

MANUAL DE INTELIGENCIA

Hoja de ruta para crear un
programa de seguridad basado
en la inteligencia

Acerca de Recorded Future

Recorded Future es la mayor empresa de inteligencia del mundo. La plataforma de inteligencia de Recorded Future ofrece la cobertura más completa de adversarios, infraestructuras y objetivos. Al combinar la recopilación y el análisis de datos automatizados persistentes y generalizados con el análisis humano, Recorded Future proporciona visibilidad en tiempo real del amplio panorama digital y permite a los clientes tomar medidas proactivas para disuadir a los adversarios y mantener la seguridad de sus empleados, sistemas e infraestructuras. Con sede en Boston y oficinas y empleados en todo el mundo, Recorded Future trabaja con más de 1400 empresas y organizaciones gubernamentales en 60 países.

recordedfuture.com

Manual de Inteligencia

Cuarta edición

Hoja de ruta para crear un programa
de seguridad basado en la inteligencia

Portada y diseño de Lucas Clauser
Prólogo de Christopher Ahlberg, Ph.D.



Manual de Inteligencia, Cuarta edición

Publicado por:

CyberEdge Group, LLC

1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

Copyright © 2022, CyberEdge Group, LLC. Todos los derechos reservados. Definitive Guide™ y el logotipo de CyberEdge Press son marcas comerciales de CyberEdge Group, LLC en Estados Unidos y otros países. Todas las demás marcas comerciales y registradas son propiedad de sus respectivos dueños.

Salvo lo permitido por la Ley de Derechos de Autor de los Estados Unidos de 1976, ninguna parte de esta publicación puede ser reproducida, almacenada en un sistema de recuperación o transmitida en cualquier forma o por cualquier medio, ya sea electrónico, mecánico, fotocopia, grabación, escaneo o de otro tipo, sin el permiso previo por escrito del editor. Las solicitudes de autorización al editor deben dirigirse al Departamento de Autorizaciones, CyberEdge Group, 1997 Annapolis Exchange Parkway, Suite 300, Annapolis, MD, 21401 o transmitirse por correo electrónico a info@cyber-edge.com.

LÍMITE DE RESPONSABILIDAD O RENUNCIA DE GARANTÍA: EL EDITOR Y EL AUTOR NO OFRECEN NINGUNA GARANTÍA CON RESPECTO A LA EXACTITUD O INTEGRIDAD DEL CONTENIDO DE ESTA OBRA Y RENUNCIAN ESPECÍFICAMENTE A CUALQUIER GARANTÍA, INCLUYENDO, SIN LIMITACIÓN, LAS GARANTÍAS DE IDONEIDAD PARA UN FIN DETERMINADO. LOS CONSEJOS Y ESTRATEGIAS AQUÍ CONTENIDOS PUEDEN NO SER ADECUADOS PARA TODAS LAS SITUACIONES. NI EL EDITOR NI EL AUTOR SERÁN RESPONSABLES DE LOS DAÑOS QUE SE DERIVEN DE ELLA. EL HECHO DE QUE EN ESTA OBRA SE HAGA REFERENCIA A UNA ORGANIZACIÓN O A UN SITIO WEB COMO CITA O FUENTE POTENCIAL DE INFORMACIÓN ADICIONAL NO SIGNIFICA QUE EL AUTOR O EL EDITOR RESPALDEN LA INFORMACIÓN QUE LA ORGANIZACIÓN O EL SITIO WEB PUEDAN PROPORCIONAR O LAS RECOMENDACIONES QUE PUEDAN HACER. ADEMÁS, LOS LECTORES DEBEN SER CONSCIENTES DE QUE LOS SITIOS WEB DE INTERNET QUE APARECEN EN ESTA OBRA PUEDEN HABER CAMBIADO O DESAPARECIDO ENTRE EL MOMENTO EN QUE SE ESCRIBIÓ ESTA OBRA Y EL MOMENTO EN QUE SE LEE.

Para obtener información general sobre los servicios de investigación y consultoría de marketing del Grupo CyberEdge, o para crear un libro *Definitive Guide™* personalizado para su organización, póngase en contacto con nuestro departamento de ventas en el 800-327-8711 o info@cyber-edge.com.

ISBN: 978-1-7371618-2-0 (libro de bolsillo)

ISBN: 978-1-7371618-3-7 (eBook)

Impreso en los Estados Unidos de América.

10 9 8 7 6 5 4 3 2 1

Agradecimientos del editor

El Grupo CyberEdge agradece a las siguientes personas sus respectivas contribuciones:

Editor de textos: Susan Shuttleworth

Diseño gráfico: Debbi Stocco

Coordinador de producción: Jon Friedman

Agradecimientos

La publicación de este libro ha sido posible gracias al personal de Recorded Future, que ha aportado sus conocimientos y experiencia a esta cuarta edición. Entre los colaboradores se encuentran: **Stas Alforov, Andrei Barysevich, Levi Gundert, Lindsay Kaye, Jason Steer, Chris Ueland, John Wetzel, y Ellen Wilson.** Gracias a **Lucas Clauser** por desarrollar el distintivo arte de la portada. También nos gustaría dar las gracias a quienes contribuyeron a las ediciones anteriores de este libro.

Prólogo del **Dr. Christopher Ahlberg**, cofundador y director general de Recorded Future.

Table of Contents

Agradecimientos	iii
Prólogo de la cuarta edición	vii
Introducción	ix
¿Qué es la inteligencia para los equipos de seguridad?	3
Visibilidad de las amenazas antes de que ataque	3
Inteligencia: Datos e información práctica	5
Inteligencia: El proceso	7
¿Quién se beneficia de la inteligencia?	9
Tipos y fuentes	11
Dos tipos de inteligencia	11
El papel de las fuentes de datos sobre amenazas	13
El papel de los canales privados y la Dark Web	15
El ciclo de vida de la inteligencia	17
Las seis fases del ciclo de vida de la inteligencia	17
Herramientas y personas	23
Inteligencia de SecOps Parte 1 - Triaje	27
Responsabilidades del equipo de SecOps	28
El abrumador volumen de alertas	29
El contexto es el rey	30
Acortar el “tiempo hasta el no”	33
Inteligencia SecOps Parte 2 - Respuesta	35
Desafíos continuos	36
El problema de la reactividad	37
Minimizar la reactividad en la respuesta a incidentes	37
Reforzar la respuesta a los incidentes con inteligencia	38
Inteligencia SecOps en acción	39
Características esenciales de la inteligencia SecOps para la respuesta a incidentes	41
Inteligencia sobre las vulnerabilidades	45
El problema de las vulnerabilidades en cifras	45
Evaluar el riesgo en función de la explotabilidad	47
La génesis de la inteligencia para los equipos de seguridad:	
Bases de datos de vulnerabilidades	48
Inteligencia sobre vulnerabilidades y riesgo real	52
Fuentes de información	54
Casos prácticos de la inteligencia cruzada	56
Reducción de las diferencias de riesgo entre los responsables de la seguridad, las operaciones y la empresa	56
Inteligencia sobre amenazas	
Parte 1: conocer a los atacantes	59
Nuestra definición de “inteligencia sobre amenazas”	59
Entienda a su enemigo	60

Las comunidades criminales y la Dark Web	62
Conectar los puntos	64
Caso práctico: Una respuesta más completa a los incidentes	65
Caso práctico: Búsqueda proactiva de amenazas	65
Caso práctico: Aviso anticipado de fraude en los pagos	66
Inteligencia sobre amenazas	
Parte 2: análisis de riesgos	69
El modelo de riesgo FAIR	70
Inteligencia y probabilidades de amenaza	72
La inteligencia y el coste financiero de los ataques	74
Inteligencia de terceros	75
El riesgo de terceros se cierne sobre nosotros	75
Las evaluaciones de riesgo tradicionales se quedan cortas	76
Qué buscar en la inteligencia de terceros	77
Supervise a los terceros en relación con estos cinco riesgos críticos	79
Respuesta a las puntuaciones de riesgo elevadas de terceros	84
Inteligencia de marca	85
Un tipo diferente de detección	86
Descubrimiento de pruebas de suplantación y abuso de marca	87
Descubrir pruebas de infracciones en la web	88
Cualidades críticas para las soluciones de inteligencia de marca	91
Inteligencia geopolítica	93
¿Qué es el riesgo geopolítico?	93
Inteligencia geopolítica	94
¿Quién utiliza la inteligencia geopolítica?	95
Recogida de datos con Geofencing	96
Fuentes de datos e información	97
Automatización, análisis y experiencia	98
Interacción con la inteligencia geopolítica	99
Geopolítica y ciberamenazas	100
Inteligencia sobre el fraude	103
Inteligencia sobre el fraude y evaluación del riesgo	103
Vigilar la exposición de la cartera de tarjetas y la filtración de credenciales	104
Identificar los puntos comunes de compra comprometidos	105
Vigilar los sitios web en busca de Magecart y otros ataques	106
Identificar las señales	107
El retorno de la inversión en inteligencia sobre el fraude	108
Inteligencia de la identidad	109
Protección de la autenticación	109
Un plan para proteger las identidades	110
Fuentes de identidades robadas	111
Triage de gran volumen	112
Uso de la información sobre la identidad	113

Inteligencia de superficie de ataque	117
Su superficie de ataque digital es más grande de lo que cree	117
Descubrir los activos de cara a Internet	119
Análisis de los activos expuestos	120
Supervisión continua de la superficie de ataque	121
¿Quién utiliza la inteligencia de superficie de ataque?	122
Inteligencia para líderes de seguridad	125
Gestión de riesgos	126
Mitigación: personas, procesos y herramientas	129
Inversión	130
Comunicación	130
Apoyo a los líderes de seguridad	131
El déficit de competencias en materia de seguridad	132
Inteligencia para priorizar las amenazas emergentes	135
Planificar hoy el próximo año	135
Uso de los ciclos de vida de los ataques para evaluar los riesgos	136
Deepfakes: la próxima frontera del fraude	138
Contratación de información privilegiada para el fraude	140
Venta de bases de datos y acceso a la red	142
Marcos analíticos para la inteligencia	147
La Cyber Kill Chain® de Lockheed Martin	148
El modelo del diamante	149
El marco MITRE ATT&CK™	152
Fuentes y tipos de datos de inteligencia: Un marco de trabajo	155
Un marco para los datos de inteligencia	155
Acceso inicial	156
Movimiento lateral, escalada y reconocimiento	158
Exfiltración de datos	160
Caída de la carga útil del ransomware	161
Un marco flexible	162
Su viaje de inteligencia	163
No comience con las alimentaciones de las amenazas	163
Aclare sus necesidades y objetivos de inteligencia	164
Factores clave del éxito	165
Empezar de forma sencilla y aumentar la escala	168
Desarrollar su equipo central de inteligencia	171
Dedicados, pero no necesariamente separados	171
Competencias básicas	173
Recogida y enriquecimiento de datos sobre amenazas	174
Compromiso con las comunidades de inteligencia	177
Utilizar la inteligencia para desbaratar a los adversarios	179
Ideas fundamentales del libro	179

Prólogo de la cuarta edición

La pandemia mundial ha acelerado la digitalización de las operaciones internas, de los clientes y de la cadena de suministro. Hoy en día, todo y todos están conectados, y los ciberdelincuentes se aprovechan. Los profesionales de la seguridad, que ya no dan abasto, ahora deben defender una superficie de ataque prácticamente infinita.

A lo largo del año pasado vimos cómo se intensificaban los ataques y las respuestas en forma de bandas de ransomware que detenían los oleoductos y las cadenas de suministro de alimentos; cómo se producían disturbios civiles en todo el mundo, y se censuraba y vigilaba el uso de Internet; cómo se pirateaban las infraestructuras críticas en campañas de cibercapitulación patrocinadas por el Estado; y cómo las campañas de desinformación se dirigían a los gobiernos y a las iniciativas de vacunación contra la COVID-19, por nombrar algunas.

Las estrategias de defensa actuales no están funcionando. Los defensores deben pasar al ataque. Las organizaciones deben pasar a programas de seguridad basados en la inteligencia que anticipen a los adversarios y sus intenciones, vigilen la infraestructura que construyen y aprendan de las organizaciones vulneradas.

En Recorded Future, creemos que la inteligencia es para todos. Independientemente de la función de seguridad que desempeñe, la inteligencia permite tomar decisiones más inteligentes y rápidas. No es un dominio separado de la seguridad. Es el contexto que le permite trabajar de forma más inteligente, ya sea para dotar de personal a un SOC, gestionar las vulnerabilidades o tomar decisiones empresariales de alto nivel. Para ser más eficaz, la inteligencia debe integrarse con las soluciones y los flujos de trabajo en los que ya confía, y tiene que ser fácil de aplicar.

En 2020, Recorded Future introdujo módulos de inteligencia, adaptados para informar sobre casos de uso específicos y resultados en toda la empresa. En 2021 y principios de 2022 ampliamos nuestra cobertura de casos de uso empresarial añadiendo tres nuevos módulos a nuestra Plataforma de Inteligencia: Inteligencia de Identidad, Inteligencia de Fraude e Inteligencia de Superficie de Ataque.

La identidad es el nuevo perímetro que hay que validar y defender. Hemos introducido la Inteligencia de Identidad para ayudar a los defensores a controlar el acceso a los datos sensibles protegiendo y verificando las identidades de los usuarios, detectando el fraude de identidad de los clientes y evitando la toma de control de las cuentas.

Del mismo modo, cada vez es más difícil para las organizaciones identificar y prevenir el fraude con tarjetas de pago antes de que se produzca. Fraud Intelligence ayuda a los defensores a supervisar la exposición de la cartera de tarjetas en tiempo real, a identificar los puntos de compra comunes comprometidos y a supervisar un flujo en tiempo real de dominios de comercio electrónico infectados.

Además, las organizaciones tienen cientos o miles de activos orientados a Internet que son susceptibles de ser atacados, pero no tienen visibilidad de muchos de ellos. La inteligencia de la superficie de ataque les ayuda a encontrar y proteger los sistemas de TI en la sombra, las cargas de trabajo en la nube, los dispositivos móviles, los “dominios olvidados”, los servidores web y los dispositivos IoT con direcciones IP.

Esta cuarta edición del Manual de Inteligencia ofrece información práctica para desarrollar un programa de seguridad basado en la inteligencia. Esperamos que le resulte un compañero informativo y útil a la hora de integrar la inteligencia en su ecosistema de seguridad.

Agradezco a todos los que han contribuido al desarrollo de este Manual: los usuarios de nuestra plataforma, nuestros clientes, los expertos del sector y el equipo de Recorded Future.

**Christopher Ahlberg, Ph.D.
Cofundador y director general
Recorded Future**

Introducción

Una imagen completa de la inteligencia para los equipos de seguridad

Es posible que haya oído que la inteligencia implica la recopilación de datos de una amplia variedad de fuentes, incluida la Dark Web. Quizá sepa que combina esos datos con las opiniones de los expertos en seguridad, y destila los datos y las opiniones en inteligencia para los profesionales de la seguridad informática. Puede trabajar con fuentes de amenazas o informes semanales sobre ataques a la red, o incluso con análisis de expertos sobre riesgos ciberneticos. Sin embargo, es probable que no conozca todos los papeles y funciones a los que da soporte la inteligencia, la cantidad de formas en que protege a las organizaciones y sus activos, y todo su potencial para reducir los riesgos.

Este manual le dará una visión completa de la inteligencia y del papel que desempeña en la protección de su organización. La sección 1 ofrece una visión general de la inteligencia para los equipos de seguridad y las fases del ciclo de vida de la inteligencia. La sección 2 examina las formas específicas en que la inteligencia refuerza varias funciones críticas de seguridad y sus flujos de trabajo. La sección 3 aborda cuestiones de gestión y aplicación, como el uso de la inteligencia para evaluar el riesgo y justificar las inversiones, y cómo crear un equipo de inteligencia.

Al final, comprenderá cómo la inteligencia amplifica la eficacia de los equipos de seguridad y de los líderes de seguridad al exponer las amenazas desconocidas, aclarar las prioridades, proporcionar datos para tomar decisiones mejores y más rápidas, e impulsar una comprensión común de la reducción de riesgos en toda la organización.

Ya no es solo “inteligencia sobre amenazas” o “inteligencia sobre seguridad”

Hasta hace poco, los temas tratados en este libro se conocían comúnmente como “inteligencia de amenazas” o “inteligencia de seguridad”.

Sin embargo, estos términos se asocian generalmente a la información sobre las amenazas a los sistemas informáticos tradicionales controlados por la organización. Esta concepción del campo es demasiado estrecha.

Los actores de las amenazas innovadoras buscan continuamente puntos débiles y desarrollan nuevas formas de penetrar o eludir las defensas informáticas tradicionales. Roban credenciales de terceros de confianza y las utilizan para introducirse en los sistemas corporativos. Recogen información personal de las plataformas de las redes sociales para producir campañas de phishing convincentes, y crean sitios web de typosquatting para hacerse pasar por marcas y estafar a los clientes. Planean ciberataques y aprovechan los eventos físicos contra instalaciones remotas en todo el mundo. Idean ataques que, sin previo aviso, son indetectables por las soluciones convencionales de seguridad informática.

