a incidentes, etc.
- Visualización de amenazas
- Funciones de búsqueda de texto completo/índice de documentos
- Integración con el marco MITRE ATT&CK
- Cronologías y análisis de eventos
- Análisis de phishing dirigido
- Supervisión proactiva del estado de las fuentes

### OPCIONES DE DESPLIEGUE:

- Local
- Basada en la nube
- Alojada
- Instancia virtual
- Entorno aislado (air-gapped)

El objetivo de ThreatQuotient es mejorar la eficacia y la eficiencia de las operaciones de seguridad mediante el empleo de una plataforma centrada en las amenazas. Gracias a la integración de los procesos y tecnologías de una organización en una sola arquitectura de seguridad, ThreatQuotient acelera y simplifica las investigaciones y facilita la colaboración tanto dentro de cada equipo, como entre distintos equipos y herramientas. Mediante la automatización, la priorización y la visualización, las soluciones de ThreatQuotient reducen la cantidad de información irrelevante y destacan las amenazas que tienen mayor prioridad con el fin de facilitar su detección y ayudar con la toma de decisiones cuando los recursos son limitados. ThreatQuotient tiene su sede central en Virginia del Norte y centros de operaciones internacionales en Europa, Asia Pacífico y Oriente Medio-Norte de África. Para obtener más información, visite **www.threatquotient.com**.

THREATQUOTIENT Sales@ThreatQ.com • +1.703.574.9885