

FICHA TÉCNICA

Desarrollo de la capacidad de inteligencia

Optimice sus capacidades de inteligencia sobre amenazas



ASPECTOS DESTACADOS

- Optimice su capacidad de consumir, analizar y aplicar inteligencia sobre amenazas dentro de sus operaciones de seguridad cibernética
- Recorra a la experiencia de más de 12 años creando capacidades gubernamentales y comerciales de inteligencia
- Capacidades de inteligencia de referencia existentes y mejoras en los planes
- Determine el riesgo cibernético que enfrenta su organización, la inteligencia que necesita para luchar contra ese riesgo y quién la utilizará
- Elabore los casos de uso estratégicos, operativos y tácticos para la aplicación de inteligencia
- Participe en talleres para mejorar las capacidades de CTI y utilícela con más eficacia en sus actividades diarias

Los atacantes cibernéticos están mejor capacitados, cuentan con mejor financiación y personal que muchas organizaciones de seguridad. Como resultado, los ciberataques se volvieron más complejos y los daños resultantes más graves. Encontrar y retener incluso a un solo profesional de seguridad calificado es complicado, pero conseguir todos los profesionales que necesita con frecuencia tiene un costo muy alto.

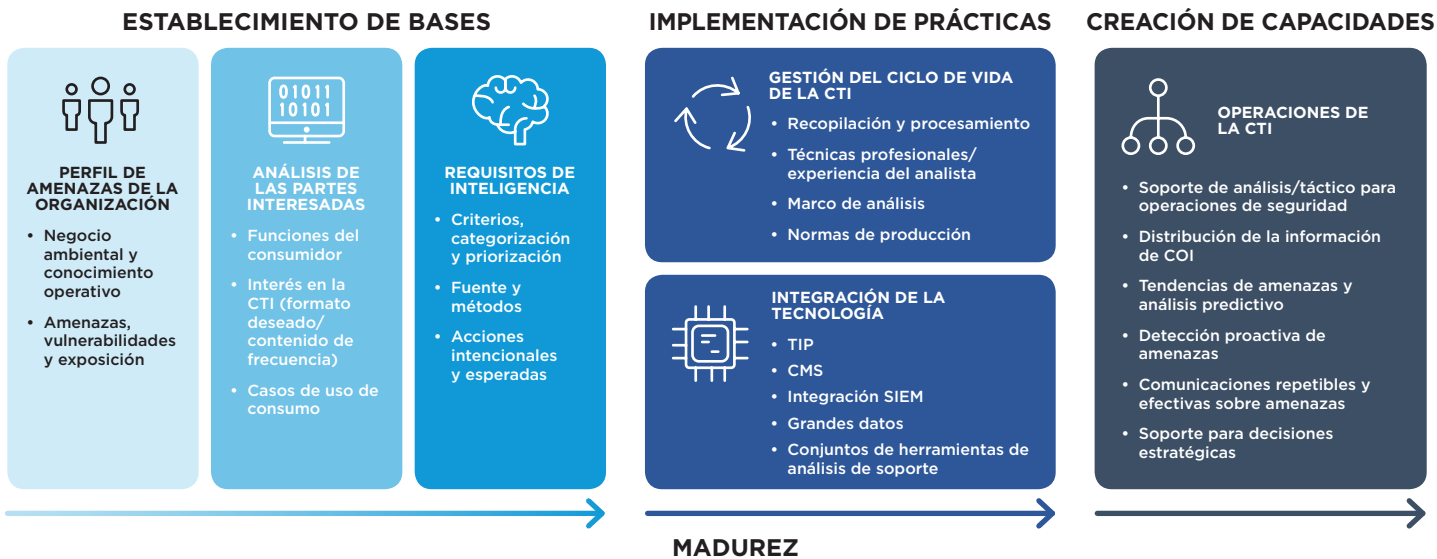
Por estos motivos, más organizaciones buscan reducir los riesgos y aumentar la seguridad con servicios de inteligencia sobre ciberamenazas (Cyber Threat Intelligence, CTI). Sin embargo, muchas organizaciones no saben por dónde comenzar, mientras que otras actúan sin comprender qué tipo de inteligencia sobre amenazas necesitan o cómo deberían utilizarla. Los resultados son generalmente ineficaces y costosos. Las organizaciones deben saber cómo obtener un mejor retorno de sus inversiones en CTI.

Los servicios de desarrollo de la capacidad de inteligencia (Intelligence Capability Development, ICD) de FireEye están diseñados específicamente para ayudar a que las organizaciones concreten el verdadero valor de la CTI. Durante la última década, cientos de organizaciones han trabajado con consultores de ICD de FireEye como asesores de confianza para desarrollar las mejores prácticas para el consumo, análisis y aplicación práctica de la CTI. Como resultado, aumentaron la efectividad y eficiencia de sus programas de seguridad.

Cómo funciona

ICD ha desarrollado un conjunto de servicios de CTI que emplea un marco estandarizado para **evaluar** el estado actual de su programa de inteligencia y amenazas, **diseñar** un programa optimizado para cumplir sus requisitos organizacionales y normativos y **mejorar** las capacidades de su personal con respecto al conjunto de habilidades de análisis y aplicar la inteligencia sobre amenazas a casos de uso específicos.