Los expertos en seguridad y los grupos de TI con visión de futuro se han dado cuenta de que tienen que llevar la batalla a los actores de las amenazas descubriendo sus métodos e interrumpiendo sus actividades antes de que ataquen. Esta constatación les ha llevado a ampliar sus programas de inteligencia para incluir áreas como el riesgo de terceros (la exposición a través de vendedores, proveedores y socios comerciales), la protección de la marca (la capacidad de detectar y resolver los problemas de seguridad que amenazan la reputación de una organización), el riesgo geopolítico (las amenazas asociadas a las ubicaciones de los activos físicos y los eventos), la inteligencia sobre el fraude (soluciones que abordan el fraude en los pagos con tarjeta de crédito y otros fraudes relacionados con las transacciones en línea), la inteligencia sobre la identidad (inteligencia en tiempo real sobre las credenciales comprometidas), etc.

Ahora, podemos utilizar el término “inteligencia” para englobar todo lo que antes se denominaba “inteligencia sobre amenazas” o “inteligencia sobre seguridad”, así como las áreas más nuevas del campo. Por eso el libro que está leyendo ahora se titula *Manual de Inteligencia*.

Esperamos que este manual le permita desbaratar a los adversarios, reducir el riesgo de su organización y le sirva de hoja de ruta para ayudarle a construir una postura de seguridad eficiente y eficaz.

Resumen de los capítulos

Sección 1: ¿Qué es la inteligencia para los equipos de seguridad?

El capítulo 1, “Qué es la inteligencia para los equipos de seguridad”, describe el valor de la inteligencia y las características de los programas de inteligencia exitosos.

En el capítulo 2, “Tipos y fuentes”, se analizan las diferencias entre la inteligencia operativa y la estratégica, así como el papel de las fuentes de datos y la Dark Web.

El capítulo 3, “El ciclo de vida de la inteligencia”, examina las fases del ciclo de vida de la inteligencia y la relación entre las herramientas y los analistas humanos.

Sección 2: Aplicaciones de la inteligencia para los equipos de seguridad

Capítulo 4, “Inteligencia de SecOps Parte 1: Triage”, explora cómo la inteligencia proporciona el contexto para el triaje y permite a los equipos de operaciones de seguridad tomar decisiones mejores y más rápidas.

Capítulo 5, “Inteligencia de SecOps Parte 2: Respuesta”, analiza cómo la inteligencia minimiza la reactividad en la respuesta a incidentes y presenta cuatro casos prácticos.

El capítulo 6, “Inteligencia sobre vulnerabilidades”, examina cómo la inteligencia permite a los profesionales priorizar las vulnerabilidades en función del verdadero riesgo para la organización.

Capítulo 7, “Inteligencia sobre amenazas, parte 1: Comprender a los atacantes”, explica el valor de investigar las tácticas, técnicas y procedimientos (TTP) de los atacantes.

Capítulo 8, “Inteligencia sobre amenazas Parte 2: Análisis de riesgos”, analiza el valor de los modelos de riesgo y cómo la inteligencia proporciona datos concretos sobre las probabilidades de ataque y los costes.

El capítulo 9, “Inteligencia de terceros”, explora cómo se utiliza la inteligencia para evaluar a los socios de la cadena de suministro y reducir el riesgo de terceros.

El capítulo 10, “Inteligencia de marca”, repasa las diferentes formas de riesgos digitales para las marcas y cómo la inteligencia permite a los equipos de seguridad defender la reputación de su organización.

El capítulo 11, “Inteligencia geopolítica”, describe cómo la inteligencia proporciona una alerta avanzada de las amenazas a las instalaciones y los activos físicos en todo el mundo.

El capítulo 12, “Inteligencia contra el fraude”, ofrece una visión general de varias formas en que la inteligencia puede frustrar el fraude con tarjetas de pago y otros tipos de fraude relacionados con las transacciones en línea.

En el capítulo 13, “Inteligencia de identidad”, se describen los métodos para proteger las identidades de los usuarios, detectar el fraude de identidad de los clientes y evitar la apropiación de cuentas.

El capítulo 14, “Inteligencia de la superficie de ataque”, investiga cómo las organizaciones pueden descubrir y proteger dominios desconocidos y activos expuestos en Internet.

El capítulo 15, “Inteligencia para los líderes de seguridad”, examina cómo la inteligencia permite a los CISO, CIO y otros líderes obtener una visión holística del panorama de los ciberriesgos y tomar mejores decisiones empresariales.

El capítulo 16, “Inteligencia para priorizar las amenazas emergentes”, destaca tres amenazas emergentes para las que toda organización debe planificar y cómo priorizarlas.

Sección 3: Creación y ampliación de su programa de inteligencia

En el capítulo 17, "Marcos analíticos para la inteligencia", se explica cómo tres de los principales marcos de amenazas proporcionan estructuras útiles para pensar en los ataques.

Capítulo 18, “Fuentes y tipos de datos de inteligencia: Un marco de trabajo”, presenta un marco de fuentes y tipos de datos de inteligencia que pueden ayudar a las organizaciones a anticipar, detectar y responder a una amenaza.

El capítulo 19, “Su viaje de inteligencia”, ofrece sugerencias sobre cómo empezar de forma sencilla y ampliar un programa de inteligencia.

El capítulo 20, “Desarrollo de su equipo central de inteligencia”, describe cómo la creación de un equipo dedicado lleva la inteligencia a un nuevo nivel.

Glosario de iconos



SUGERENCIA
Los consejos ofrecen una serie de recomendaciones prácticas que puede aplicar en su propia organización.

NO OLVIDAR
Cuando vea este ícono, tome nota, ya que el contenido relacionado contiene información clave que querrá recordar.

PRECAUCIÓN
Proceda con precaución, porque puede resultar costoso para usted y su organización si no lo hace.

CHARLA TÉCNICA
El contenido asociado a este ícono es de naturaleza más técnica y está destinado a los profesionales de la informática y la seguridad.

EN LA WEB
¿Desea saber más? Siga la URL correspondiente para descubrir contenidos adicionales en línea.

Sección 1: ¿Qué es la inteligencia para los equipos de seguridad?

Capítulo 1

¿Qué es la inteligencia para los equipos de seguridad?

En este capítulo

- Entender por qué la inteligencia es importante para los equipos de seguridad
- Revisar las características de los programas de inteligencia exitosos
- Sepa quién se beneficia del uso de la inteligencia

Visibilidad de las amenazas antes de que ataquen

Las amenazas ciberneticas tienen muchas formas. Ciertamente, algunos de ellos son ciberdelincuentes que atacan su red en el cortafuegos. Sin embargo, también incluyen actores de amenazas que operan en la web abierta y oscura y que intentan obtener acceso no autorizado a través de sus empleados y sus socios comerciales. Algunos devastan su marca a través de las redes sociales y sitios web externos sin llegar a tocar su red. Las personas malintencionadas o simplemente descuidadas también pueden causar estragos en sus datos y en su reputación.

Cuando vea indicadores de estas amenazas en su red, probablemente sea demasiado tarde. Para prevenir los daños, es necesario avisar con antelación de las amenazas, acompañadas de hechos procesables para:

- Priorice a la aplicación de parches para sus vulnerabilidades más graves antes de que sean explotadas
- Detectar las sondas y los ataques lo antes posible y con gran confianza
- Comprender las tácticas, técnicas y procedimientos (TTP) de los probables atacantes y establecer defensas eficaces
- Identifique y corrija los puntos débiles de seguridad de sus socios comerciales
- Detecte las fugas de datos y las suplantaciones de su marca corporativa
- Realice inversiones inteligentes en seguridad para maximizar el rendimiento y minimizar el riesgo

Muchas organizaciones de TI han creado programas de inteligencia para obtener la advertencia previa y los datos procesables que necesitan para proteger sus empresas y sus marcas. La Figura 1-1 enumera las métricas que muestran la espectacular mejora de la seguridad y la eficiencia que proporciona un programa de inteligencia.



Figura 1-1: Un programa de inteligencia puede producir mejoras dramáticas en la seguridad, la eficiencia y la escala. (Fuente: IDC)

Inteligencia: Datos e información práctica

Cuando la gente habla de inteligencia, a veces se refiere a ciertos tipos de hechos y percepciones, y otras veces al proceso que los produce. Veamos el primer caso.

Más datos o información

Incluso los profesionales de la seguridad utilizan a veces las palabras “datos”, “información” e “inteligencia” indistintamente, pero las distinciones son importantes. La figura 1-2 pone de manifiesto estas diferencias.

Los datos consisten en hechos discretos y estadísticas recogidas como base para un análisis posterior.

La información se compone de múltiples puntos de datos que se combinan para responder a preguntas específicas.

La inteligencia es el resultado de un análisis de datos e información que descubre patrones y proporciona un contexto vital para la toma de decisiones.

Figura 1-2: Distinción entre datos, información e inteligencia.

Por supuesto, los detalles de los datos, la información y la inteligencia difieren entre los programas de inteligencia política, militar, económica, empresarial y de otros tipos. En el contexto de la inteligencia para los equipos de seguridad:

- Los datos suelen ser solo indicadores como direcciones IP, URL o hashes. Los datos no nos dicen mucho sin un análisis.
- La información responde a preguntas como: “¿Cuántas veces ha sido mencionada mi organización en las redes sociales este mes?” Aunque se trata de un resultado mucho más útil que los datos brutos, sigue sin informar directamente de una acción concreta.



La inteligencia es una visión objetiva basada en el análisis que correlaciona los datos y la información de diferentes fuentes para descubrir patrones y añadir ideas. Permite a las personas y a los sistemas tomar decisiones informadas y emprender acciones efectivas para prevenir infracciones, remediar vulnerabilidades, mejorar la postura de seguridad de la organización y reducir el riesgo.

La figura 1-3 muestra la relación entre datos, información e inteligencia.

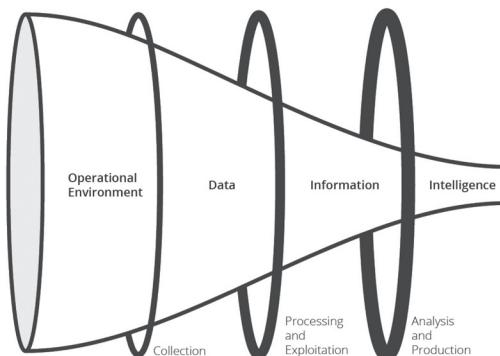


Figura 1-3: La relación entre datos, información e inteligencia.
(Fuente: U.S. Joint Chiefs of Staff, Joint Publication 2.0, Joint Intelligence)

Esta definición de “inteligencia” lleva implícita la idea de que cada instancia de inteligencia es *procesable* para un *público específico*. Es decir, la inteligencia debe hacer dos cosas:

1. Apunta a decisiones o acciones específicas
2. Estar adaptado para facilitar su uso a una persona, grupo o sistema específico que lo utilizará para tomar una decisión o realizar una acción

Las fuentes de datos que nunca se utilizan y los informes que nunca se leen no son inteligencia. Tampoco lo es la información, por muy precisa o perspicaz que sea, si se proporciona a alguien que no puede interpretarla correctamente o no está en condiciones de actuar en consecuencia.

Inteligencia: El proceso

La inteligencia también se refiere al proceso mediante el cual se recogen, analizan y difunden los datos y la información en toda la organización. En la jerga de la industria, esto se denomina “tradecraft”. Las etapas de este proceso se analizarán en el capítulo 3, donde se describe el ciclo de vida de la inteligencia. Sin embargo, es importante señalar desde el principio que los procesos de inteligencia exitosos tienen cuatro características.

1. Un proceso y un marco de colaboración

En muchas organizaciones, los esfuerzos de inteligencia están aislados. Por ejemplo, los equipos de operaciones de seguridad (SecOps), de prevención del fraude y de riesgos de terceros pueden tener sus propios analistas y herramientas para recopilar y analizar la inteligencia. Pueden responder a cadenas de información completamente independientes. Esto conduce al despilfarro, a la duplicación y a la incapacidad de compartir análisis e información. Los silos también impiden evaluar el riesgo en toda la organización y dirigir los recursos de seguridad hacia donde tendrán el mayor impacto. Los programas de inteligencia deben compartir un proceso y un marco comunes, permitir un amplio acceso a los conocimientos y a los flujos de trabajo operativos, fomentar una visión “global” del riesgo y dar cuenta de la asignación de recursos.

2. Visibilidad de 360 grados

Dado que las ciberamenazas pueden provenir de cualquier lugar, los programas de inteligencia necesitan visibilidad dentro y fuera de la empresa, incluyendo:

- Registros y eventos de seguridad de puntos finales y dispositivos de red
- Listas externas de proveedores de seguridad
- Herramientas comunitarias como la información sobre amenazas
- Foros web comunitarios en los que los investigadores de seguridad comparten y discuten la observación y los nuevos hallazgos

- Foros web abiertos y cerrados en los que los atacantes anuncian nuevos programas maliciosos y parches y discuten y demuestran métodos para explotar las vulnerabilidades
- Mercados de la Dark Web donde los actores de amenazas anuncian máquinas explotadas, bots y bases de datos de credenciales filtradas
- Cuentas de redes sociales en las que los actores de la amenaza intimidan y acosan a las víctimas a través de canales abiertos

En la actualidad, muchas organizaciones se centran en fuentes de datos sobre amenazas gratuitas o preempaquetadas, y solo ahora están tomando conciencia de la necesidad de escanear una mayor variedad y cantidad de fuentes de forma regular.

3. Amplia automatización e integración

Dado que hay tantos datos e información que capturar, correlacionar y procesar, un programa de inteligencia necesita un alto grado de automatización para reducir los esfuerzos manuales y producir rápidamente resultados significativos. Para añadir contexto a los hallazgos iniciales y difundir eficazmente la inteligencia, los programas de inteligencia exitosos también deben integrarse con muchos tipos de soluciones de seguridad, como los paneles de seguridad, las soluciones de gestión de eventos e información de seguridad (SIEM), los sistemas de gestión de vulnerabilidades, los productos para puntos finales y XDR, los cortafuegos y las herramientas de orquestación, automatización y respuesta de seguridad (SOAR).

4. Alineación con la organización y los casos prácticos de la seguridad

Las organizaciones suelen desperdiciar enormes recursos capturando y analizando información que no es relevante para ellas. Un programa de inteligencia exitoso necesita determinar y documentar sus necesidades de inteligencia para asegurar que las actividades de recolección y procesamiento se alineen con las prioridades reales de la organización. Alinear también significa adaptar el contenido y el formato de la inteligencia para que sea fácil de usar para las personas y los sistemas.

¿Quién se beneficia de la inteligencia?

A veces se imagina que la inteligencia es simplemente un servicio de investigación para los equipos de operaciones de seguridad y respuesta a incidentes, o el dominio de los investigadores de élite. En realidad, añade valor a todas las funciones de seguridad y a varios otros equipos de una organización.

La sección central de este manual examina los principales casos prácticos:

- Los equipos de operaciones de seguridad y de respuesta a incidentes** se ven habitualmente desbordados por las alertas. La inteligencia acelera la clasificación de las alertas, minimiza los falsos positivos, proporciona contexto para una mejor toma de decisiones y les permite responder más rápidamente.
- Los equipos de gestión de vulnerabilidades** a menudo luchan por diferenciar entre las vulnerabilidades relevantes y críticas y las que son menos críticas para la postura de defensa de su organización. La inteligencia ofrece un contexto y una puntuación de los riesgos que les permite reducir el tiempo de inactividad a la vez que parchan primero las vulnerabilidades que realmente importan.
- Los analistas de amenazas** deben comprender las motivaciones y las TTP de los actores de las amenazas y hacer un seguimiento de las tendencias de seguridad de los sectores, las tecnologías y las regiones. La inteligencia les proporciona conocimientos más profundos y amplios para generar ideas más valiosas.
- Los programas de riesgo de terceros** necesitan información actualizada sobre las posturas de seguridad de los vendedores, proveedores y otros terceros que acceden a los sistemas de la organización. La inteligencia les proporciona un flujo continuo de información objetiva y detallada sobre los socios comerciales que los cuestionarios estáticos de los proveedores y los métodos tradicionales de adquisición no pueden ofrecer.

- Los equipos de protección de la marca** necesitan una visibilidad continua de las menciones no autorizadas en la web y en las redes sociales, de las filtraciones de datos, de las suplantaciones de empleados, de los productos falsificados, de los sitios web de typosquatting, de los ataques de phishing, etc. Las herramientas de inteligencia vigilan la presencia de estas amenazas en Internet a gran escala y agilizan los procesos de retirada y corrección.
- Los equipos de riesgo geopolítico y de seguridad física** dependen de la advertencia anticipada de ataques, protestas y otras amenazas a los activos en lugares de todo el mundo. Los programas de inteligencia captan datos y “charlas” de múltiples fuentes y los filtran para ofrecer información precisa sobre lo que ocurre en las ciudades, países y regiones de interés.
- Los equipos de prevención del fraude** utilizan la información sobre los ataques en línea y las credenciales filtradas para detectar las campañas de fraude, reforzar la autenticación basada en el riesgo y mejorar las defensas contra el fraude en línea.
- Los equipos de gestión de identidades y accesos** pueden emplear la inteligencia de la Dark Web para identificar las credenciales comprometidas de los empleados y socios comerciales y evitar que la gente reutilice las contraseñas expuestas.
- Los responsables de seguridad** utilizan la información sobre las amenazas probables y su posible impacto en el negocio para evaluar los requisitos de seguridad, cuantificar los riesgos (idejalmente en términos monetarios), desarrollar estrategias de mitigación y priorizar y defender las inversiones en ciberseguridad ante los directores generales, los directores financieros y los miembros del consejo de administración.



