CASO DE ÉXITO DE CLIENTE

Sysdig elige ThreatQ para ampliar las soluciones de detección de amenazas y respuesta

Sysdig elige la plataforma ThreatQ para centralizar las operaciones de seguridad basadas en inteligencia, lo que le ha permitido ahorrar tiempo y mejorar las funciones de detección e investigación de amenazas a gran escala.

Desafío

En los últimos años, la transición a la nube se ha acelerado de forma dramática y esto ha generado una enorme demanda de los servicios de Sysdig por parte de las empresas para mejorar su nivel de seguridad en la nube. Como líder en seguridad para la nube y los contenedores, Sysdig detecta amenazas en tiempo real mediante una combinación de aprendizaje automático, reglas filtradas y directivas de Threat Research de Sysdig. Sysdig analiza cientos de indicadores de compromiso (IoC) de una amplia variedad de fuentes para enriquecer y contextualizar sus detecciones. Gracias a esta inteligencia sobre amenazas en constante evolución, el equipo Threat Research de Sysdig crea, ajusta y distribuye las reglas a los clientes a través de la plataforma Sysdig a fin de detectar amenazas en los contenedores, la infraestructura de nube y el plano de control de Kubernetes, y aplica la respuesta.

El equipo, que incluye expertos en seguridad informática y aprendizaje automático de todo el mundo, también crea otros recursos relacionados con las amenazas (informes, artículos y blogs), para compartir inteligencia sobre amenazas de manera más amplia.

Con el aumento de las operaciones de Sysdig, Michael Clark, director de Threat Research en Sysdig, sabía que el equipo de Threat Research había sobrepasado la capacidad de la base de datos estándar que utilizaban para almacenar los datos de indicadores. Necesitaban una solución con funciones que les ayudaran a agregar, gestionar y almacenar múltiples fuentes de inteligencia, incluidas OSINT, fuentes de otros proveedores de primer nivel e inteligencia sobre amenazas desarrollada internamente por Sysdig, por ejemplo a través de su red de honeypots.

"Con la plataforma ThreatQ, podemos escalar nuestras capacidades de investigación sobre amenazas ahora y en el futuro. Ya sea añadiendo nuevas fuentes de inteligencia, nuevas y mejores reglas, o incorporando ThreatQ Data Exchange para compartir datos entre equipos distintos".

– Michael Clark, director de Threat Research en Sysdig

DESCRIPCIÓN

SECTOR: Tecnología

CLIENTE DESDE: 2022

EMPLEADOS: 700

INGRESOS TOTALES: Capital privado

UBICACIÓN: San Francisco, CA (EE. UU.)

DESAFÍO

Recopilación, seguimiento y generación de informes paralelamente al crecimiento del volumen de datos de amenazas y el número de fuentes. Mejora de las reglas de detección de amenazas con los datos de fuentes de detección.

SOLUCIÓN

La plataforma ThreatQ con el motor DataLinq Engine satisface los principales criterios de Sysdig para una gestión más eficaz y eficiente de la inteligencia sobre amenazas: compatibilidad con múltiples fuentes, caducidad de datos sobre amenazas, priorización de indicadores, integración basada en API, facilidad de exportación y flexibilidad para adaptarse a los requisitos de la nube.

RESULTADO

- ✔ Mejora de las reglas de detección para los clientes
- ✔ Ahorro de tiempo para el equipo Threat Research de Sysdig
- ✔ Simplificación y mejora de los informes de inteligencia sobre amenazas

Sysdig también necesitaba una forma más eficaz de proporcionar contexto con cada regla, de manera que los analistas no perdieran tiempo intentando averiguar por qué un indicador es malicioso. Para evitar que el equipo tuviera que recopilar información de distintos sitios y herramientas, querían disponer de un solo lugar para recopilar el contexto que necesitan para enriquecer una regla, y así acelerar los análisis y mejorar el conocimiento.

Solución

Como proveedor de tecnología, lógicamente Sysdig se planteó la opción de crear una solución en lugar de comprarla, pero descartaron la idea por dos razones. Si bien tanto Michael como varios miembros del equipo contaban con experiencia como desarrolladores de software, no quería que fuera necesario ser programador para ser miembro del equipo.

