MANDIANT®

LIBRO ELECTRÓNICO

CONSIDERACIONES PARA EVOLUCIONAR HACIA LA SEGURIDAD BASADA EN INTELIGENCIA

Introducción

El panorama de ataques actual aparentemente no tiene límites.

Los ciberdelincuentes están activando campañas en todos los países del mundo, utilizando una gran cantidad de técnicas de ataque. Para reducir con éxito el riesgo cibernético, los equipos de seguridad deben saber más sobre los agresores que atacan a su organización, incluyendo quiénes son, las regiones y las industrias que atacan, cuándo fueron vistos, su motivación y las tácticas, técnicas y procedimientos que adoptan. Esta es la promesa de la inteligencia sobre ciberamenazas (cyber threat intelligence, CTI).

Cuando los equipos conocen a los agresores que atacan a su organización y la forma en que operan, los programas para mitigar el riesgo se pueden desarrollar de manera proactiva, impulsando las inversiones en herramientas para proteger su negocio de manera eficaz.

Este libro electrónico analiza lo que los equipos deben considerar a medida que evolucionan su programa de seguridad hacia una capacidad basada en inteligencia, ayuda a evaluar el valor de una postura más proactiva y proporciona un marco para la implementación que incorpora:

- Las fases de transformación hacia un enfoque de seguridad basado en inteligencia
- Cómo evaluar e identificar los componentes clave necesarios para la transformación
- Los componentes básicos de la capacidad de CTI
- Los componentes avanzados de la capacidad de CTI

Para reducir el riesgo cibernético con éxito, los equipos de seguridad deben saber más sobre los agresores específicos que atacan a su organización

Los desafíos de la seguridad basada en el cumplimiento de normativas

Algunas organizaciones confían en la seguridad basada en el cumplimiento de normativas para gestionar su riesgo cibernético. Este enfoque, con su método predecible o de carácter universal, no tiene en cuenta la gran cantidad de complejidades y puntos de diferenciación entre las organizaciones y las industrias en las que operan. Al usar seguridad basada en el cumplimiento de normativas, es probable que las organizaciones se encuentren con lo siguiente:

- **Tienen una estrategia de recopilación de datos sin enfoque:** La organización no puede recopilar inteligencia pertinente porque no conoce a sus atacantes
- **No tienen una misión definida o una declaración de misión:** Sin un propósito, el equipo no puede ser eficaz
- **No comprenden las necesidades comerciales:** No pueden identificar herramientas y estrategias útiles para una protección adecuada
- **No tienen requisitos de análisis:** La organización no sabe qué o a quién debe rastrear

Como resultado, los equipos de seguridad se encontrarán con que tienen un nivel de seguridad reactivo, no saben qué amenazas priorizar, carecen de un enfoque comercial y lo que dificulta la cuantificación del programa de seguridad y su valor.

El valor de una estrategia de seguridad basada en inteligencia

La ciberseguridad basada en inteligencia transforma un nivel de seguridad reactivo en uno proactivo, lo que permite a los equipos de seguridad crear conciencia sobre las amenazas y mitigar los impactos de las vulneraciones. Las decisiones se basan en un análisis profundo, corroboración e información técnica. Incluyen predicciones de expertos y la gestión eficaz de las expectativas de las partes interesadas.

La seguridad basada en inteligencia agrega valor al:

Perfeccionar la estrategia de ciberseguridad

- Identificar las amenazas más relevantes e impactantes que tienen como objetivo una organización, no solo de forma diaria, sino también durante períodos de cambio, como fusiones y adquisiciones o expansión comercial
- Influir en la inversión alineando el riesgo comercial con el programa de seguridad de una organización
- Alinear los recursos contra las amenazas más probables y las capacidades de los perpetradores

Aumentar la eficiencia operativa

- Proporcionar alertas tempranas y habilitar respuestas automatizadas para las amenazas más importantes
- Respaldar el ciclo de vida de la gestión de parches y facultar a los equipos para solucionar las vulnerabilidades que representan el mayor riesgo para una organización
- Permitir que los equipos busquen de manera proactiva a los agresores que atacan su organización e identifiquen su intención, técnicas y herramientas para ayudar a mejorar las defensas de seguridad

Acelerar la capacidad de respuesta

- Brindar los detalles y la inteligencia detrás de un incidente de seguridad
- Ayudar a los equipos a priorizar su respuesta a las alertas

Estos atributos son comunes en entornos que están verdaderamente basados en inteligencia. En las organizaciones donde el programa de CTI está desarrollado, un enfoque basado en inteligencia también puede ayudar a establecer un programa sostenible, lo que satisface las exigencias comerciales y cuantifica el retorno de las inversiones en seguridad.

