FIREEYE™

FICHA TÉCNICA

Suscripciones de Threat Intelligence

Informe a su empresa y no solo a sus dispositivos

ASPECTOS DESTACADOS

- Brinda información integral viable sobre amenazas con respecto a una amplia gama de temas
- Ofrece visibilidad más allá del ciclo de vida típico del ataque, incorporando contexto y prioridad a las amenazas globales
- Mejora la protección de los activos e informa mejor las decisiones de riesgos comerciales
- Alinea los programas y recursos de seguridad con respecto a las amenazas y perpetradores más probables
- Aborda casos de uso tácticos, operativos y estratégicos
- Mejora la priorización y corrección de las alertas de seguridad y la solución a vulnerabilidades de seguridad

A menudo, los atacantes cibernéticos están mejor capacitados, cuentan con mejor financiación y están mejor organizados que muchas organizaciones de seguridad. Los ataques cibernéticos son cada vez más complejos y los daños resultantes más graves. Encontrar y retener a un profesional de seguridad calificado es bastante complicado, pero conseguir todos los números necesarios para enfrentar estos desafíos tiene un costo muy alto.

Las organizaciones de seguridad buscan formas de aumentar su propia experiencia y eficacia en seguridad. Necesitan mejorar sus capacidades de respuesta y garantizar que sus defensas estén alineadas contra las amenazas más probables. Todo esto sin caer en bancarrota.

Las suscripciones de FireEye Threat Intelligence enfrentan estos desafíos, de manera rentable, con una amplia gama de información de seguridad viable, efectiva a niveles estratégicos, operacionales y tácticos.

Tabla 1. Beneficios de FireEye Threat Intelligence.

La información identifica...	Ventaja
A qué amenazas y perpetradores se enfrenta debido a su negocio, sector o región	Le permite invertir en medidas de seguridad adecuadas e implementarlas para poder abordar las amenazas
Qué alertas deben investigarse en primer lugar con información contextual asociada	Reduce el tiempo de detección y fatiga por alertas, y aumenta el conocimiento del personal
Qué vulnerabilidades se deben solucionar primero según aquellas que están siendo aprovechadas contra organizaciones similares	Prioriza los esfuerzos en soluciones y reduce la probabilidad de ataques exitosos

Las suscripciones de FireEye Threat Intelligence se personalizan para satisfacer las necesidades de su organización. Los tipos de suscripción incluyen:

- **Fusion:** Información completa sobre la actividad actual, pasada y posibles amenazas futuras. Incluye Operational, Cyber Crime, Cyber Espionage, la mayor parte del contenido de Cyber Physical cibernéticos y una versión adjunta de FireEye Digital Threat Monitoring.
- **Operational:** Análisis técnico de malware y de tácticas, técnicas y procedimientos (TTP) relacionados de perpetradores maliciosos conocidos, incluyendo el acceso a una biblioteca de perfiles de malware, descripciones de perpetradores e indicadores de riesgo (Indicators of Compromise, IOC) legibles por máquina para obtener un marco contextual mejorado sobre las amenazas.
- **Cyber Physical:** Información viable sobre amenazas cibernéticas y entornos industriales y la tecnología operativa (operational technology, OT) en riesgo. Incluye la totalidad de la OT y los sistemas de control industrial (Industrial Control System, ICS) centrados en la inteligencia de FireEye.
- **Cyber Crime:** Evaluaciones en profundidad y seguimiento de perpetradores de amenazas que se centran en delitos financieros: lo que quieren, a quién se dirigen y cómo operan.
- **Cyber Espionage:** Información sobre grupos de amenazas persistentes avanzadas (Advanced Persistent Threat, APT) asociados con naciones específicas, incluido a quién se dirigen y qué TTP utilizan, para ayudar a los equipos de seguridad a comprender y abordar las amenazas inminentes y continuas.
- **Strategic:** Evaluaciones de amenazas en todos los sectores y regiones importantes de la industria, incluyendo la geopolítica, desarrollos que afectan el panorama de las amenazas cibernéticas, y estimaciones sobre cómo evolucionarán los problemas importantes de amenazas cibernéticas a corto y largo plazo.
- **Vulnerability:** Evaluaciones de información sobre vulnerabilidades de software identificadas en muchas tecnologías, junto con evaluaciones patentadas de la probabilidad de explotación y recomendaciones de mitigación.