Para una introducción concisa a la inteligencia y a seis áreas de soluciones críticas, lea el libro blanco de Recorded Future, “[Security Intelligence: Impulsar la seguridad desde el análisis a la acción.](#)”

Capítulo 2

Tipos y fuentes

En este capítulo

- Diferenciar entre inteligencia operativa y estratégica
 - Apreciar las funciones de las fuentes de datos, los canales privados y la Dark Web
-

Dos tipos de inteligencia

Para los equipos de seguridad, hay dos tipos de inteligencia: la **operativa** y la **estratégica**. Estos varían en sus fuentes, las audiencias a las que sirven y los formatos en los que aparecen.

El propósito de hacer esta distinción es reconocer que los distintos equipos de seguridad tienen diferentes objetivos y grados de conocimiento técnico. Como hemos dicho antes, la inteligencia debe ser procesable, pero como las responsabilidades de un equipo de gestión de vulnerabilidades difieren significativamente de las de un CISO, la “procesabilidad” tiene distintas implicaciones para cada uno, y la forma y el contenido de la inteligencia de la que se beneficiarán más variará.

Inteligencia operativa

La **inteligencia operativa** es el conocimiento de los ciberataques, eventos y campañas en curso. Proporciona información especializada que permite a las personas que la utilizan comprender la naturaleza, la intención y el momento en que se producen los ataques específicos.

La inteligencia operativa se denomina a veces **inteligencia técnica de seguridad** o **inteligencia técnica de amenazas**, porque suele incluir información técnica sobre los ataques, como qué vectores de ataque se están utilizando, qué vulnerabilidades se están explotando y qué dominios de mando y control están empleando los atacantes. Este tipo de información suele ser más útil para el personal directamente implicado en la defensa

de una organización, como los arquitectos de sistemas, los administradores y el personal de seguridad.

Las fuentes de datos sobre amenazas se utilizan a menudo para proporcionar contexto a la información interna, como los eventos de telemetría de la red interna o los eventos de detección y respuesta de puntos finales (EDR). Estos feeds suelen centrarse en un único tipo de indicador de amenaza, como los hashes de malware o los dominios sospechosos. Como comentamos más adelante, las fuentes de datos sobre amenazas proporcionan datos, pero esos datos no son inteligencia. Carece de información contextual, como el hecho de que una dirección IP externa sea un servidor de comando y control de ransomware.



SUGERENCIA La inteligencia operativa se utiliza habitualmente para orientar las mejoras de los controles de seguridad existentes, generar o mejorar nuevas reglas en un SIEM, mejorar los procesos de seguridad y los libros de jugadas, y acelerar la respuesta a los incidentes. Una solución de inteligencia operativa que se integre con los datos de su red es crucial porque responde a preguntas urgentes exclusivas de su organización, como: “¿Debería priorizarse la aplicación de parches a esta vulnerabilidad crítica, que está siendo explotada activamente por actores de amenazas contra mi sector?”

Inteligencia estratégica

La **inteligencia estratégica** proporciona una amplia visión del panorama de amenazas presente y futuro de una organización. Informa sobre las decisiones de recursos por parte de la dirección de seguridad y dentro de la arquitectura de seguridad, la seguridad de las aplicaciones y otros proyectos de desarrollo de seguridad. El contenido suele estar orientado al riesgo y se presenta a través de informes o reportes.

Este tipo de inteligencia requiere la interacción humana, ya que se necesita pensamiento analítico y creatividad para prever las tendencias futuras, por ejemplo, para evaluar y probar las TTP nuevas y emergentes de los adversarios contra los controles de seguridad existentes. Algunas partes de este proceso pueden estar automatizadas, pero se necesita una mente humana para completar el ejercicio.

Una buena inteligencia estratégica debe proporcionar información sobre los riesgos asociados a determinadas acciones, patrones generales en las tácticas y objetivos de los actores de las amenazas, acontecimientos y tendencias geopolíticas y temas similares.

Las fuentes de inteligencia estratégica más comunes son:

- Tendencias e informes de investigación de las empresas de seguridad
- Documentos políticos de Estados nacionales u organizaciones no gubernamentales
- Noticias de los medios de comunicación locales y nacionales, artículos de publicaciones sectoriales y temáticas, y aportaciones de expertos en la materia

Las organizaciones deben establecer los requisitos de inteligencia estratégica formulando preguntas concretas y específicas.

Para recopilar e interpretar la inteligencia estratégica se necesitan analistas con conocimientos ajenos a los típicos de la ciberseguridad, en particular, una gran comprensión de los conceptos políticos, sociopolíticos y empresariales.



Algunos aspectos de la producción de inteligencia estratégica se aceleran drásticamente gracias a la recopilación automatizada. La elaboración de una inteligencia estratégica eficaz requiere una profunda investigación de grandes volúmenes de datos, a menudo en varios idiomas. Estos retos hacen que la recopilación y el procesamiento inicial de los datos sean demasiado difíciles de realizar manualmente, incluso para los escasos analistas que poseen los conocimientos lingüísticos, la formación técnica y el oficio adecuados. Una solución de inteligencia que automatiza la recopilación y el procesamiento de datos reduce esta carga y permite a los analistas con distintos niveles de experiencia trabajar con mayor eficacia.

El papel de las fuentes de datos sobre amenazas

Ya hemos mencionado que los datos no son inteligencia, y que las fuentes de datos sobre amenazas a menudo abruman a los analistas, ya cargados con innumerables alertas y notificaciones diarias. Sin embargo, cuando se utilizan correctamente, las fuentes de datos sobre amenazas proporcionan una valiosa materia prima para la inteligencia.

Los flujos de datos sobre amenazas son flujos de datos en tiempo real que proporcionan información sobre posibles ciberamenazas y riesgos. Suelen ser listas de indicadores sencillos o artefactos centrados en un solo ámbito de interés, como dominios sospechosos, hashes, IP malas o código malicioso. Proporcionan una visión rápida y en tiempo real del panorama de las amenazas.



PRECAUCIÓN Muchos feeds están llenos de datos obsoletos, errores, redundancias y falsos positivos. Los datos carecen de contexto. Muchas organizaciones se dan cuenta de que han obtenido tantas fuentes que necesitan pasos adicionales para procesar la información, normalmente la curación manual en otra herramienta como una plataforma de inteligencia de amenazas (TIP), antes de poder introducir los datos en la producción en un SIEM. Este problema se agrava cuando los responsables de seguridad intentan ampliar la cobertura invirtiendo en un número asombroso de fuentes de datos, lo que acaba creando más ruido en su entorno.

Evaluación de las fuentes de datos sobre amenazas

Utilice estos criterios para evaluar las fuentes de datos sobre amenazas para su organización:

- **Fuentes de datos:** los feeds extraen sus datos de todo tipo de fuentes. Debe seleccionar las fuentes con cuidado y tomarse el tiempo necesario para evaluar la utilidad y el ruido de cada una antes de implantarla en su entorno.
- **Transparencia de las fuentes:** saber de dónde proceden los datos le permite evaluar su relevancia y utilidad. Algunas fuentes se agregan desde otros lugares, por lo que la duplicación puede ser un problema si se extrae de varias fuentes. Debe entender cómo las fuentes procesan y actualizan esta información y cómo purgan los datos antiguos.
- **Porcentaje de datos únicos:** algunos feeds de pago se limitan a agregar datos de otros feeds, mientras que otros no se preocupan de incluir en su lista de permitidos fuentes habituales de ruido, como las direcciones RFC 1918.
- **Periodicidad de los datos:** los datos deben recogerse con frecuencia y deben abarcar el periodo de tiempo pertinente para su organización. Además, debe abarcar un periodo de tiempo lo suficientemente largo como para apoyar la inteligencia estratégica sobre las tendencias a largo plazo. También es importante saber cuándo los datos se extinguen de la alimentación.
- **Resultados medibles:** poder hacer un seguimiento de la tasa de correlación -el porcentaje de alertas que se corresponden con su telemetría interna en una semana, un mes o un trimestre determinados- es fundamental para calcular los resultados medibles de una alimentación concreta.



SUGERENCIA En lugar de ver docenas de feeds por separado, algunas organizaciones utilizan una plataforma de inteligencia de amenazas (TIP) que los combina todos en un único feed antes de la ingestión en un SIEM. Aunque esto puede resolver algunas de las preocupaciones anteriores, como la eliminación de duplicados y falsos positivos, este proceso puede requerir muchos recursos en comparación con el suministro de datos de calidad directamente a un SIEM.

El papel de los canales privados y la Dark Web

Las fuentes de datos sobre amenazas y la información disponible públicamente no son las únicas fuentes externas de datos de inteligencia. La inteligencia operativa y estratégica vital sobre ataques específicos, las TTP de los atacantes, los objetivos políticos de los hacktivistas y los actores estatales, y otros temas clave, pueden ser recogidos mediante la infiltración o la irrupción en los canales privados de comunicación utilizados por los grupos de amenaza. Entre ellas se encuentran las aplicaciones de mensajería, los foros exclusivos de la Dark Web y otras fuentes.

Sin embargo, hay obstáculos para reunir este tipo de información:

- Acceso:** los grupos de amenazas pueden comunicarse a través de canales privados y encriptados, o requerir una validación previa o una invitación de un administrador.
- Idioma:** la actividad en muchos foros se lleva a cabo en muchos idiomas, y el argot y la jerga especializada se utilizan regularmente
- Ruido:** los altos volúmenes de conversación dificultan o imposibilitan la recopilación manual de buena información de fuentes como las salas de chat y las redes sociales.
- Ofuscación:** para evitar la detección, muchos grupos de amenazas emplean tácticas de ofuscación como el uso de nombres en clave.
- Política interna:** los responsables legales y de seguridad de una organización pueden dudar en comunicarse abiertamente con los actores criminales, especialmente cuando esto requiere el uso de activos corporativos para pagar el acceso a sus foros.

Superar estas barreras requiere una gran inversión en herramientas y conocimientos para supervisar los canales privados, o un proveedor de servicios de inteligencia que ya haya realizado esa inversión.



SUGERENCIA Busque soluciones y servicios de inteligencia que empleen algoritmos y procesos analíticos para la recopilación automática de datos a gran escala. Una solución que utilice el procesamiento del lenguaje natural, por ejemplo, podrá recopilar información de fuentes en idiomas extranjeros sin necesidad de conocimientos humanos para descifrarla.

Capítulo 3

El ciclo de vida de la inteligencia

En este capítulo

- Examinar las fases del ciclo de vida de la inteligencia
 - Revisar las fuentes de información para los equipos de seguridad
 - Explorar las funciones de las herramientas de inteligencia y de los analistas humanos
-

Las seis fases del ciclo de vida de la inteligencia

La inteligencia se basa en técnicas analíticas perfeccionadas a lo largo de varias décadas por los organismos gubernamentales y militares. Hay seis fases distintas que conforman lo que se llama el “ciclo de la inteligencia”:

1. Dirección
2. Colección
3. Procesamiento
4. Análisis
5. Difusión
6. Comentarios

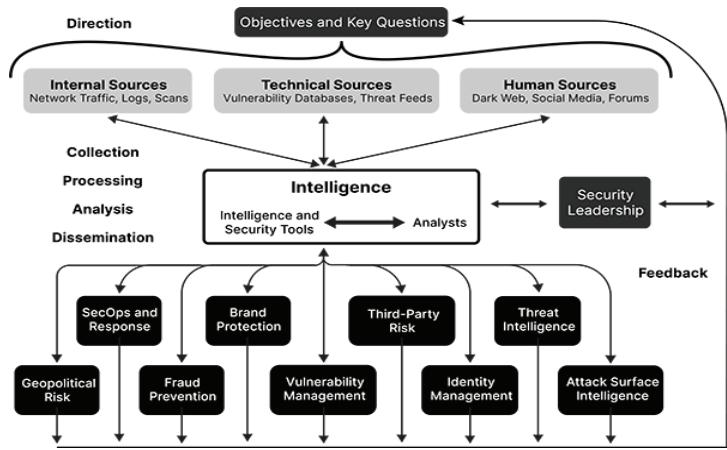


Figura 3-1: La inteligencia y las seis fases del ciclo de la inteligencia.

Dirección

La fase de dirección del ciclo de vida de la inteligencia es cuando se establecen los objetivos de su programa de inteligencia. Esto implica comprender y articular:

- Los activos de información y los procesos empresariales que hay que proteger
- Los impactos potenciales de la pérdida de esos activos o de la interrupción de esos procesos
- Los tipos de inteligencia que su organización necesita para proteger los activos y responder a las amenazas
- Las prioridades sobre lo que hay que proteger

Una vez determinadas las necesidades de inteligencia de alto nivel, una organización es capaz de formular preguntas que canalizan la necesidad de información en requisitos discretos. Por ejemplo, si el objetivo es conocer a los posibles adversarios, una pregunta lógica sería: “¿Qué actores de amenazas en foros clandestinos están solicitando activamente datos relativos a nuestra organización?”

Colección

La recopilación es el proceso de reunir información para responder a las necesidades de inteligencia más importantes. Puede producirse de forma orgánica a través de diversos medios, entre ellos:

- Obtención de metadatos y registros de redes internas y dispositivos de seguridad
- Suscripción a fuentes de datos sobre amenazas de organizaciones del sector y proveedores de ciberseguridad
- Conversaciones y entrevistas específicas con fuentes informadas
- Exploración de sitios web de noticias y blogs
- Exploración de las plataformas de medios sociales
- Raspado y recolección de sitios web y foros
- Infiltración de fuentes cerradas, como los foros de la Dark Web

Los datos recogidos suelen ser una combinación de información acabada, como informes de inteligencia de expertos y proveedores de seguridad, y datos brutos, como firmas de malware o credenciales filtradas en un sitio de pasta.

Fuentes de información

Fuentes técnicas: las fuentes de datos técnicos pueden estar disponibles públicamente, como URLscan.io, y pueden ser ingeridas a través de una API. Las fuentes técnicas suelen proporcionar datos estructurados que pueden integrarse con las tecnologías de seguridad existentes, pero pueden contener una elevada proporción de falsos positivos y resultados obsoletos.

Medios de comunicación (por ejemplo, sitios web de seguridad, investigación de proveedores): estas fuentes suelen proporcionar información útil sobre las amenazas emergentes, pero son difíciles de conectar con los indicadores técnicos para medir el riesgo.

Las redes sociales: los canales sociales ofrecen enormes cantidades de datos valiosos, pero tienen un precio. La mayoría de los datos de las redes sociales no son relevantes para la seguridad. Los falsos positivos y la información errónea proliferan, por lo que se requiere una enorme cantidad de referencias cruzadas con otras fuentes para determinar qué datos son utilizables.

Foros de actores de amenazas: diseñados específicamente para albergar debates sobre las herramientas y técnicas de los adversarios, estos foros ofrecen algunos de los conocimientos más prácticos disponibles en cualquier lugar. Sin embargo, una vez más, el análisis y las referencias cruzadas son esenciales para determinar lo que es realmente valioso.

NO OLVIDAR

Se necesitan múltiples fuentes de inteligencia para formar una imagen completa de las amenazas potenciales y reales. Como se muestra en la Figura 3-1, estos incluyen:

- Fuentes internas** como registros de cortafuegos y routers, herramientas de captura de paquetes de red y escáneres de vulnerabilidades
- Fuentes técnicas** como repositorios de malware y escáneres C2 conocidos
- Fuentes humanas**, incluyendo medios de comunicación tradicionales y sociales, foros y blogs de ciberseguridad y foros de la Dark Web

La omisión de cualquiera de ellos puede ralentizar las investigaciones y provocar lagunas en la reparación.



iAutomatizar! Los analistas deben dedicar el menor tiempo posible a la recopilación de datos y el mayor tiempo posible a la evaluación y comunicación de la información sobre las amenazas.

Procesamiento

El procesamiento es la transformación de la información recogida en un formato utilizable por la organización. Casi todos los datos brutos recogidos necesitan ser procesados de alguna manera, ya sea por humanos o por máquinas.

Los diferentes métodos de recogida suelen requerir diferentes medios de tratamiento. Es posible que haya que correlacionar y clasificar los informes humanos, coordinarlos y comprobarlos. Un ejemplo podría ser extraer las direcciones IP del informe de un proveedor de seguridad y añadirlas a un archivo CSV para importarlas a un SIEM. En un ámbito más técnico, el procesamiento puede consistir en extraer indicadores de un correo electrónico, enriquecerlos con otra información y, a continuación, comunicarse con las herramientas de gestión de tickets y de protección de puntos finales para la corrección del sistema.



iAutomaticice más! Las herramientas adecuadas le permitirán automatizar la mayoría de los flujos de trabajo de tramitación y los procesos de cobro. Por ejemplo, un evento de seguridad puede marcar un indicador de compromiso (IOC) sospechoso y, a continuación, realizar una secuencia de comprobaciones para contextualizar el IOC. Esto ahorra al analista un valioso tiempo que, de otro modo, tendría que dedicar a realizar esas comprobaciones manualmente.



Para saber más sobre cómo la automatización mejora la inteligencia, lea el breve libro electrónico de Recorded Future, “[“Beyond SOAR: 5 formas de automatizar la seguridad con inteligencia.”](#)

Análisis

El análisis es el proceso de convertir la información en inteligencia para fundamentar las decisiones. Dependiendo de las circunstancias, estas decisiones pueden implicar si se investiga una amenaza potencial, qué acciones tomar inmediatamente para bloquear un ataque, cómo reforzar los controles de seguridad o cuánto se justifica invertir en recursos de seguridad adicionales. El análisis lo realiza generalmente un humano o un algoritmo muy sofisticado.