Fases de la transformación de la seguridad basada en inteligencia

Generalmente, la transformación en cualquier negocio requiere de un enfoque por fases para garantizar que los cambios satisfagan las necesidades de una organización y se implementen de manera metódica. Los expertos de Mandiant recomiendan cuatro fases para transformar un negocio en una operación de seguridad basada en inteligencia, lo que incluye evaluar las capacidades actuales, identificar los requisitos comerciales, implementar sistemas y poner en operación los sistemas.

Fase 1. Evaluación
Obtener una comprensión de las amenazas actuales que enfrenta su organización; quiénes son las partes interesadas clave y cómo la inteligencia sobre amenazas puede ayudar a esas partes interesadas con el tiempo. Examinar las brechas de la CTI y sus correcciones e identificar cómo la CTI podría beneficiar al equipo de ciberseguridad en general.

Fase 2. Diseño
Durante la fase de diseño, elaborar recomendaciones para un programa de CTI alineado con los procesos organizacionales y el ciclo de vida del proceso de la CTI. Documentar los endpoints de integración para todo el equipo de defensa cibernética y crear flujos de trabajo de comunicación específicos de la organización.

Fase 3. Mejora
Desarrollar habilidades y experiencia dentro de su equipo de CTI, lo que puede ser especialmente útil cuando se carece de una base tradicional sobre inteligencia cibernética. Esta fase no solo fortalece las capacidades del equipo, sino que también promueve el consumo, la aplicación y los beneficios de la inteligencia sobre amenazas para las partes interesadas en toda la organización.

Fase 4. Puesta en operación
Alinear la estrategia de la CTI con los procesos y procedimientos. La presentación del programa en etapas hará que la implementación sea manejable y las oportunidades de mejora se puedan registrar después de revisar cada etapa.

Un marco para la seguridad basada en inteligencia

Presentar un programa de CTI puede ser una tarea compleja. La adopción de un marco asegura que se implementen bases sólidas, sobre las cuales una organización puede presentar la tecnología y los procesos que respaldarán sus necesidades a medida que las mismas se desarrollan. Con muchos años de experiencia trabajando en la primera línea de respuesta ante incidentes, los expertos de Mandiant desarrollaron un marco confiable y comprobado para guiar a una organización en su experiencia.

Componentes fundamentales de un marco para la seguridad basada en inteligencia

Establecimiento de bases

Perfil de amenazas de la organización

- Negocio ambiental y conocimiento operativo
- Amenazas, vulnerabilidades y exposición

Análisis de las partes interesadas

- Funciones del consumidor
- Interés en la CTI (formato deseado/ contenido de frecuencia)
- Casos de uso de consumo

Requisitos de inteligencia

- Criterios, categorización y priorización
- Fuente y métodos
- Acciones intencionales y esperadas

Implementación de prácticas

Gestión del ciclo de vida de la CTI

- Recopilación y procesamiento
- Técnicas profesionales/ experiencia del analista
- Marco de análisis
- Normas de producción

Integración de la tecnología

- TIP
- CMS
- Integración al SIEM
- Grandes datos
- Conjuntos de herramientas de análisis de soporte

Creación de capacidades

Operaciones de la CTI

- Soporte de análisis/ táctico para operaciones de seguridad
- Distribución de la información de COI
- Tendencias de amenazas y análisis predictivo
- Detección proactiva de amenazas
- Comunicaciones repetibles y eficaces sobre amenazas
- Soporte a decisiones estratégicas

Madurez

Los desafíos de la seguridad basada en el cumplimiento de normativas | El valor de una estrategia de seguridad basada en inteligencia | Fases de la transformación de la seguridad basada en inteligencia | Un marco para la seguridad basada en inteligencia | El ciclo de vida de la inteligencia | Soporte a través del desarrollo de la capacidad de inteligencia (Intelligence Capability Development, ICD)

Componentes fundamentales de un marco para la seguridad basada en inteligencia (cont.)