Además, Michael explicó que no solo se trataba de crear una solución. El mantenimiento sería complejo y laborioso, sobre todo si tenemos en cuenta la amplia lista de criterios de Sysdig:

- Compatibilidad con múltiples fuentes
- Caducidad de los datos de amenazas
- Priorización de indicadores para que los clientes reciban solo los que les afectan
- Basada en API para integrarse con la infraestructura de recopilación de datos
- Facilidad de exportación desde la plataforma al proyecto Falco de código abierto para la generación de reglas
- Flexibilidad para adaptarse a la arquitectura de nube y a los distintos tipos de datos

Tras analizar a los principales proveedores de plataformas, Sysdig determinó que la plataforma ThreatQ cumplía los principales criterios y ofrecía importantes funciones adicionales, concretamente:

Flexibilidad: el amplísimo conjunto de API y de conectores personalizados de ThreatQ puede desarrollarse y desplegarse rápidamente para facilitar la integración bidireccional, que permite al equipo Threat Research de Sysdig dar sentido y utilizar enormes cantidades de datos de indicadores y otros datos de amenazas de manera eficaz. Es muy sencillo importar datos de una amplia variedad de fuentes que incluyen tipos de indicadores personalizados, enriquecer los datos de amenazas con contexto, crear y automatizar flujos de trabajo, gestionar la caducidad de la inteligencia sobre amenazas y exportar datos a las herramientas existentes para generar conjuntos de reglas. Al redactar informes y blogs, la visualización a través de los paneles personalizados también es extremadamente valiosa para medir y clasificar los datos para su análisis.

Resultado

Reglas de detección adicionales enriquecidas con contexto

El equipo puede crear reglas de manera más rápida con datos de un mayor número de fuentes enriquecidas con más contexto, lo que se traduce en mejores detecciones para los clientes. Esto resulta particularmente importante dado el clima geopolítico actual y la rápida evolución del panorama de amenazas.

Ahorro de tiempo para el equipo de investigación de amenazas

La plataforma ThreatQ automatiza las tareas (agregación, deduplicación y normalización). Además, gracias a los parámetros definidos por el equipo de investigación de amenazas de Sysdig, la plataforma también automatiza el enriquecimiento, calificación, priorización y caducidad, lo que permite ahorrar tiempo y reducir el ruido.

Simplificación y mejora de la generación de informes de inteligencia sobre amenazas

La visualización facilita al equipo analizar e informar sobre lo que ve, y compartir su inteligencia con la comunidad de seguridad en general gracias a gráficos atractivos.

Sales@ThreatQ.com • +1 703.574.9885

Arquitectura: la arquitectura flexible y ampliable de ThreatQ es muy importante para Sysdig, ya que les permite cubrir casos de uso específicos y el máximo control, eficacia y velocidad.

Equipo: la experiencia y capacidad de respuesta del equipo de ThreatQuotient estuvieron a la altura durante el período de evaluación y posteriormente. La compatibilidad con flujos de trabajo personalizados e integraciones es rápida, en ocasiones en unas horas o menos, por lo que Sysdig puede moverse a "velocidad de la nube" y ayudar a los usuarios a adelantarse a las amenazas.

Después de trabajar con ThreatQuotient durante unos meses, Sysdig consiguió cubrir sus principales casos de uso.

Exportación: gracias a la exportación de lenguajes de ThreatQ, el equipo Threat Research de Sysdig puede generar rápidamente listas Falco y automatizar la creación de reglas sin tener que utilizar Python o cualquier otro lenguaje externo.

Contenedores: la capacidad de almacenar datos de contenedores en la plataforma ThreatQ, junto con el contexto para comprender por qué un indicador es malicioso, les permite crear su propia fuente enriquecida que se actualiza de manera continua y automática. Las visualizaciones a través de los paneles personalizados también mejoran la generación de informes.

Honeynet: cuando un honeypot de Sysdig está en peligro, el equipo crea un nuevo incidente y utiliza ThreatQ como repositorio de ese conocimiento, lo que les permite determinar si han visto o no un indicador con anterioridad. Si el indicador es nuevo, registran los datos y los comparten como regla con los clientes, asegurándose primero de eliminar el ruido a través de listas blancas. Almacenar estos datos también resulta útil para la investigación de inteligencia sobre amenazas y la generación de informes internos y públicos.

> ***"Nuestra estrategia basada en casos de uso del proceso de evaluación nos llevó claramente a elegir la plataforma ThreatQ para alcanzar nuestros objetivos y devolver el valor a la empresa rápidamente".***
>
> – Michael Clark,
> director de Threat Research en Sysdig

ACERCA DE ThreatQuotient

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. 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. De esta forma se consigue reducir las detecciones irrelevantes, determinar qué amenazas son prioritarias y 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 de inteligencia sobre amenazas. 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**.

Sales@ThreatQ.com • +1 703.574.9885