Por lo general la información se presenta como informes. La información legible por máquina y los IOC están disponibles, cuando corresponda, para integrarse con sus productos de seguridad existentes, como SIEM y administradores de vulnerabilidades. Las suscripciones de FireEye Threat Intelligence también incluyen varios recursos:

- **Portal FireEye Intelligence:** Acceso en línea a los informes de inteligencia y a la biblioteca histórica completa de FireEye Threat Intelligence relacionada con su suscripción específica. Los IOC asociados con tipos específicos de información se pueden descargar y puede realizar búsquedas para encontrar información sobre perpetradores, malware, sectores y otras áreas temáticas.
- **Acceso a los analistas:** Acceda a los analistas de FireEye Threat and Technical Intelligence para obtener una comprensión más clara y profunda sobre los perpetradores, ataques y riesgos. Obtendrá una mejor comprensión sobre cómo cierta información o determinados eventos se relacionan directamente con sus intereses.
- **Opciones de entrega:** Determine la manera en que desea que se entregue su información y con qué frecuencia, incluidas alertas por correo electrónico y resúmenes.
- **Análisis de las novedades diarias:** Un correo electrónico diario que hace un seguimiento de las historias de seguridad actuales que cubren los medios para brindarle una comprensión detallada del panorama de seguridad. Incluye la cobertura de los medios de la historia, la evaluación de FireEye de la precisión de la historia y la información de FireEye relacionada a fin de aumentar su capacidad de comprensión y respuesta.
- **API de información:** Este punto de integración entre equipos le permite utilizar la información de FireEye y nuestros IOC de alta eficacia dentro de sus operaciones de redes y seguridad, gestión de vulnerabilidades y sistemas de respuesta ante incidentes.
- **Complemento para navegadores:** Este complemento amplía la integración técnica de FireEye Threat Intelligence a cualquier página web a la que acceda. El mismo analiza la página web de manera automática en busca de indicadores técnicos (como direcciones IP, dominios, códigos hash), consulta a la API de información acerca de cualquier información relevante de FireEye y luego crea un hipervínculo hacia esa información.
- **Herramientas de análisis:** Los clientes utilizan estas herramientas en línea, vinculadas con la información para preguntar sobre nombres de dominio específicos, direcciones IP y amenazas, y subir archivos sospechosos para su análisis.

Incluso el mejor personal de seguridad no puede conocer todo acerca de cada área temática (incluyendo perpetradores, amenazas, vulnerabilidades, correcciones eficaces, cacería de amenazas). Con las suscripciones de FireEye Threat Intelligence , puede contar con el conocimiento, la experiencia, visibilidad y capacidad de análisis de FireEye, la organización de información sobre amenazas líder en el mundo. Y ahora todos en su organización pueden tener acceso al tipo de información que los mejores profesionales de seguridad pasan años aprendiendo.

La ventaja FireEye

FireEye conoce las amenazas cibernéticas y las personas responsables de ellas más que cualquier otra empresa. Esto se debe a nuestro acceso sin precedentes a la actividad cibernética y nuestras extensas operaciones de información sobre amenazas. FireEye combina información de adversarios, víctimas y campañas con datos de telemetría de productos a fin de generar información sobre amenazas viable que ningún competidor puede igualar. Nuestra inteligencia se basa en lo siguiente:

- Investigadores de campo en 22 países de todo el mundo que hablan más de 30 idiomas que explotan la web profunda y oscura para proporcionar información sobre métodos, motivaciones e infraestructura de adversarios.
- Más de 15 000 sensores de red en modo bidireccional en ubicaciones de clientes que brindan datos sobre qué amenazas están atacando a nuestros clientes en todo el mundo.
- FireEye Mandiant, la organización de respuesta ante incidentes líder en el mundo, proporciona información a partir de investigaciones de ataques sobre las TTP que perpetradores avanzados utilizaron para realizar ataques exitosos.
- La base de datos histórica más grande de actividades relacionadas con amenazas del sector, creada a partir de los datos recopilados en los eventos e incidentes cubiertos por todos nuestros expertos y tecnología.
- FireEye fue nombrado como el único líder en The Forrester New Wave™: servicios externos de información sobre amenazas, T3 2018.

SOPORTE DEDICADO AL CLIENTE

Tres niveles de adaptación y soporte de información para elegir:

NIVEL 1

Básico: Materiales y procesos básicos requeridos para utilizar el portal FireEye Intelligence y configurar la API de información en su organización.

NIVEL 2

Coordinación de información: Básico más un gerente de adaptación de información designado, acceso a consultas con analistas de FireEye Intelligence, informes trimestrales de amenazas y revisiones formales semestrales.

NIVEL 3

Optimización de la información: Coordinación de información más un analista de optimización de información designado, consultas adicionales sobre el análisis, informes sobre amenazas personalizados, talleres estratégicos y reuniones informativas sobre amenazas.

Para obtener más información, visite: **https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.html** y lea el **informe de Forrester**.

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a la de una nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.

FIREEYE™