Establecimiento de bases

Los componentes fundamentales de la primera etapa deben crear una organización de inteligencia cibernética duradera que pueda determinar:

- Las amenazas que enfrenta una organización, incluidas las amenazas que deben priorizarse
- Las partes interesadas que necesitarán y utilizarán inteligencia sobre amenazas dentro de la empresa
- Los requisitos de inteligencia que servirán mejor a las partes interesadas

Los elementos fundamentales son críticos para un programa de CTI exitoso. Descuidar los componentes fundamentales puede complicar la alineación de las capacidades de inteligencia con las necesidades comerciales cuando las organizaciones deben centrarse en los bloques avanzados a medida que maduran.

Implementación de prácticas

Esta etapa se centra en desarrollar los procesos necesarios para respaldar el uso de la CTI en toda una organización e incluye:

- Capacitar a los analistas que ejecutarán el programa con capacidades de CTI
- Determinar la estrategia de adquisición de datos
- Implementar las herramientas y la tecnología adecuadas

Creación de capacidades

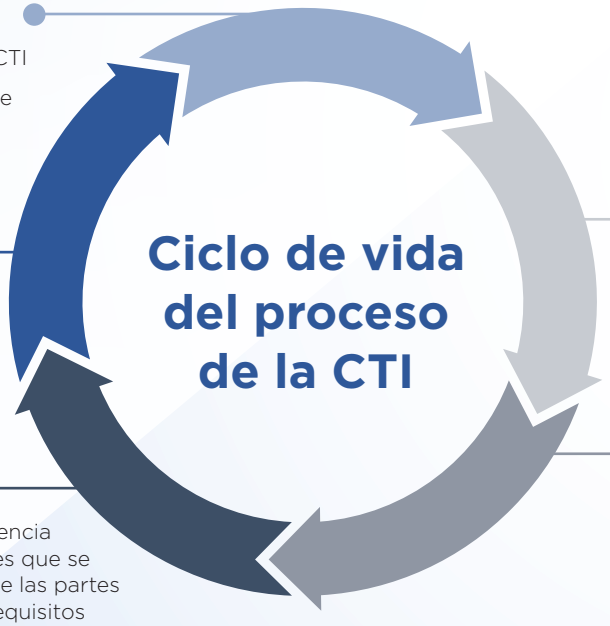
La etapa final crea la capacidad de la CTI, al implementar un flujo de trabajo diario de los procesos que se identificaron en la etapa dos. Esto permite que un equipo de inteligencia sobre amenazas cambie de una posición de detección de amenazas reactiva a una proactiva.

Descuidar los componentes fundamentales puede complicar la alineación de las capacidades de inteligencia con las necesidades comerciales

El ciclo de vida de la inteligencia

Cuando se ha puesto en operación una capacidad basada en inteligencia, los equipos pueden adoptar un ciclo de vida del proceso de la CTI que sirva de guía a través del flujo continuo de planificación, recopilación de datos, análisis, producción y revisión tanto de la inteligencia sobre amenazas como de los medios por los cuales se recopila y aplica en todo el negocio.

El uso de un proceso organizado de la CTI garantiza prácticas estructuradas y coherentes en toda la organización. Para aprovechar todas las ventajas de la gestión comercial y de riesgos de este enfoque, el ciclo de vida del proceso de la CTI y los componentes clave del programa deben manejarse a nivel ejecutivo.



Planificación y requisitos

- Definir las directivas centrales de la CTI
- Identificar y priorizar los requisitos de inteligencia
- Gestionar la ejecución de forma continua

Recopilaciones y procesamiento

- Descifrar la estrategia de adquisición de datos para cumplir con los requisitos
- Normalizar, eliminar los duplicados y enriquecer los datos sin procesar en formas que se pueden utilizar

Análisis

- Evaluar, analizar e interpretar la inteligencia procesada en comparación con los requisitos
- Evaluar las brechas de la recopilación

Producción

- Elaborar productos de inteligencia oportunos, relevantes y viables que se alineen con las necesidades de las partes interesadas y satisfagan los requisitos
- Documentar las deficiencias

Difusión y sugerencias

- Entregar productos de inteligencia terminados a las partes interesadas con frecuencias y métodos definidos
- Obtener y analizar las sugerencias de las partes interesadas

Soporte a través del desarrollo de la capacidad de inteligencia (Intelligence Capability Development, ICD)

Mandiant Threat Intelligence ha pasado la última década ayudando a organizaciones de diversas industrias a adoptar e integrar la CTI de manera eficaz en sus operaciones de seguridad.