Los analistas deben tener claro quién va a utilizar su inteligencia y qué decisiones toman esas personas. La información que proporcionan debe ser percibida como práctica, no como académica. La mayor parte de este libro está dedicada a ofrecer una imagen clara de cómo la inteligencia mejora la toma de decisiones y las acciones en diferentes ámbitos de la seguridad.

La forma en que se presenta la información es especialmente importante. Es inútil y un despilfarro recoger y procesar la información solo para entregarla en una forma que no puede ser entendida y utilizada por el responsable de la toma de decisiones.

Por ejemplo, si quiere comunicarse con líderes no técnicos, su informe debería:

- Ser conciso (una nota de una página o un puñado de diapositivas)
- Evitar términos y jerga confusos y demasiado técnicos
- Articular los problemas en términos empresariales (como los costes directos e indirectos y el impacto en la reputación)
- Incluir un curso de acción recomendado

Es posible que algunos datos deban entregarse en varios formatos para diferentes audiencias, como una transmisión de vídeo en directo y un informe escrito. No toda la información necesita ser digerida a través de un informe formal. Los equipos

de inteligencia exitosos proporcionan informes técnicos continuos a otros equipos de seguridad con contexto externo en torno a los COI, el malware, los actores de amenazas, las vulnerabilidades y las tendencias de las amenazas.

Difusión

La difusión consiste en hacer llegar el resultado final de la inteligencia a los lugares a los que debe llegar.

Como se ilustra en la Figura 3-1, la mayoría de las organizaciones de seguridad cuentan con varios equipos y líderes de seguridad que se benefician de la inteligencia. Para cada uno de estos públicos, hay que preguntar:

- ¿Qué información necesitan y cuál es la mejor manera de que la información externa apoye sus actividades?
- ¿Cómo debe seleccionarse y organizarse la información para que sea fácilmente comprensible y procesable para ese público?
- ¿Con qué frecuencia debemos proporcionar actualizaciones y otra información?
- ¿A través de qué medios (correos electrónicos, boletines, foros web, documentos, diapositivas, presentaciones orales) debe difundirse la información?
- ¿Cómo debemos hacer el seguimiento si tienen preguntas?

Comentarios

Es necesario realizar aportaciones periódicas para comprender las necesidades de cada grupo y realizar ajustes a medida que cambian sus necesidades y prioridades. Esta información se recoge en la fase de retroalimentación. Es de vital importancia comprender las prioridades generales de la inteligencia y los requisitos de sus “clientes”, es decir, los equipos de seguridad que consumen la inteligencia. Sus necesidades guían todas las fases del ciclo vital y te lo dicen:

- Qué tipos de datos recoger
- Cómo procesar y enriquecer los datos para convertirlos en información útil

- Cómo analizar la información y presentarla como inteligencia procesable
- A quién hay que difundir cada tipo de información, con qué rapidez hay que difundirla y con qué rapidez hay que responder a las preguntas



Para cada equipo “cliente”, establezca canales tanto para la retroalimentación rápida e informal (como una dirección de correo electrónico, un foro interno o una herramienta de colaboración en equipo), como para un proceso formal y estructurado (como una encuesta en línea o una reunión presencial trimestral). El canal informal le permite reaccionar y ajustarse de inmediato, mientras que el proceso estructurado le garantiza que obtendrá las aportaciones de todos y podrá hacer un seguimiento de su progreso a lo largo del tiempo.

Herramientas y personas

Las herramientas son esenciales para automatizar los pasos de recopilación, procesamiento y difusión en el ciclo de vida de la inteligencia, y para apoyar y acelerar el análisis. Sin las herramientas adecuadas, los analistas dedicarán todo su tiempo a los aspectos mecánicos de estas tareas y nunca tendrán tiempo para el análisis.

La mayoría de los grupos de inteligencia maduros aprovechan dos tipos de herramientas:

- Una solución de inteligencia diseñada para recoger, procesar y analizar todo tipo de datos sobre amenazas procedentes de fuentes internas, técnicas y humanas
- Las herramientas de seguridad existentes, como los SIEM y los análisis de seguridad, que recogen y correlacionan los eventos de seguridad y los datos de registro

Los analistas humanos son igual de importantes, si no más. No se puede confiar en las herramientas para entrevistar a los expertos en seguridad y sondear los foros cerrados de la Dark Web. Además, se necesitan personas que analicen y sinteticen la información para los equipos de seguridad y los directivos que la consumirán.

Los analistas no necesitan pertenecer a un departamento de inteligencia central y de élite. Es necesario que alguien adopte una visión de la función de inteligencia a nivel de toda la organización, que tome decisiones sobre los recursos y las prioridades, y que haga un seguimiento de los progresos, pero el éxito puede lograrse en una variedad de estructuras organizativas. Podría tener un grupo central con analistas de inteligencia dedicados, o un pequeño grupo dentro de la organización de operaciones de seguridad y respuesta a incidentes. Alternativamente, los miembros de los diferentes grupos de seguridad pueden ser responsables de analizar la inteligencia para sus colegas directos.

En el capítulo 19, analizamos cómo la estructura organizativa suele evolucionar a medida que la función de inteligencia madura, y el capítulo 20 ofrece consejos sobre cómo organizar un equipo central de inteligencia.

Sección 2: Aplicaciones de la inteligencia para los equipos de seguridad

Capítulo 4

Inteligencia de SecOps

Parte 1 - Triaje

En este capítulo

- Vea cómo la “fatiga de las alertas” corre el riesgo de deshacer el buen trabajo de los equipos de SecOps
- Comprender el valor del contexto para mejorar el triaje
- Aprenda cómo la inteligencia reduce la pérdida de tiempo y mejora las decisiones de triaje

El triaje es un trabajo crítico pero agotador para los equipos de operaciones de seguridad. Se encuentran rehenes de los enormes volúmenes de alertas generados por las redes que supervisan. Según el informe Ponemon “Cost of Malware Containment”, los equipos de seguridad pueden esperar registrar casi 17 000 alertas de malware en una semana típica. Esto supone más de 100 alertas por hora para un equipo que trabaja las 24 horas del día. Y esas son solo las alertas de incidentes de malware. Para poner estas cifras en perspectiva, todas estas alertas pueden obligar a los equipos de seguridad a destinar más de 21 000 horas-hombre cada año persiguiendo falsos positivos. Son 2625 turnos estándar de ocho horas necesarios solo para distinguir las alertas malas de las buenas.

Examinemos cómo la inteligencia mitiga esta sobrecarga filtrando las falsas alarmas, acelerando el análisis de las alertas y proporcionando contexto para tomar mejores decisiones de triaje.

Responsabilidades del equipo de SecOps

Sobre el papel, las responsabilidades del equipo de SecOps parecen sencillas:

- Vigilar las posibles amenazas
- Detectar actividades sospechosas en la red
- Contener las amenazas activas
- Remediar las amenazas utilizando la tecnología disponible

Cuando se detecta un evento sospechoso, el equipo de SecOps lo investiga y luego trabaja con otros equipos de seguridad para reducir el impacto y la gravedad del ataque. Piense en las funciones y responsabilidades de las SecOps como las de los equipos de servicios de emergencia que responden a las llamadas al 911, como se muestra en la Figura 4-1.

Stage	Role	Responsibilities
Triage	Operator (911 Center) Security Analyst (SOC)	Determine the relevance and urgency of each incoming alert. Decide if the alert is legitimate and should be escalated.
First Response	First Responder (911) Incident Responder (SOC)	Determine the scope of the incident. Identify affected and vulnerable systems. Recommend actions to contain the effects.
Investigation	Detective (911) Threat Hunter (SOC)	Determine root causes and weaknesses in defenses. Recommend actions to prevent recurrences.

Figura 4-1: Las funciones y responsabilidades de los equipos de servicios de emergencia y los equipos de SecOps son similares.

El abrumador volumen de alertas

En los últimos años, la mayoría de las organizaciones han incorporado a sus redes nuevos tipos de tecnologías de detección de amenazas. Cada una de estas herramientas hace sonar una alarma cuando detecta un comportamiento anómalo o sospechoso. En combinación, estas herramientas crean una cacofonía de alertas de seguridad. Los analistas de SecOps son simplemente incapaces de revisar, priorizar e investigar todas estas alertas por sí mismos. Con demasiada frecuencia ignoran las alertas, persiguen falsos positivos y cometan errores debido a la fatiga de las alertas.

La investigación confirma la magnitud de este reto. En su informe “[2020 State of the SOC](#)”, el proveedor de SIEM Exabeam reveló que los centros de operaciones de seguridad (SOC) carecen de personal suficiente según el 39 % de los profesionales que trabajan en ellos, y de ellos, el 50 % piensa que necesitan al menos seis empleados más. Además, el “[2020 CISO Benchmark Study](#)” de Cisco descubrió que las organizaciones solo pueden investigar el 48 % de las alertas de seguridad que reciben en un día determinado, y de esas alertas investigadas, solo el 26 % se consideran legítimas (Figura 4-2).

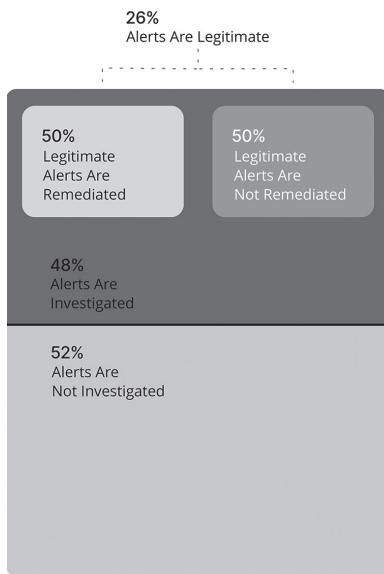


Figura 4-2: Muchas alertas de amenazas no se investigan ni se remedian. (Fuente: Cisco)

El contexto es el rey

La inteligencia de SecOps se utiliza específicamente para apoyar el triaje enriqueciendo las alertas internas con la información externa y el contexto necesario para tomar decisiones basadas en el riesgo. El contexto es fundamental para el triaje rápido, y también es muy importante para delimitar y contener los incidentes.

El triaje requiere mucho contexto

Una gran parte del día de un analista de SecOps se dedica a responder a las alertas generadas por los sistemas de seguridad internos, como las tecnologías SIEM o de detección y respuesta de puntos finales (EDR). Las fuentes de datos internos son vitales para identificar actividades de red potencialmente maliciosas o una violación de datos.

Por desgracia, estos datos suelen ser difíciles de interpretar de forma aislada. Determinar si una alerta es relevante y urgente requiere recopilar información relacionada (contexto) de una amplia variedad de registros del sistema interno, dispositivos de red y herramientas de seguridad (Figura 4-3), y de bases de datos de amenazas externas. Buscar en todas estas fuentes de datos sobre amenazas el contexto que rodea a cada alerta requiere mucho tiempo.

Key Aspects	Security Monitoring Requirement
 Business Traffic Crossing a Boundary	Traffic exchanges are authorized and conform to security policy. Transport of malicious content and other forms of attack by manipulation of business traffic are detected and alerted.
 Activity at a Boundary	Detect suspect activity indicative of the actions of an attacker attempting to breach the system boundary, or other deviation from normal business behavior.
 Internal Workstation, Server, or Device	Detect changes to device status and configuration from accidental or deliberate acts by a user, or by malware.
 Internal Network Activity	Detect suspicious activity that may indicate attacks by internal users, or external attackers who have penetrated the internal network.
 Network Connections	Prevent unauthorized connections to the network made by remote access, VPN, wireless, or any other transient means of network connection.
 Session Activity By User and Work Station	Detect unauthorized activity and access that is suspicious or violates security policy requirements.
 Alerting on Events	Be able to respond to security incidents in a time frame appropriate to the perceived criticality of the incident.
 Accurate Time in Logs	Be able to correlate event data collected from disparate sources.
 Data Backup Status	Be able to recover from an event that compromises the integrity or availability of information assets.

Figura 4-3: Aspectos clave de la vigilancia de la seguridad y fuentes internas de contexto. (Fuente: UK NCSC)

Caso práctico: Correlación y enriquecimiento de las alertas

Un analista que intente clasificar una alerta inicial sin tener acceso a suficiente contexto es como una persona que intenta entender una noticia tras leer solo el titular. Incluso cuando el analista tiene acceso a información externa en forma de fuentes de amenazas (Figura 4-4), esa información es muy difícil de asimilar y correlacionar con otros datos relacionados con la alerta.

2021-09-13 02:46:26	E	<u>63.153.27.53</u>	offline
2021-09-12 21:41:44	E	<u>75.130.100.165</u>	online
2021-09-12 18:54:45	E	<u>71.172.252.50</u>	online
2021-09-12 15:51:16	E	<u>118.189.9.243</u>	offline
2021-09-12 14:11:41	E	<u>31.167.248.50</u>	offline
2021-09-12 08:32:01	E	<u>78.134.74.39</u>	online
2021-09-12 05:03:02	E	<u>42.114.73.81</u>	offline
2021-09-12 04:56:53	E	<u>216.59.200.206</u>	offline
2021-09-11 11:35:10	E	<u>183.82.97.20</u>	offline
2021-09-11 08:59:59	E	<u>128.2.98.139</u>	offline
2021-09-11 08:12:12	E	<u>47.38.231.174</u>	offline
2021-09-11 08:01:28	E	<u>217.36.122.251</u>	offline
2021-09-11 07:45:59	E	<u>107.184.160.132</u>	offline
2021-09-11 06:45:54	E	<u>71.75.206.192</u>	online
2021-09-11 06:43:49	E	<u>123.231.21.141</u>	offline
2021-09-11 05:54:51	E	<u>189.222.75.8</u>	offline
2021-09-11 05:54:51	E	<u>189.211.177.113</u>	offline
2021-09-11 05:54:51	E	<u>92.27.115.15</u>	offline
2021-09-11 05:54:51	E	<u>207.107.101.210</u>	offline
2021-09-11 05:51:45	E	<u>195.97.22.6</u>	online

Figura 4-4: Es muy difícil encontrar información relevante en un feed de amenazas en bruto y correlacionarla con otros datos relacionados con una alerta.

La inteligencia de SecOps transforma completamente esta situación. Tiene la capacidad de sacar a la superficie automáticamente información sobre amenazas en tiempo real y correlacionarla con las alertas, como se ilustra en la Figura 4-5. El contexto proporcionado podría incluir las primeras y más recientes referencias a un programa malicioso o a una dirección IP sospechosa, el número de avistamientos, las asociaciones con tipos de ataques y actores de amenazas específicos, y las descripciones del comportamiento del programa malicioso o los usos de la dirección IP (por ejemplo, como parte de una red de bots).

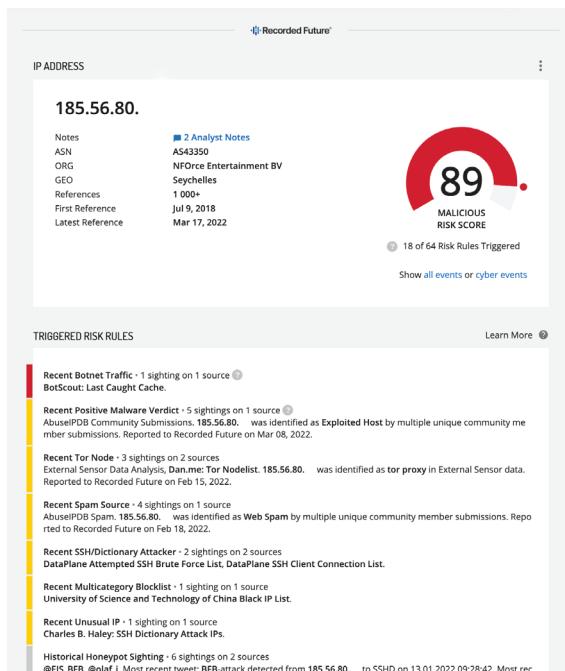


Figura 4-5: Una solución de inteligencia de SecOps enriquece automáticamente las alertas con el contexto, como los avistamientos anteriores, las asociaciones con los tipos de ataque y los actores de la amenaza, y las puntuaciones de riesgo. (Fuente: Recorded Future)

Este enriquecimiento permite a los analistas de SecOps identificar rápidamente las amenazas más significativas y tomar acciones inmediatas e informadas para resolverlas.

El enriquecimiento permite incluso a los analistas de SecOps relativamente noveles “dar un golpe por encima de su peso” haciendo conexiones que, de otro modo, habrían requerido más experiencia de la que tienen. También proporciona una forma de formación acelerada en el puesto de trabajo al proporcionar información en profundidad sobre las últimas amenazas.

Como ejemplo de este perfeccionamiento para analistas relativamente jóvenes, supongamos que se genera una alerta cuando una dirección IP externa desconocida intenta conectarse a través del puerto TCP 445. Los analistas experimentados podrían saber que un exploit reciente para SMB ha sido utilizado por el ransomware para propagarse e identificarían la IP como



probablemente comprometida basándose en el propietario, la ubicación y los datos de código abierto. Un analista inexperto podría no ser capaz de realizar estas conexiones sin ayuda, pero la inteligencia contextualizada de SecOps le mostraría al analista que otros dispositivos de la red utilizan SMB en el puerto 445 para transferir archivos y datos entre servidores. También informaría al analista de que el nuevo exploit y el ransomware se han asociado a esa dirección IP.