Este marco define los componentes más críticos de un programa de CTI efectivo.



Los servicios de ICD abordan todos los aspectos del marco y van desde acciones de enfoque limitado centradas en casos de uso específicos hasta implementaciones de programas de inteligencia de gran escala. Todos los resultados se enfocan en aumentar la capacidad de una organización de maximizar el valor de su inteligencia sobre ciberamenazas externas. Las ofertas específicas incluyen:

- **Bases de inteligencia sobre amenazas**
Establece los componentes fundamentales para desarrollar capacidades de inteligencia sobre amenazas. Esto incluye la identificación de amenazas relevantes, las partes interesadas que se beneficiarían del uso de la inteligencia sobre amenazas y las prácticas pragmáticas para lograr una entrega y consumo efectivos. [Evaluar]
- **Diagnóstico de ciberamenazas**
Identifica y documenta el panorama de las amenazas de su organización al analizar el entorno de procesamiento actual para detectar ataques maliciosos. El panorama de las amenazas es una parte crítica de la seguridad basada en la información porque le permite alinear mejor sus defensas y priorizar sus acciones basadas en los motivos e intenciones de los perpetradores que atacan su negocio. [Evaluar]
- **Evaluación de la capacidad de inteligencia**
Evalúa la efectividad de sus capacidades actuales de inteligencia sobre amenazas y qué tan bien se integra la inteligencia en su programa de seguridad. Un análisis detallado de deficiencias acompaña a un plan de actuación estratégico para abordar aquellas deficiencias con recursos, procesos y tecnología. [Evaluar]

- **Mejora de la capacidad de inteligencia**
Desarrolla el plan para ver cómo puede implementar un programa de inteligencia sobre amenazas de clase mundial que incluya procesos repetibles y escalables para la recopilación, análisis y difusión de la inteligencia a lo largo de su organización. [Diseñar]
- **Inicio de la inteligencia**
Presenta muchas de las áreas temáticas que están cubiertas por servicios de consultoría exhaustivos. Este taller interactivo de un día se nutre de la experiencia de nuestros profesionales estratégicos y tácticos de inteligencia para elaborar usos de casos técnicos y operativos para la aplicación de inteligencia dentro de su organización. [Diseñar]
- **Taller sobre la técnica profesional del análisis**
Mejora el conjunto de habilidades de análisis que necesita su equipo para dar soporte a las actividades internas de inteligencia sobre amenazas. En este taller de un día, se cubrirán temas como los conceptos centrales de CTI, técnicas de análisis estructuradas, habilidades de comunicación contra amenazas y enlaces a la gestión de riesgos y amenazas. [Mejorar]
- **Taller de misión de cacería**
Presenta a su equipo un marco de cacería de amenazas que puede utilizarse para estandarizar la forma de realizar esta cacería dentro de su organización. Puede analizar los métodos actuales que emplea para identificar un conjunto de procesos repetibles que representa las mejores prácticas de cacería de amenazas. El programa está diseñado para el Centro de Operaciones de Seguridad (SOC), para la respuesta ante incidentes y los analistas tácticos de inteligencia responsables de las actividades de detección de amenazas. [Mejorar]

La ventaja FireEye

Una asociación estratégica con FireEye asegurará que sus recursos, procesos y procedimientos estén preparados para cumplir con las demandas de un cambiante panorama de amenazas, en cualquier alcance y escala.

El grupo de ICD de FireEye cuenta con más de una década de experiencia creando capacidades de CTI líderes en la industria. Esta experiencia incluye todas las lecciones aprendidas y las mejores prácticas identificadas a través del trabajo con FireEye Threat Intelligence. La investigación de Forrester ha identificado recientemente a FireEye como el único proveedor de inteligencia sobre amenazas en la categoría "líder" en su informe, "The Forrester New Wave™: servicios externos de inteligencia sobre amenazas, T3 2018".

FireEye ha dedicado la última década a trabajar con compañías de sectores verticales para adoptar e integrar la CTI en sus operaciones de seguridad de manera efectiva. Estas experiencias ayudaron a desarrollar y perfeccionar un conjunto de servicios que se adaptan a cualquier necesidad y misión de la organización. Los medios, el gobierno y las organizaciones del sector privado de todo el mundo dependen del liderazgo y de las ofertas de la inteligencia de FireEye.

Si se combinan o entregan por separado, los servicios de ICD apoyan el desarrollo y mantenimiento de un programa integral de inteligencia sobre amenazas.

Para obtener más información, visite: <https://www.fireeye.com/solutions/cyber-threat-intelligence/intelligence-capability-development.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

©2019 FireEye, Inc. Todos los derechos reservados.
FireEye es una marca comercial registrada de FireEye, Inc. Todas las demás marcas, productos o nombres de servicios son o pueden ser marcas comerciales o marcas de servicios de sus respectivos propietarios. I-EXT-DS-US-EN-000201-01

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 los 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.