Estas experiencias ayudaron a que FireEye desarrollara y perfeccionara un conjunto de servicios diseñados para generar sistemáticamente las mejores prácticas para el consumo, análisis y aplicación práctica de la CTI.

Los servicios de ICD de Mandiant Threat Intelligence van desde operaciones con requisitos específicos hasta implementaciones de programas de inteligencia a gran escala que ayudan a los equipos de seguridad a realizar lo siguiente:

- Encontrar la referencia para las capacidades de inteligencia existentes y las mejoras en la planificación
- Determinar el riesgo cibernético que enfrenta su organización, la inteligencia que necesita para luchar contra ese riesgo y quién la utilizará
- Elaborar los casos de uso estratégicos, operativos y tácticos para la aplicación de inteligencia
- Brindar talleres para mejorar las capacidades de la CTI y utilizarla con más eficacia en las actividades diarias

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

Un conjunto de servicios diseñados para desarrollar sistemáticamente las mejores prácticas para el consumo, análisis y aplicación práctica de la CTI

Acceso a una CTI sin precedentes mediante Mandiant Advantage

Mandiant Advantage ofrece a las organizaciones de todos los tamaños información sobre amenazas actualizada, relevante y fácil de consumir, lo que acelera la toma de decisiones para reducir el riesgo y mejorar el nivel de seguridad de una organización. Los usuarios acceden a inteligencia sobre amenazas que va más allá de las capacidades de las plataformas SaaS de código abierto actuales con información que se obtiene a partir de lo siguiente:

Inteligencia sobre vulneraciones
Durante los últimos 15 años, Mandiant se ha ganado la reputación de ser el principal responsable de la respuesta ante incidentes del sector, asistiendo a más de 800 operaciones de respuesta ante incidentes al año.

Inteligencia operativa
El equipo de Mandiant Managed Defense presta servicios de detección y respuesta a más de 300 clientes desde cuatro centros de operaciones de ciberamenazas internacionales, encargándose de más de 99 millones de eventos y validando más de 21 millones de alertas.

Inteligencia sobre adversarios
Mandiant Threat Intelligence cuenta con más de 200 analistas e investigadores de inteligencia ubicados en 23 países que recopilan hasta 1 millón de muestras de malware por día de más de 70 fuentes diferentes.

Inteligencia artificial
Los expertos de Mandiant aprovechan las tecnologías de FireEye, que tienen aproximadamente cuatro millones de Guest Images virtuales desplegadas a nivel mundial en 102 países, generando decenas de millones de detonaciones en entornos aislados por hora, lo que confirma entre 50.000 y 70.000 eventos maliciosos por hora.

Conclusión

La ciberseguridad basada en inteligencia es transformadora para una organización. Un equipo de seguridad proactivo que opera con inteligencia en tiempo real está mejor equipado para proteger a su organización contra las amenazas, ya que es muy consciente de las amenazas específicas que debe enfrentar.

Las organizaciones necesitan un marco comprobado para que las organizaciones sigan y desarrollen un programa de CTI sostenible y exitoso. En última instancia, sus equipos utilizarán diversos envíos de datos, resúmenes informativos, investigaciones y recomendaciones de priorización para tomar decisiones estratégicas comerciales y de seguridad a diario. Pero primero deben establecer una base sólida que garantice la alineación de cualquier inversión en nuevas capacidades de inteligencia con las necesidades de la organización. Con el tiempo, un compromiso con la evolución continua de la seguridad, combinado con un esfuerzo consciente para incorporar CTI en la estrategia comercial, conducirá a una práctica de ciberseguridad madura y basada en inteligencia.

Para obtener más información sobre cómo mejorar su nivel de seguridad, visite: **www.fireeye.com/intel.**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de Mandiant Solutions
Mandiant Solutions reúne la experiencia en inteligencia sobre amenazas y de primera línea más importante del mundo con una validación de la seguridad continua a fin de armar a las organizaciones con las herramientas necesarias para aumentar la eficacia de la seguridad y reducir el riesgo comercial.

MANDIANT®