Acortar el “tiempo hasta el no”

Por muy importante que sea para los analistas de SecOps recopilar información sobre amenazas reales de forma más rápida y precisa, se puede argumentar que la capacidad de descartar rápidamente las falsas alarmas es aún más importante.

La inteligencia de SecOps proporciona al personal el contexto necesario para clasificar las alertas rápidamente y con mucho menos esfuerzo. Evita que los analistas pierdan horas persiguiendo alertas basadas en:

- Acciones que probablemente sean inocuas y no maliciosas
- Ataques que no son relevantes para su organización
- Ataques para los que ya existen defensas y controles

Algunas soluciones de inteligencia SecOps realizan automáticamente gran parte de este filtrado personalizando las fuentes de riesgo para ignorar o rebajar las alertas que no coinciden con los criterios específicos de la organización y el sector.

Los equipos de seguridad ven reducido el tiempo de investigación en un 40 %.

Un estudio de Forrester Consulting Total Economic Impact™, encargado por Recorded Future, ha descubierto que los usuarios de la inteligencia de Recorded Future obtienen beneficios que incluyen una mayor eficiencia de las operaciones de seguridad, una mayor capacidad para evitar las

brechas de seguridad y una mejor defensa del valor de su marca. Para leer el informe completo del estudio, vaya a <https://go.recordedfuture.com/forrester-tei-study>.

Capítulo 5

Inteligencia SecOps

Parte 2 - Respuesta

En este capítulo

- Aprenda cómo la inteligencia minimiza la reactividad
- Repasar las características de las soluciones de inteligencia de SecOps que las hacen eficaces para afrontar los retos de la respuesta a incidentes
- Explorar los casos de uso de la inteligencia por parte de los equipos de respuesta a incidentes

Una vez identificados los ataques reales, se ponen en marcha los procesos de respuesta a incidentes. Pero ambos flujos de trabajo se han vuelto más estresantes para los equipos de seguridad. Entre las razones:

- El volumen de incidentes cibernéticos ha aumentado constantemente durante dos décadas.
- Las amenazas se han vuelto más complejas y difíciles de analizar; mantenerse al tanto del cambiante panorama de las amenazas se ha convertido en una tarea importante en sí misma.
- Al responder a los incidentes de seguridad, los analistas se ven obligados a dedicar un tiempo considerable a la comprobación y difusión manual de datos procedentes de fuentes dispares.
- La contención de los ataques y la erradicación de las vulnerabilidades son cada vez más difíciles.

Como resultado, los equipos de respuesta a incidentes operan rutinariamente bajo enormes presiones de tiempo y a menudo son incapaces de contener los incidentes cibernéticos con prontitud.

Desafíos continuos

Aunque es difícil precisar el número de incidentes experimentados por una organización típica, no cabe duda de que el volumen de ciberataques está creciendo. Aunque parte de esta creciente presión se ve mitigada por las tecnologías preventivas, los equipos de respuesta a incidentes se ven sometidos a una enorme presión adicional debido a los siguientes factores.

Un déficit de competencias

La respuesta a incidentes no es una función de seguridad de nivel básico. Abarca una amplia gama de competencias, como el análisis estático y dinámico del malware, la ingeniería inversa y la ciencia forense digital. Se necesitan analistas con experiencia en el sector y capaces de realizar operaciones complejas bajo presión.

El tan publicitado déficit de competencias en materia de ciberseguridad no ha dejado de aumentar en la última década. Cyber Seek calcula que solo en Estados Unidos hay casi 600 000 puestos de trabajo en ciberseguridad. Según el informe de ISSA-ESG “[La vida y los tiempos de los profesionales de la ciberseguridad 2021](#)”, el 57 % de las organizaciones se ven afectadas negativamente por la escasez de profesionales de la ciberseguridad.

Aumento de los tiempos de respuesta

Cuando hay muy poco personal cualificado y demasiadas alertas, solo hay un resultado: El tiempo para resolver auténticos incidentes de seguridad aumentará. Según el informe “[2021 Coste de un informe sobre la filtración de datos](#)” de Ponemon Institute e IBM Security, el tiempo para detectar y contener una violación de datos aumentó de 257 días en 2017 a 287 días en 2021.

Por supuesto, los ciberdelincuentes no tienen esas limitaciones. Una vez que consiguen entrar en una red objetivo, el tiempo para comprometerla suele medirse en minutos. En el próximo capítulo hablaremos de ello.

Un enfoque fragmentario

La mayoría de las organizaciones tienen grupos de seguridad que crecen orgánicamente en paralelo al aumento de los riesgos cibernéticos. En consecuencia, muchos solo añaden tecnologías y procesos de seguridad para satisfacer necesidades específicas, y lo hacen sin un diseño estratégico.

Aunque este enfoque ad hoc es perfectamente normal, obliga a los equipos de respuesta a incidentes a dedicar mucho tiempo a la agregación de datos y contexto a partir de una variedad de tecnologías de seguridad (por ejemplo, SIEM, EDR y registros de cortafuegos) y fuentes de amenazas. Este esfuerzo alarga significativamente los tiempos de respuesta y aumenta la probabilidad de errores.

El problema de la reactividad

Una vez que se marca una alerta, hay que clasificarla, remediarla y hacer un seguimiento lo más rápido posible para minimizar el riesgo cibernético. Considere un proceso típico de respuesta a incidentes:

1. **Detección de incidentes** : recibir una alerta de un producto SIEM, EDR o similar.
2. **Descubrir**: determinar lo que ha sucedido y cómo responder.
3. **Triaje y contención** : tomar medidas inmediatas para mitigar la amenaza y minimizar los daños.
4. **Remediación** : reparar los daños y eliminar las infecciones.
5. **Empuje hacia el BAU** : pasar el incidente a los equipos de “negocios como de costumbre” para las acciones finales.

Obsérvese la naturaleza reactiva de este proceso. Para la mayoría de las organizaciones, casi todo el trabajo necesario para remediar un incidente se acumula, lo que significa que no puede completarse hasta después de que se marque una alerta. Aunque esto es inevitable hasta cierto punto, dista mucho de ser lo ideal cuando los equipos de respuesta a incidentes ya tienen dificultades para resolverlos con suficiente rapidez.

Minimizar la reactividad en la respuesta a incidentes

Para reducir los tiempos de respuesta, los equipos de respuesta a incidentes deben ser menos reactivos. Dos áreas en las que la preparación avanzada es especialmente impactante son la identificación de las amenazas probables y la priorización.

Identificación de probables amenazas

Cuando un equipo de respuesta a incidentes identifica de antemano las amenazas más frecuentes, le permite desarrollar procesos sólidos y coherentes para hacerles frente. Esta preparación reduce drásticamente el tiempo que el equipo necesita para contener los incidentes individuales y evitar errores, y libera a los analistas para hacer frente a las amenazas nuevas e inesperadas cuando surgen.

Priorización

No todas las amenazas son iguales. Cuando los equipos de respuesta a incidentes comprenden qué vectores de amenaza suponen el mayor nivel de riesgo para su organización, pueden asignar su tiempo y recursos en consecuencia.

Reforzar la respuesta a los incidentes con inteligencia

De lo dicho hasta ahora debería quedar claro que las tecnologías de seguridad *por sí solas* no pueden hacer lo suficiente para reducir la presión sobre los analistas humanos.

La inteligencia de SecOps reduce las demandas de los equipos de respuesta a incidentes y aborda muchos de los problemas que hemos estado revisando:

- Identificar y descartar automáticamente las alertas de falsos positivos
- Enriquecer las alertas con el contexto en tiempo real de la open web, la dark web y las fuentes técnicas
- Reunir y comparar información procedente de fuentes de datos internas y externas para identificar auténticas amenazas
- Calificación y priorización de las amenazas según las necesidades específicas de la organización y la infraestructura

En otras palabras, la inteligencia, especialmente la de SecOps, proporciona a los equipos de respuesta a incidentes exactamente la información procesable que necesitan para tomar decisiones más rápidas y mejores, a la vez que frena la marea de alertas irrelevantes y poco fiables que suelen dificultar tanto su trabajo.

Inteligencia SecOps en acción

Veamos tres casos de uso y uno de abuso que muestran cómo la inteligencia de SecOps afecta a los equipos de respuesta a incidentes en el mundo real.

Caso práctico: Preparar los procesos con antelación

Como se ha señalado anteriormente, los procesos típicos de respuesta a incidentes son muy reactivos, y la mayor parte de la actividad tiene lugar solo después de que se produzca un incidente. Esto prolonga el tiempo necesario para alcanzar y remediar los incidentes.

La inteligencia de SecOps permite a los equipos de respuesta a incidentes prepararse para las amenazas proporcionando:

- Una imagen completa y actualizada del panorama de las amenazas
- Información sobre las TTP populares de los actores de amenazas
- Tendencias de ataque específicas del sector y de la región

La inteligencia de SecOps permite a los equipos de respuesta a incidentes desarrollar y mantener procesos sólidos para los incidentes y amenazas más comunes. Disponer de estos procesos acelera el descubrimiento, la clasificación y la contención de los incidentes. También mejora en gran medida la coherencia y la fiabilidad de las acciones en toda la función de respuesta a incidentes.

Caso práctico: Alcance y contención de los incidentes

Cuando se produce un incidente, los analistas de respuesta a incidentes deben tomar decisiones rápidas sobre tres factores:

1. ¿Qué ha sucedido?
2. Lo que el incidente puede significar para la organización
3. Qué medidas tomar

Estos factores deben ser analizados lo más rápidamente posible con un alto grado de precisión. La inteligencia de SecOps tiene un impacto medible al:

- Descartar automáticamente los falsos positivos, permitiendo a los equipos centrarse en los auténticos incidentes de seguridad
- Enriquecer los incidentes con información relacionada de toda la open web y la dark web, facilitando la determinación del grado de amenaza que suponen y cómo podría verse afectada la organización
- Proporcionar detalles sobre la amenaza y conocimientos sobre las TTP de los atacantes, lo que permite al equipo tomar decisiones rápidas y eficaces de contención y reparación.

Caso práctico: Remediar la exposición de los datos y los activos robados

Es habitual que las organizaciones tarden en darse cuenta de que se ha producido una infracción. Según el informe de IBM “[Informe sobre el coste de una filtración de datos en 2021](#)”, el tiempo medio para identificar una filtración de datos es de 212 días.

No es de extrañar que los datos robados y los activos de propiedad aparezcan a menudo a la venta en la dark web antes de que sus legítimos propietarios se den cuenta de lo ocurrido.

Una potente capacidad de inteligencia de SecOps proporciona una enorme ventaja al alertar de una brecha y proporcionar una advertencia temprana de que sus activos están expuestos en línea, o alguien está ofreciendo esos activos para la venta.

Obtener esta información en tiempo real es vital porque le permite contener el incidente lo antes posible e identificar cuándo y cómo se ha producido la violación de su red.

Caso de abuso: Las medias tintas son peores que nada

Queremos advertirle sobre un caso de abuso en el que la inteligencia puede socavar la respuesta al incidente.

Al principio de su viaje de inteligencia, algunas organizaciones optan por una solución minimalista como una solución de inteligencia SecOps emparejada con una variedad de feeds de amenazas gratuitos. Es posible que crean que este enfoque de “sumergirse en el agua” minimizará los costes iniciales.

Aunque este tipo de implementación dota a los equipos de respuesta a incidentes de cierta inteligencia procesable, generalmente empeora las cosas al obligar a los analistas a vadear grandes cantidades de falsos positivos y alertas irrelevantes. Para abordar plenamente los principales puntos conflictivos de la respuesta a incidentes, una capacidad de inteligencia de SecOps debe ser completa, pertinente, contextualizada e integrada.

Características esenciales de la inteligencia SecOps para la respuesta a incidentes

Ahora es el momento de examinar las características de una poderosa capacidad de inteligencia SecOps, y cómo abordan los mayores puntos de dolor para los equipos de respuesta a incidentes.

Completo

Para que sea valiosa para los equipos de respuesta a incidentes, la inteligencia debe ser capturada automáticamente desde la más amplia gama de ubicaciones a través de fuentes abiertas, fuentes técnicas y la dark web. De lo contrario, los analistas se verán obligados a realizar su propia investigación manual para asegurarse de que no se ha perdido nada importante.



Imagínese que un analista necesita saber si una dirección IP ha sido asociada a una actividad maliciosa. Si está segura de que su información se ha extraído de una amplia gama de fuentes de amenazas, puede consultar los datos al instante y estar segura de que el resultado será preciso. Si no está segura, tendrá que dedicar tiempo a comprobar manualmente la dirección IP con varias fuentes de datos sobre amenazas. La Figura 5-1 muestra cómo la inteligencia de SecOps podría conectar una dirección IP con el malware Trickbot. Este tipo de inteligencia puede correlacionarse con los registros de la red interna para revelar indicadores de compromiso.

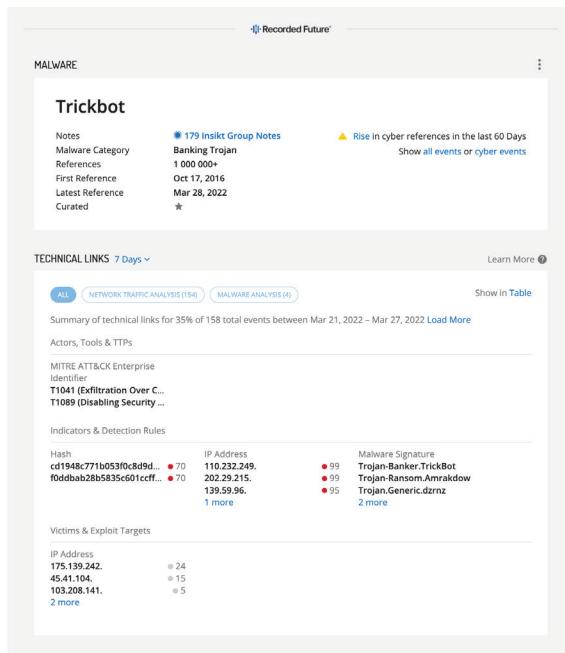


Figura 5-1: Inteligencia que conecta una dirección IP con el malware Trickbot. (Fuente: Recorded Future)



Para saber cómo destilar cantidades masivas de datos para producir un flujo pequeño pero constante de inteligencia procesable, lea el artículo del blog Recorded Future, “[Optimice su apilamiento tecnológico de seguridad con SecOps Intelligence](#).”

Relevante

Es imposible evitar todos los falsos positivos cuando se trabaja para identificar y contener los incidentes. Pero la inteligencia de SecOps permite a los equipos de respuesta a incidentes identificar y purgar rápidamente los falsos positivos generados por tecnologías de seguridad como los productos SIEM y EDR.

Hay que tener en cuenta dos categorías de falsos positivos:

1. Alertas que son relevantes para una organización pero que son inexactas o poco útiles
2. Alertas que son precisas o interesantes pero que *no son* relevantes para la organización

Ambos tipos tienen el potencial de hacer perder una enorme cantidad de tiempo a un analista de respuesta a incidentes.

Los productos avanzados de inteligencia SecOps emplean ahora potentes algoritmos y procesos analíticos para identificar y descartar automáticamente los falsos positivos y atraer la atención de los analistas hacia la inteligencia más importante (es decir, la más relevante).

PRECAUCIÓN



Si no elige la tecnología de inteligencia de SecOps con cuidado, es probable que su equipo pierda una gran cantidad de tiempo en inteligencia que es inexacta, anticuada o irrelevante para su organización.

Contextualizado

No todas las amenazas son iguales. Incluso entre las alertas de amenazas relevantes, algunas serán inevitablemente más urgentes e importantes que el resto. Una alerta de una sola fuente podría ser precisa y pertinente, pero no especialmente prioritaria. Por eso el contexto es tan importante: Proporciona pistas decisivas sobre las alertas que más interesan a su organización.

La inteligencia contextual relacionada con una alerta podría incluir:

- Corroboration por parte de múltiples fuentes de que el mismo tipo de alerta se ha asociado a ataques recientes
- Confirmación de que se ha asociado con actores de amenazas que se sabe que están activos en su industria
- Una línea de tiempo que muestra que la alerta se produjo un poco antes o después de otros eventos relacionados con los ataques

Los análisis y algoritmos modernos hacen posible que una solución de inteligencia SecOps considere múltiples fuentes simultáneamente y determine qué alertas son más importantes para una organización específica.

Integrado

Una de las características más importantes de un producto de inteligencia SecOps es su capacidad para integrarse con una amplia gama de herramientas de seguridad, incluidas las soluciones SIEM y de respuesta a incidentes. Mediante la integración, el producto es capaz de examinar las alertas que generan y:

- Determinar si cada alerta debe ser descartada como un falso positivo
- Puntúa la alerta según su importancia
- Enriquecer la alerta con contexto y pruebas valiosas en tiempo real

La integración efectiva elimina la necesidad de que los analistas comparén manualmente cada alerta con la información encontrada en su ecosistema de herramientas de seguridad e inteligencia. Y lo que es más importante, la integración y los procesos automatizados son capaces de filtrar un gran número de falsos positivos *sin necesidad de la supervisión de un analista humano..* Ahorrar tiempo y evitar la frustración son quizás los mayores beneficios de la inteligencia SecOps para los equipos de respuesta a incidentes.

Capítulo 6

Inteligencia sobre las vulnerabilidades

En este capítulo

- Examinar los desafíos actuales para abordar las vulnerabilidades
- Aprenda cómo la inteligencia de vulnerabilidades ofrece información sobre los comportamientos de los actores de amenazas
- Vea cómo la inteligencia basada en el riesgo agiliza los elementos operativos de la gestión de vulnerabilidades

La gestión de vulnerabilidades no es glamorosa, pero es una de las pocas maneras de ser proactivo en la seguridad de su organización. No se puede exagerar su importancia.

La clave del éxito en la gestión de vulnerabilidades es cambiar la mentalidad de sus equipos de seguridad, pasando de intentar parchear todo a tomar decisiones basadas en el riesgo. Esto es fundamental porque el vasto océano de vulnerabilidades que se revelan cada año pone una tensión increíble en los equipos responsables de identificar los activos vulnerables y desplegar los parches. Para tomar decisiones inteligentes basadas en el riesgo, aproveche más fuentes de inteligencia.

El problema de las vulnerabilidades en cifras

Según la Guía de Mercado de Productos y Servicios de Inteligencia sobre Amenazas a la Seguridad de Gartner, en la última década se revelaron unas 8000 vulnerabilidades al año. El número solo aumentó ligeramente de un año a otro, y solo una de cada ocho de esas vulnerabilidades fue realmente explotada. Sin embargo, durante el mismo periodo, la cantidad de nuevos programas informáticos que entran en funcionamiento ha crecido enormemente, y el número de amenazas ha aumentado exponencialmente.

En otras palabras, aunque el número de infracciones y amenazas ha aumentado en los últimos 10 años, solo un pequeño porcentaje se basó en nuevas vulnerabilidades. Como dice Gartner, “más amenazas están aprovechando el mismo pequeño conjunto de vulnerabilidades”.

Día cero no significa prioridad máxima

Las amenazas de día cero atraen regularmente una cantidad exagerada de atención. Sin embargo, la gran mayoría de las nuevas amenazas etiquetadas como de día cero son en realidad variaciones sobre un tema, explotando las mismas viejas vulnerabilidades de maneras ligeramente diferentes. La implicación es que el enfoque más eficaz para la gestión de vulnerabilidades no es centrarse en las amenazas de día cero, sino identificar y parchear las vulnerabilidades en el software que su organización utiliza.

El tiempo es esencial

Los actores de las amenazas se han vuelto más rápidos a la hora de explotar las vulnerabilidades. Según Gartner, el tiempo medio que transcurre entre la identificación de una vulnerabilidad y la aparición de un exploit in the wild ha bajado de 45 a 15 días en la última década.

Esta tendencia tiene dos implicaciones para los equipos de gestión de vulnerabilidades:

1. Tiene aproximadamente dos semanas para parchear o remediar sus sistemas contra un nuevo exploit.
2. Si no puede parchear en ese plazo, necesita un plan para mitigar los daños.

Las investigaciones de IBM X-Force muestran que, si una vulnerabilidad no se explota entre dos semanas y tres meses después de su anuncio, es estadísticamente improbable que se explote alguna vez. Por lo tanto, las vulnerabilidades “antiguas” no suelen ser una prioridad para la aplicación de parches.



Para conocer las vulnerabilidades recientes, lea el análisis de amenazas de Recorded Future “[2021 Panorama de las Vulnerabilidades](#).”



Todas estas estadísticas apuntan a una conclusión: Su objetivo no debe ser parchear el mayor número de vulnerabilidades, ni siquiera el mayor número de amenazas de día cero, sino identificar y abordar las vulnerabilidades con mayor probabilidad de ser explotadas contra su organización.

Evaluar el riesgo en función de la explotabilidad

Considere esta comparación: Si pone parches a las vulnerabilidades para mantener la seguridad de la red es como ponerse vacunas para protegerse de las enfermedades, entonces hay que identificar qué vacunas son prioritarias y cuáles son innecesarias. Puede que necesites una vacuna contra la gripe cada temporada para mantenerte sano, pero no es necesario que te vacunes contra la fiebre amarilla o la malaria a menos que vayas a estar expuesto a ellas.

Dos de los mayores valores de una solución de inteligencia de vulnerabilidades son la identificación de vulnerabilidades específicas que representan un riesgo real para su organización y la visibilidad de su probabilidad de explotación.

La figura 6-1 ilustra este punto. Se han revelado miles de vulnerabilidades. Se están explotando cientos de ellas, y existe un cierto número de vulnerabilidades en su entorno. En realidad, solo hay que preocuparse por las que se encuentran en la intersección de esas dos últimas categorías, es decir, las vulnerabilidades que se encuentren en su entorno y que están siendo explotadas activamente.

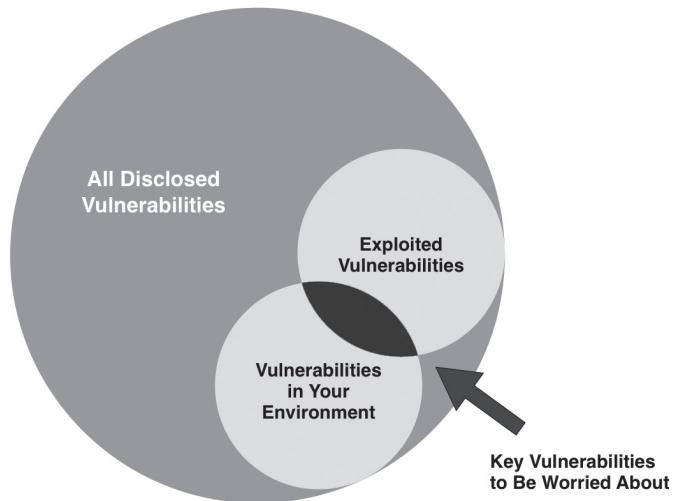


Figura 6-1: Los mayores riesgos reales son las vulnerabilidades que están presentes en el entorno de su organización y que están siendo explotadas. (Fuente: Gartner)

Las puntuaciones CVSS suelen ser engañosas

Clasificar las amenazas en términos de gravedad es un error que los gestores de vulnerabilidades cometen con regularidad. Los sistemas de clasificación y jerarquización, como la denominación de Vulnerabilidades y Exposiciones Comunes (CVE) y los Sistemas de Puntuación de Vulnerabilidades Comunes (CVSS), no tienen en cuenta si los actores de las amenazas están explotando realmente las vulnerabilidades en este momento en su sector o lugares. Es importante tener en cuenta que a los actores de las amenazas no les importan las puntuaciones CVSS.

La génesis de la inteligencia para los equipos de seguridad: Bases de datos de vulnerabilidades

Las bases de datos de vulnerabilidades consolidan la información sobre las vulnerabilidades reveladas y también puntúan su capacidad de explotación.

De hecho, una de las primeras formas de inteligencia para

los equipos de seguridad fue la Base de Datos Nacional de Vulnerabilidades (NVD) del NIST. Centraliza la información sobre las vulnerabilidades reveladas para facilitar a las organizaciones la posibilidad de verse afectadas. Durante más de 20 años, el NVD ha recopilado información sobre más de 150 000 vulnerabilidades, lo que lo convierte en una fuente inestimable para los profesionales de la seguridad de la información. Países como China y Rusia han seguido el ejemplo del NIST creando bases de datos de vulnerabilidades.



Encuentre el NVD del NIST en <https://nvd.nist.gov/>. La organización del sector FIRST publica un catálogo de bases de datos de vulnerabilidades aquí: <https://www.first.org/global/sigs/vrdx/vdb-catalog>.



La mayoría de las bases de datos de vulnerabilidades tienen dos limitaciones importantes:

1. Se centran en la explotabilidad técnica más que en la explotación activa.
2. No se actualizan con la suficiente rapidez como para advertir de algunas amenazas que se propagan rápidamente.

Explotabilidad frente a explotación

La información de las bases de datos de vulnerabilidades se centra casi por completo en la explotabilidad técnica, es decir, un juicio sobre la probabilidad de que la explotación de una determinada vulnerabilidad provoque un daño mayor o menor en los sistemas y redes. En el NVD, esto se mide a través del sistema de puntuación CVSS.

Sin embargo, la explotabilidad técnica y la explotación activa no son lo mismo. Las puntuaciones base de CVSS proporcionan una métrica razonablemente precisa y fácil de entender, pero hay que saber qué información transmite la puntuación. A menos que la puntuación base se modifique por una puntuación temporal o una puntuación de entorno, en realidad solo te dice lo mala que es la vulnerabilidad hipotéticamente, no si realmente se está explotando en la naturaleza.

La Figura 6-2 muestra el tipo de información valiosa que proporciona una herramienta de inteligencia de vulnerabilidades. En este caso, el riesgo que supone una vulnerabilidad se determina en base a los informes que implican la aparición del CVE antes de que se le haya asignado una puntuación CVSS por parte de NVD.

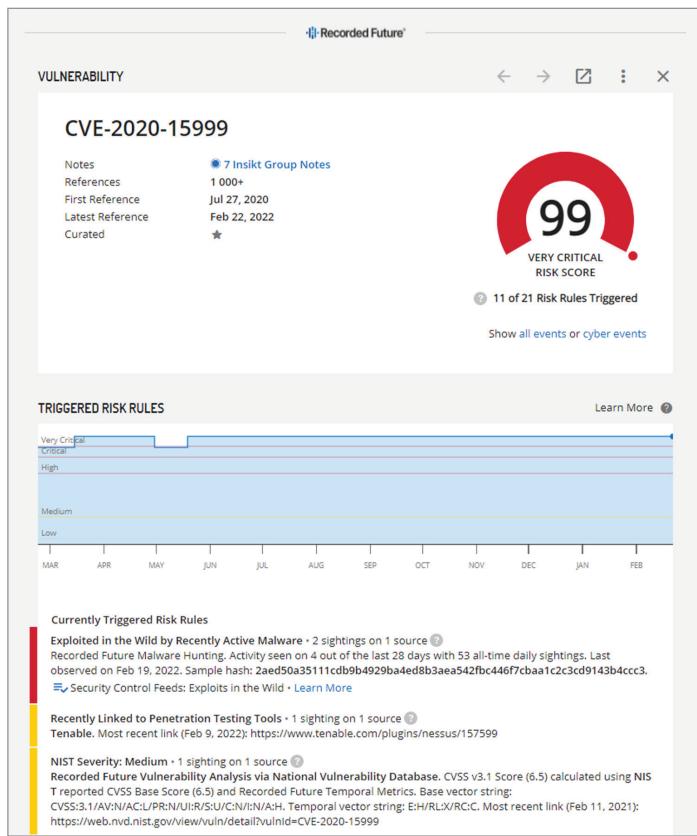


Figura 6-2: Inteligencia relacionada con una vulnerabilidad. (Fuente: Recorded Future)



Una lección objetiva sobre la diferencia entre el “riesgo oficial” del NVD y el “riesgo real” de una vulnerabilidad en la naturaleza es CVE- 2020-15999. A pesar de tener una puntuación de gravedad CVSS de solo 6.5 (en el rango medio), Recorded Future lo consideró un riesgo muy alto debido a la evidencia reciente de explotación generalizada.

La próxima semana frente a la actual

La falta de puntualidad es otro de los defectos de muchas bases de datos de vulnerabilidades. Por ejemplo, un análisis de Recorded Future descubrió que el 75 % de las vulnerabilidades reveladas aparecen en otras fuentes en línea antes de que aparezcan en el NVD, y en promedio esas vulnerabilidades

tardan una semana en aparecer allí. Este es un problema muy serio, porque perjudica a los equipos de seguridad en la carrera por parchear una vulnerabilidad antes de que los adversarios sean capaces de explotarla, como se ilustra en la Figura 6-3.

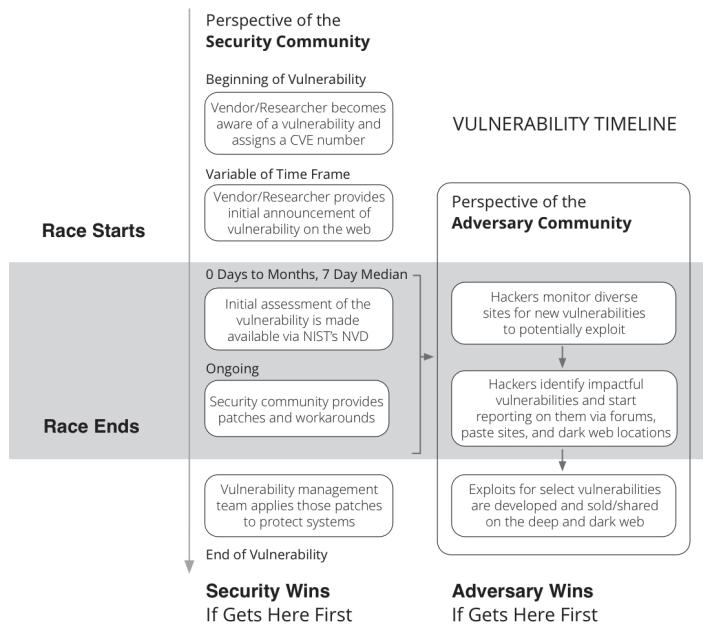


Figura 6-3: La carrera entre los profesionales de la seguridad y los adversarios. (Fuente: Recorded Future)



La manera informal en que se divultan y anuncian las vulnerabilidades contribuye al retraso en su reconocimiento en las bases de datos de vulnerabilidades. Normalmente, un vendedor o investigador revela la vulnerabilidad al NVD, que asigna un número CVE y comienza un análisis. Mientras tanto, el vendedor o investigador publica más información en su propio blog o en una cuenta en las redes sociales. Buena suerte en la recopilación de datos de estas fuentes dispares y difíciles de encontrar antes de que los actores de las amenazas desarrollen pruebas de concepto de malware y las añadan a los kits de exploits.



Para conocer los detalles de los procesos que utilizan los actores de las amenazas para explotar las vulnerabilidades, consulte la publicación del blog de Recorded Future “[Entre bastidores del proceso de explotación del adversario..](#)”

Inteligencia sobre vulnerabilidades y riesgo real

La forma más eficaz de evaluar el verdadero riesgo de una vulnerabilidad para su organización es combinar todo lo siguiente:

- Datos de exploración de vulnerabilidades internas
- Información externa procedente de una gran variedad de fuentes
- Contexto empresarial, como la criticidad de los activos y la exposición de la red
- Entender por qué los actores de las amenazas apuntan a ciertas vulnerabilidades e ignoran otras

Exploración de vulnerabilidades internas

Casi todos los equipos de gestión de vulnerabilidades escanean los sistemas internos en busca de vulnerabilidades, correlacionan los resultados con la información reportada en las bases de datos de vulnerabilidades y utilizan la correlación para determinar qué parches aplicar. Se trata de un uso básico de la inteligencia operativa, aunque no solemos pensarlo así.

El escaneo convencional es una excelente manera de *dejar de priorizar* las vulnerabilidades que no aparecen en sus sistemas. Sin embargo, el escaneo por sí mismo no es una forma adecuada de priorizar con precisión las vulnerabilidades que se encuentran.

Hitos de riesgo para las vulnerabilidades

Una forma poderosa de evaluar el riesgo de una vulnerabilidad es observar hasta qué punto ha progresado desde la identificación inicial hasta la disponibilidad, la militarización y la mercantilización en kits de exploits.

El nivel de riesgo real aumenta drásticamente a medida que la vulnerabilidad pasa por los hitos mostrados en la Figura 6-4. La inteligencia de vulnerabilidades de base amplia revela el progreso de una vulnerabilidad a lo largo de este camino.

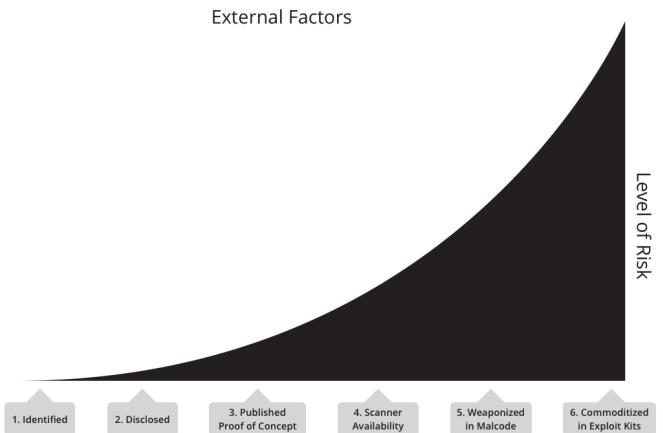


Figura 6-4: El riesgo real aumenta drásticamente cuando las vulnerabilidades se convierten en un arma y en una mercancía.
(Fuente: Recorded Future)

Entender al adversario

Como ya se ha comentado en este libro, una buena inteligencia no debe limitarse a proporcionar información en forma de resultados y estadísticas. Por ello, la inteligencia sobre vulnerabilidades permite comprender mejor cómo y por qué los actores de las amenazas se centran en ciertas vulnerabilidades e ignoran otras. A continuación, analizamos las fuentes de inteligencia que contribuyen a esta comprensión.

Cómo crear puntuaciones de riesgo significativas

Más allá de las características técnicas, ¿cuáles son los factores que pueden utilizarse para calcular las puntuaciones de riesgo de las vulnerabilidades? El sistema nativo de puntuación de riesgos de Recorded Future incorpora

datos sobre la adopción de delitos, patrones de intercambio de exploits y el número de enlaces a programas maliciosos. Esta información suele proceder de fuentes de difícil acceso, como los foros de la dark web.

Fuentes de información

Los datos de los escaneos de activos y las bases de datos de vulnerabilidades externas son solo el punto de partida para generar inteligencia que le permita evaluar el riesgo de las vulnerabilidades. A menos que la inteligencia sobre vulnerabilidades incluya datos de una amplia gama y variedad de fuentes, los analistas corren el riesgo de pasar por alto las vulnerabilidades emergentes hasta que sea demasiado tarde.

Entre las fuentes de información valiosas para evaluar el verdadero riesgo de su empresa se encuentran:

- Sitios de seguridad de la información**, como blogs de proveedores, información oficial sobre vulnerabilidades y sitios de noticias de seguridad
- Las redes sociales**, donde el intercambio de enlaces proporciona puntos de partida para descubrir información útil
- Repositorios de código** como GitHub, que permiten conocer el desarrollo de código de prueba para explotar vulnerabilidades
- Sitios como** Pastebin y Ghostbin (que a veces se definen erróneamente como fuentes de la dark web) que suelen albergar listas de vulnerabilidades explotables
- La dark web**, compuesta por comunidades y mercados con una barrera de entrada, donde se desarrollan, comparten y venden exploits
- Foros** sin barrera de entrada ni requisito de uso de software específico, donde los actores de las amenazas intercambian información sobre vulnerabilidades y exploits
- Fuentes técnicas** que proporcionan flujos de datos de indicadores potencialmente maliciosos, que añaden un contexto útil en torno a las actividades del malware y los kits de exploit

Charla sobre vulnerabilidades en la Dark Web

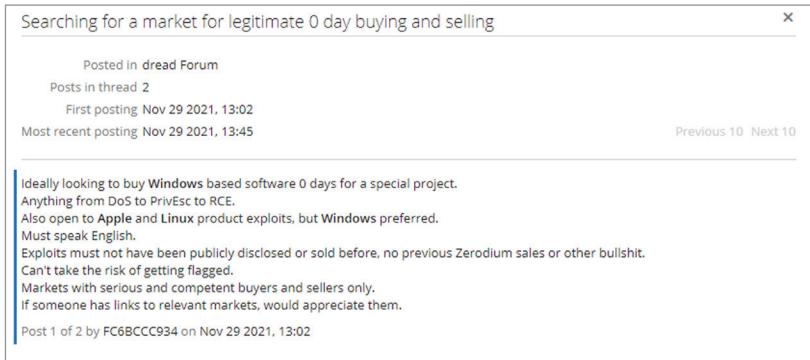
Hay varias razones por las que es difícil (y potencialmente peligroso) espiar los canales que los actores de las amenazas utilizan para comunicarse y operar:

- Los foros clandestinos son difíciles de encontrar (después de todo, no existe Google para la dark web).
- Los actores de la amenaza cambian de ubicación cuando sienten que su anonimato está en peligro.
- Hay que buscar mucho para encontrar las migajas de información que son relevantes para su seguridad.
- El acceso puede requerir el pago de una cuota de entrada o el aval

de los miembros existentes de la comunidad.

- Muchos de estos foros funcionan exclusivamente en las lenguas locales.

Aquí entran en juego los proveedores de inteligencia con experiencia en la recopilación y el análisis de la inteligencia de la dark web. Ofrecen información contextualizada de los foros de la dark web sobre las vulnerabilidades directamente relevantes para su red, sin ponerle a usted o a su organización en peligro.



The screenshot shows a forum post titled "Searching for a market for legitimate 0 day buying and selling". The post was made in the "dread Forum" and has 2 posts in the thread. It was first posted on Nov 29 2021, 13:02 and most recently on Nov 29 2021, 13:45. The post content is as follows:

```

Ideally looking to buy Windows based software 0 days for a special project.
Anything from DoS to PrivEsc to RCE.
Also open to Apple and Linux product exploits, but Windows preferred.
Must speak English.
Exploits must not have been publicly disclosed or sold before, no previous Zerodium sales or other bullshit.
Can't take the risk of getting flagged.
Markets with serious and competent buyers and sellers only.
If someone has links to relevant markets, would appreciate them.

Post 1 of 2 by FC6BCCC934 on Nov 29 2021, 13:02

```

Figura 6-5: Un intercambio de información entre actores de amenazas en un foro de la dark web traducido del ruso. (Fuente: Recorded Future)

Casos prácticos de la inteligencia cruzada

Para evaluar con precisión el riesgo real, hay que ser capaz de correlacionar la información de múltiples fuentes. Una vez que empiece a entender cómo se combinan las referencias individuales para contar la historia completa, podrá asignar la inteligencia que tiene a los hitos de riesgo por los que suele pasar una vulnerabilidad.

Por ejemplo, puede notar una nueva vulnerabilidad divulgada en el sitio web de un proveedor. Entonces, descubre un tuit con un enlace al código de prueba de concepto del exploit en GitHub. Más tarde, descubre que el código se vende en un foro de la dark web. Eventualmente, podría ver informes de noticias sobre la vulnerabilidad explotada en la naturaleza.

He aquí otro ejemplo. El sitio web de un Centro de Análisis e Intercambio de Información (ISAC) de su sector muestra que una organización como la suya ha sido víctima de un kit de exploit que ataca una vulnerabilidad en una aplicación de software especializada y específica del sector. Descubre que hay cuatro copias de ese software en rincones de su organización que no han sido parcheados en tres años.



Las referencias cruzadas de este tipo de inteligencia le permiten alejarse de un modo de operación de “carrera para parchear todo”, y le permite centrarse en las vulnerabilidades que presentan el mayor riesgo real.

Reducción de las diferencias de riesgo entre los responsables de la seguridad, las operaciones y la empresa

En la mayoría de las organizaciones, la responsabilidad de la protección contra las vulnerabilidades recae sobre los hombros de dos equipos:

1. El equipo de gestión de vulnerabilidades realiza escaneos y prioriza las vulnerabilidades en función del riesgo potencial.
2. El equipo de operaciones de TI despliega los parches y repara los sistemas afectados.

Esta dinámica crea una tendencia a abordar la gestión de vulnerabilidades “por los números”. Por ejemplo, el equipo de gestión de vulnerabilidades de la organización de seguridad podría determinar que varias vulnerabilidades en los servidores web Apache suponen un riesgo muy alto para la empresa y deberían tener la máxima prioridad. Sin embargo, el equipo de operaciones de TI puede dar soporte a muchos más sistemas Windows que a servidores Apache. Si los miembros del equipo se miden estrictamente por el número de sistemas parcheados, tienen un incentivo para mantener su atención en las vulnerabilidades de Windows de menor prioridad.

La información sobre la capacidad de explotación también prepara a su organización para lograr el equilibrio correcto entre la aplicación de parches en los sistemas vulnerables y la interrupción de las operaciones comerciales. La mayoría de las organizaciones tienen una fuerte aversión a perturbar la continuidad del negocio. Sin embargo, si sabe que un parche protegerá a la organización contra un riesgo real e inminente, entonces una breve interrupción está completamente justificada.

El marco de hitos de riesgo esbozado en la Figura 6-4 hace mucho más fácil comunicar el peligro de una vulnerabilidad a través de sus equipos de seguridad y operaciones, a través de los altos directivos, e incluso a la junta directiva. Este nivel de visibilidad de los fundamentos de las decisiones tomadas en torno a las vulnerabilidades aumentará la confianza en el equipo de seguridad de toda la organización.

**SUGERENCIA**

Para reducir la brecha entre los equipos de gestión de vulnerabilidades y de operaciones de TI, introduzca el riesgo de explotabilidad como un factor clave para priorizar los parches. Dotar al equipo de gestión de vulnerabilidades de datos más contextualizados sobre el riesgo de explotabilidad los permitirá identificar un número menor de CVE de alto riesgo, lo que les llevará a exigir menos al equipo de operaciones. El equipo de operaciones podrá entonces dar la máxima prioridad a ese pequeño número de parches críticos, y seguir teniendo tiempo para abordar sus otros objetivos.

Capítulo 7

Inteligencia sobre amenazas

Parte 1: conocer a los atacantes

En este capítulo

- Explorar el papel de los analistas de amenazas
- Vea cómo las conversaciones en las comunidades clandestinas presentan oportunidades para reunir información valiosa
- Examine los casos prácticos para aplicar los conocimientos sobre los atacantes a las actividades de seguridad

Nuestra definición de “inteligencia sobre amenazas”

Hasta hace poco, muchos de los temas tratados en este manual eran conocidos en toda la comunidad de seguridad como “inteligencia sobre amenazas”. Sin embargo, el término inteligencia sobre amenazas se ha asociado estrechamente con la información sobre amenazas directas a los sistemas informáticos tradicionales. Ahora utilizamos “inteligencia para equipos de seguridad”, o simplemente “inteligencia” para incluir esa información, además de detalles adicionales sobre los riesgos relacionados con áreas como terceros, la presencia de la marca en sitios web y plataformas de medios sociales fuera de la red corporativa, los riesgos para los activos físicos en todo el mundo, y más.

Este cambio no ha eliminado la necesidad de inteligencia sobre amenazas. Sigue siendo esencial para que los analistas de amenazas puedan realizar sus funciones más importantes, entre ellas:

- Identificar a los actores que amenazan más activamente a la organización
- Comprender los motivos y los objetivos de los atacantes
- Investigar y documentar sus TTP
- Seguimiento de las macrotendencias que afectan a la organización, incluidas las tendencias relevantes para su sector y las regiones en las que opera

Una solución de inteligencia es esencial para el éxito de los analistas de amenazas, porque señala las amenazas más relevantes, reduce el tiempo que dedican a investigarlas y genera más inteligencia sobre ellas, a menudo procedente de fuentes a las que sería difícil o imposible que los analistas encontraran y accedieran por sí mismos.

En este capítulo y en el siguiente examinaremos varias de las principales responsabilidades de los analistas de amenazas.

Entienda a su enemigo

Los analistas de amenazas no pueden centrarse únicamente en detectar y responder a las amenazas ya presentes en su entorno. Deben anticiparse a los ataques reuniendo información sobre las bandas de cibercriminales, los grupos de piratas informáticos patrocinados por el Estado, los “hacktivistas” ideológicos y otros que atacan a sus organizaciones.

Como ejemplo, veamos el tipo de información que se puede encontrar sobre las bandas de cibercriminales con ánimo de lucro. Son un importante objetivo de inteligencia, ya que el “[Informe sobre investigaciones de filtraciones de datos de Verizon 2021](#)” atribuye el 80 % de las filtraciones confirmadas al crimen organizado (Figura 7-1).

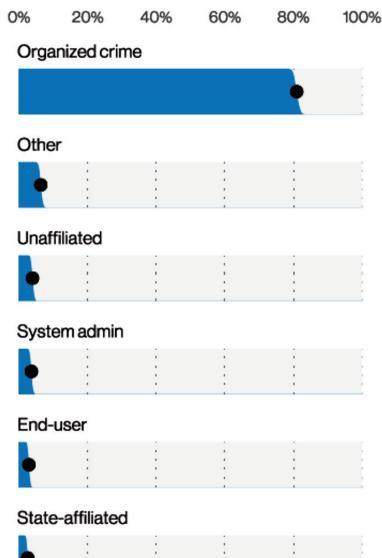


Figura 7-1: Principales variedades de actores externos en las violaciones de datos. (Fuente: Verizon Data Breach Investigation Report 2021)

La información recopilada por Recorded Future en las comunidades mundiales de la dark web muestra que los grupos delictivos organizados (GDO) emplean a trabajadores autónomos para estafar a empresas y particulares. Estos grupos operan como las empresas legítimas en muchos aspectos, con una jerarquía de miembros que funcionan como un equipo para crear, operar y mantener los esquemas de fraude.

Un OCG típico está controlado por un único cerebro (Figura 7-2). Puede incluir especialistas con conocimientos relevantes para los delitos que cometen. Por ejemplo, los banqueros con amplias conexiones en la industria financiera podrían organizar el blanqueo de dinero, los falsificadores podrían ser responsables de los documentos falsos y el papeleo de apoyo, los gestores de proyectos profesionales podrían supervisar los aspectos técnicos de las operaciones, los ingenieros de software escribirían el código y otros codificadores cualificados podrían participar en tareas específicas. Algunos grupos incluyen incluso a ex agentes de las fuerzas del orden que recopilan información y dirigen operaciones de contrainteligencia.

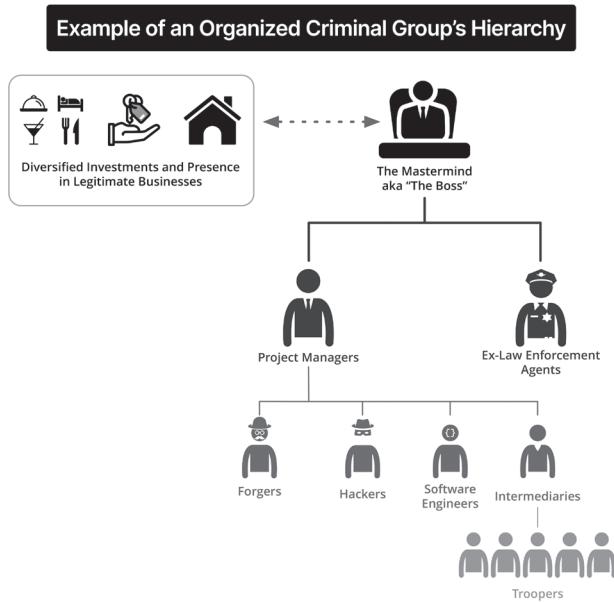


Figura 7-2: Organigrama típico de un sindicato de ciberdelincuentes. (Fuente: Recorded Future)

Los miembros de los sindicatos de ciberdelincuentes suelen tener fuertes vínculos en la vida real, y a menudo son miembros respetados de sus grupos sociales. Desde luego, no se consideran delincuentes callejeros ordinarios. Rara vez se cruzan con lo que la mayoría de la gente considera gánsteres tradicionales, pues prefieren permanecer en la sombra y evitar la atención de las fuerzas del orden y de las ramas locales de la mafia. Sin embargo, los esquemas que requieren un gran número de personas, como los que implican sacar dinero de varios cajeros automáticos simultáneamente, pueden implicar una cadena de intermediarios que reclutan y dirigen a los soldados que hacen el trabajo de campo.

Las comunidades criminales y la Dark Web

Solo en raras ocasiones los analistas de amenazas pueden atribuir un ciberataque a un solo individuo que actúe de forma aislada. Los ataques avanzados suelen requerir una amplia gama de habilidades y herramientas, así como una infraestructura capaz de lanzar y apoyar campañas que utilizan ransomware,

phishing y otras herramientas técnicas y técnicas de ingeniería social.

Hoy en día, todos esos productos y servicios se pueden comprar o alquilar en una sofisticada economía criminal clandestina. Los ciberdelincuentes y sus cómplices intercambian información y realizan transacciones relacionadas con actividades ilícitas en la deep web (zonas de la web que no están indexadas por los motores de búsqueda) y la dark web (zonas de la web a las que solo se puede acceder con programas y herramientas especiales que enmascaran la identidad de los visitantes).

Comunidades cerradas

No todos los actores de amenazas operan exclusivamente en lo que técnicamente se denominaría la dark web. Algunos construyen comunidades basadas en tableros de discusión bastante estándar que están encriptados detrás de un inicio de sesión y utilizan tecnologías de colaboración web como Jabber y Telegram para llevar a cabo sus actividades.

Los posibles miembros de estas redes clandestinas son investigados por los participantes activos en las salas de chat y los foros antes de que se les permita unirse. Es posible que tengan que pagar una cuota de entrada, que oscila entre 50 y 2000 dólares o más. De hecho, se sabe que al menos un foro exige un depósito de más de 100 000 dólares a los posibles miembros.

Un punto fuerte y un punto débil

La dark web y las comunidades criminales dan a los actores de las amenazas acceso a información, herramientas, infraestructura y servicios contratados que multiplican su poder y alcance. Sin embargo, estas comunidades también suponen un riesgo para los actores de las amenazas, ya que son susceptibles de ser vigiladas, lo que proporciona información que permite a los equipos de seguridad anticiparse a los ataques y vencerlos.

Conozca sus Dark Networks

Descubrimos que la dark web está organizada en tres comunidades distintas: foros clandestinos de bajo nivel, foros de la dark web de alto nivel y mercados de la dark web. El análisis ha revelado que un grupo importante de actores publica tanto en los foros de nivel bajo como en los de nivel alto, lo que demuestra una conexión

entre estas dos comunidades. Sin embargo, los mercados de la dark web están muy desconectados de estos foros. Conozca mejor cómo la delincuencia clandestina mantiene una jerarquía de usuarios leyendo esta investigación de Recorded Future: “[Dark Networks: análisis de redes sociales de las comunidades de la Dark Web..](#)”

Conectar los puntos

La inteligencia obtenida de las comunidades clandestinas es una ventana a las motivaciones, los métodos y las tácticas de los actores de las amenazas, especialmente cuando esta inteligencia se correlaciona con la información de la red de superficie, incluidas las fuentes e indicadores técnicos.

El poder de la inteligencia verdaderamente contextualizada queda demostrado por su capacidad para reunir datos de una amplia variedad de fuentes y establecer conexiones entre piezas de información dispares.

Por ejemplo, la siguiente información contextual podría utilizarse para convertir las noticias sobre una nueva variante de malware en inteligencia:

- Pruebas de que los actores de la amenaza están utilizando este malware en la naturaleza
- Los informes indican que los kits de exploits que utilizan el malware están disponibles para la venta en la dark web
- Confirmación de que las vulnerabilidades a las que se dirigen los kits de exploits están presentes en su organización



Vigile la dark web y las comunidades clandestinas en busca de menciones directas a su organización y sus activos. Estas menciones suelen indicar la existencia de objetivos o posibles infracciones. También es importante vigilar las menciones a su sector y otros términos menos específicos que puedan apuntar a

sus operaciones. El uso de la inteligencia de amenazas para evaluar el riesgo de esta manera le dará mayor confianza sobre sus defensas y le permitirá tomar mejores decisiones.

Caso práctico: Una respuesta más completa a los incidentes

Cuando se detectan indicadores de una amenaza, los equipos de SecOps toman medidas inmediatas para proteger los activos objetivo. Sin embargo, confían en que los analistas de amenazas investiguen el ataque y proporcionen información adicional para cerrarlo de forma más completa, remediar sus efectos y evitar que se produzca en el futuro.

Por ejemplo, los analistas de amenazas suelen ser capaces de atribuir un ataque a un ciberdelincuente concreto o a un grupo de piratas informáticos patrocinado por el Estado e investigar las TTP del grupo. Los equipos de seguridad pueden utilizar esa información para tomar medidas como encontrar otros casos de malware y correos electrónicos de phishing utilizados en el ataque, limpiar los sistemas afectados, poner en cuarentena los correos electrónicos, obligar a cambiar las contraseñas de las cuentas comprometidas y tomar otras medidas para interrumpir la cadena asesina del atacante.



La investigación para responder a los incidentes y remediarlos de forma exhaustiva requiere una cantidad de tiempo considerable. Para lograr una respuesta rápida, es fundamental utilizar una solución de inteligencia con automatización e integración para recopilar y procesar grandes volúmenes de datos procedentes de muchas fuentes y encontrar el contexto y las perspectivas pertinentes. La solución de inteligencia también debe ser capaz de automatizar los flujos de trabajo para analizar la inteligencia y difundirla rápidamente a los equipos de seguridad y a la dirección adecuados, dentro de sus herramientas de seguridad existentes y en sus formatos preferidos.

Caso práctico: Búsqueda proactiva de amenazas

La mayoría de los programas de seguridad son reactivos, es decir, dependen de las alertas antes de actuar. Sin embargo, muchas organizaciones están creando equipos de caza de amenazas para buscar proactivamente indicadores de amenazas antes de que

se genere una alerta e, idealmente, antes de que el ataque haya avanzado mucho.

Hay cientos de pistas que los cazadores de amenazas pueden buscar en las redes y los puntos finales. Entre ellas se encuentran: Archivos de malware, cambios sospechosos en las claves del registro, configuraciones del sistema y permisos de las aplicaciones, DLL, scripts y controladores inusuales, uso indebido de utilidades como PowerShell y PSEexec, comportamientos anómalos de los archivos JOB, binarios que inician conexiones fuera de la red corporativa, secuencias de eventos inusuales (como aplicaciones que descargan y ejecutan scripts al iniciarse) y técnicas utilizadas para robar credenciales.

Las soluciones de inteligencia proporcionan perfiles detallados de los actores de las amenazas que actualmente atacan a organizaciones similares y de las técnicas y herramientas que utilizan. Esta información permite a los cazadores de amenazas evitar “hervir el océano” tratando de capturar y analizar grandes cantidades de datos. En cambio, pueden priorizar las búsquedas de las amenazas más peligrosas para su organización y centrarse en la búsqueda de indicadores y artefactos específicos relacionados con esos ataques.



SUGERENCIA Para reforzar la caza de amenazas, explore el uso del análisis del tráfico de red (NTA). La NTA consiste en supervisar y analizar los datos de la red para identificar anomalías y proporcionar información y contexto sobre la infraestructura maliciosa conectada a su red. Los atacantes utilizan estas conexiones maliciosas para enviar comandos, recibir actualizaciones de información y exfiltrar datos. A través de la NTA, una organización puede detectar los hosts maliciosos que se conectan a una red y avisar cuando esas conexiones exfiltran datos. La NTA proporciona inteligencia procesable en tiempo real que advierte a los equipos de seguridad sobre las acciones de los adversarios y muestra hasta qué punto han progresado sus ataques.

Caso práctico: Aviso anticipado de fraude en los pagos

Desde el nacimiento del comercio, los delincuentes han buscado la manera de utilizar la tecnología disponible para obtener un beneficio fácil de los que poseen bienes. En la Inglaterra del siglo XVII, por ejemplo, el aumento de los viajes en carruaje entre una

clase mercantil acomodada, combinado con la invención de la pistola portátil de pedernal, dio origen al salteador de caminos.

En nuestra era digital, las empresas que realizan negocios y transacciones en línea encuentran sus datos en el punto de mira de diversas formas de ciberfraude, incluido el fraude en los pagos.

El término “fraude en los pagos” engloba una amplia variedad de técnicas mediante las cuales los ciberdelincuentes se benefician de los datos de pago comprometidos. Por ejemplo, pueden utilizar la suplantación de identidad para obtener los datos de las tarjetas de pago. Ataques más complejos podrían comprometer sitios de comercio electrónico o sistemas de puntos de venta para lograr el mismo objetivo. Una vez adquiridos los datos de las tarjetas, los delincuentes los revenden (a menudo en forma de paquetes de números) y se llevan su parte.

Un ejemplo del uso eficaz de la inteligencia sobre amenazas es proporcionar a los analistas de amenazas una advertencia anticipada de los próximos ataques relacionados con el fraude en los pagos. La supervisión de fuentes como las comunidades clandestinas, los sitios de pasta y otros foros en busca de números de tarjetas de pago relevantes, números de identificación bancaria o referencias específicas a las instituciones financieras proporciona potencialmente visibilidad de las operaciones nefastas que podrían afectar a su organización. A continuación, los analistas pueden trabajar con otros equipos de seguridad para evitar los ataques planeados, corrigiendo las vulnerabilidades pertinentes, aumentando la vigilancia de los sistemas objetivo y reforzando los controles de seguridad. El capítulo 12 contiene más información sobre el uso de la inteligencia para frustrar el fraude en los pagos.

Capítulo 8

Inteligencia sobre amenazas

Parte 2: análisis de riesgos

En este capítulo

- Explorar el valor de los modelos de riesgo como el marco FAIR
- Descubrir las formas correctas e incorrectas de recopilar datos sobre el riesgo
- Aprenda cómo la inteligencia le permite prever las probabilidades de ataque y los costes financieros de los ataques

Una función clave de los analistas de amenazas es modelar los riesgos y capacitar a los gestores para que tomen decisiones informadas sobre la reducción del riesgo. La modelización de riesgos ofrece una forma de evaluar objetivamente los riesgos actuales y de estimar un rendimiento financiero claro y cuantificable de las inversiones en ciberseguridad.

Sin embargo, muchos modelos de ciberriesgo adolecen de cualquiera de las dos cosas:

- Resultados vagos y no cuantificados, a menudo en forma de “gráficos de semáforo” que muestran los niveles de amenaza verde, amarilla y roja
- Estimaciones sobre las probabilidades de amenaza y los costes que se recopilan apresuradamente, se basan en información parcial y están plagadas de suposiciones infundadas

Los resultados no cuantificados no son muy útiles, mientras que los modelos basados en datos defectuosos dan lugar a escenarios de “basura entrante, basura saliente” con resultados que parecen ser precisos, pero que en realidad son engañosos. Para evitar estos problemas, las organizaciones necesitan un modelo de

riesgo bien diseñado y mucha información válida y actualizada, incluida la inteligencia sobre amenazas.

SUGERENCIA


Las evaluaciones de los riesgos de ciberseguridad no deben basarse únicamente en criterios definidos para demostrar el cumplimiento de la normativa. Con estos criterios, la evaluación del riesgo suele convertirse en un ejercicio de comprobación de las casillas de los controles de ciberseguridad, como los cortafuegos y el cifrado. Contar el número de casillas marcadas da una imagen muy engañosa del riesgo real.

El modelo de riesgo FAIR

La ecuación en la que se basa cualquier modelo de riesgo es sencilla:

“La probabilidad de ocurrencia multiplicada por el impacto es igual al coste esperado”.

Pero, evidentemente, el diablo está en los detalles. Afortunadamente, algunas personas muy inteligentes han desarrollado modelos y metodologías de riesgo eficaces que usted puede utilizar y adaptar a sus propias necesidades. Uno de los que nos gusta es el modelo de Análisis de Factores de Riesgo de la Información (FAIR) del Instituto FAIR. La figura 8-1 muestra el marco de este modelo.

El marco FAIR es útil para crear un modelo cuantitativo de evaluación de riesgos que contenga probabilidades específicas de pérdidas por tipos específicos de amenazas.

EN LA WEB


Más información sobre [FAIR en el sitio web del Instituto FAIR](#). Este modelo cuantitativo para la seguridad de la información y el riesgo operativo se centra en comprender, analizar y cuantificar el riesgo de la información en términos financieros reales.

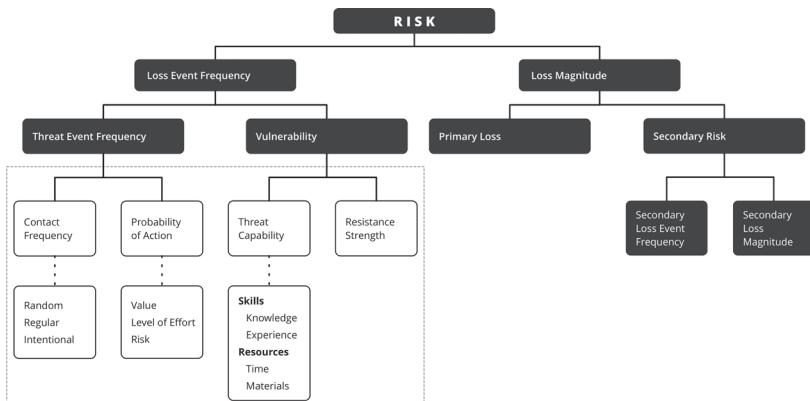


Figura 8-1: El Marco FAIR, con elementos informados por la inteligencia destacados. (Fuente: The FAIR Institute)

Las medidas y la transparencia son fundamentales

El marco FAIR (y otros similares) permite crear modelos de riesgo que:

- Realizar mediciones definidas del riesgo
- Son transparentes en cuanto a los supuestos, las variables y los resultados
- Mostrar las probabilidades de pérdida específicas en términos financieros

Las mediciones, las fórmulas, los supuestos, las variables y los resultados deben ser transparentes para poder ser discutidos, defendidos y modificados. Dado que gran parte del modelo FAIR se define en términos empresariales y financieros, los ejecutivos, los directores de línea de negocio y otras partes interesadas pueden aprender a hablar el mismo idioma para clasificar los activos, las amenazas y las vulnerabilidades de la misma manera.



SUGERENCIA

Siempre que sea posible, incorpore en su modelo de riesgo probabilidades específicas sobre pérdidas futuras. Las probabilidades específicas permiten a los gestores de riesgos y a los altos ejecutivos debatir el modelo y las posibles formas de mejorarlo, tras lo cual aumentará su confianza en el modelo y en las recomendaciones que de él se deriven.

¿Qué declaración es más útil?

“La amenaza de los ataques DDoS para nuestro negocio ha pasado de alta a media (de rojo a amarillo).”

O

“Hay un 20 % de probabilidades de que nuestro negocio sufra una pérdida de más de 300 000 dólares en los próximos 12 meses porque un ataque de denegación de servicio distribuido (DDoS) interrumpa la disponibilidad de nuestros sitios web de cara al cliente.”

Inteligencia y probabilidades de amenaza

Como se muestra en la parte izquierda de la Figura 8-1, una parte importante de la creación de un modelo de amenaza implica la estimación de la probabilidad de ataques exitosos (o “frecuencia de eventos de pérdida” en el lenguaje del marco FAIR).

El primer paso es crear una lista de categorías de amenazas que puedan afectar a la empresa. Esta lista suele incluir malware, ataques de phishing, kits de exploits, ataques de día cero, exploits de aplicaciones web, ataques DDoS, ransomware y muchas otras amenazas.

El siguiente paso es mucho más difícil: Estimar las probabilidades de que los ataques se produzcan y de que tengan éxito (es decir, las probabilidades de que la organización contenga vulnerabilidades relacionadas con los ataques y los controles existentes no sean suficientes para detenerlos).

PRECAUCIÓN



Evite el siguiente escenario: Un miembro del equipo de GRC (gobernanza, riesgo y cumplimiento) pregunta a un analista de seguridad: “¿Cuál es la probabilidad de que nos enfrentemos a este ataque en particular?” El analista de seguridad (que realmente no puede ganar) piensa durante 30 segundos en la experiencia pasada y los controles de seguridad actuales y hace una conjetura salvaje: “No sé, tal vez el 20 %”.

Para no parecer despistado, su equipo de seguridad necesita respuestas mejor informadas. La inteligencia permite responder a preguntas como:

- ¿Qué actores de la amenaza están utilizando este ataque, y se dirigen a nuestra industria?
- ¿Con qué frecuencia se ha observado recientemente este ataque específico en organizaciones como la nuestra?
- ¿La tendencia es al alza o a la baja?
- ¿Qué vulnerabilidades aprovecha este ataque y están presentes en nuestra organización?
- ¿Qué tipo de daños, técnicos y financieros, ha causado este ataque en organizaciones como la nuestra?

Los analistas de amenazas siguen necesitando saber mucho sobre la organización y sus defensas de seguridad, pero la inteligencia sobre amenazas enriquece su conocimiento de los ataques, los actores que están detrás de ellos y sus objetivos. También proporciona datos concretos sobre la prevalencia de los ataques.

Las figuras 8-2 y 8-3 muestran algunas de las formas que puede adoptar la inteligencia. La figura 8-2 enumera los tipos de preguntas sobre una muestra de malware que una solución de inteligencia responde para los analistas.

The screenshot shows a digital interface for analyzing a cyber attack. At the top, it says "Samsam Cyber attack". Below that are two buttons: "Add Reference to List..." and "Share Event" on the left, and "Report as Inaccurate" and "Hide This Event" on the right. A horizontal line separates this from a list of questions. The questions are:

- Who is reported together with Samsam?
- What attackers are using Samsam?
- Who is targeted using Samsam?
- What operations are reported with Samsam?
- What technical indicators are related to Samsam?
- Which authors are reporting about Samsam?

Figura 8-2: Preguntas sobre una muestra de malware a las que responde una solución de inteligencia. (Fuente: Recorded Future)

La Figura 8-3 muestra las tendencias en la proliferación de las familias de ransomware. La línea de tendencia a la derecha de cada familia de ransomware indica el aumento o la disminución de las referencias a través de una gran variedad de fuentes de datos sobre amenazas, como repositorios de código, sitios de pasta, blogs de investigación de seguridad, foros clandestinos y foros .onion (accesibles por Tor). Puede haber información adicional sobre cómo las familias de ransomware se conectan con los actores de la amenaza, los objetivos y los kits de exploits.



Figura 8-3: Línea de tiempo que muestra la proliferación de nuevas familias de ransomware. (Fuente: Recorded Future)

La inteligencia y el coste financiero de los ataques

El otro componente principal de las fórmulas de nuestro modelo es el coste probable de los ataques con éxito. La mayor parte de los datos para estimar los costes probablemente procedan del interior de la organización. Sin embargo, la inteligencia sobre amenazas proporciona puntos de referencia útiles sobre temas como:

- El coste de ataques similares a organizaciones del mismo tamaño y del mismo sector
- Los sistemas que necesitan ser remediados después de un ataque, y el tipo de remediación que requieren

Hablaremos más de la gestión de riesgos en el capítulo 15, incluyendo el marco de Riesgo de Categoría de Amenaza (TCR) que fue desarrollado por Levi Gundert de Recorded Future, y se explica en detalle en su libro, “*El negocio del riesgo, lo que los CISO necesitan saber sobre la ciberseguridad basada en el riesgo.*”

Capítulo 9

Inteligencia de terceros

En este capítulo

- Explorar el impacto del aumento del riesgo de terceros y comprender por qué la evaluación estática de ese riesgo se queda corta
- Conozca los principales riesgos que debe vigilar
- Vea por qué el uso de inteligencia automatizada en tiempo real es la mejor manera de mitigar el riesgo de terceros

El riesgo de terceros se cierne sobre nosotros

Dado que las empresas y sus cadenas de suministro están tan estrechamente integradas, es fundamental tener en cuenta la seguridad de sus socios, proveedores y otros terceros al evaluar el perfil de riesgo de su propia organización.

Una encuesta reciente del Instituto Ponemon, “[transformación digital y ciberriesgo: lo que debe saber para estar seguro](#),” descubrió que el 55 % de las organizaciones han sufrido una brecha originada por un tercero, y solo el 29 % cree que sus socios les notificarían un compromiso. En la Figura 9-1 se muestran las estadísticas correspondientes.

Third-Party Risk Is Real



Figura 9-1: La mayoría de las organizaciones están expuestas a importantes riesgos a través de sus relaciones con terceros. (Fuente: Ponemon Institute)

La escritura está en la pared: Los ataques de terceros seguirán aumentando y empeorando, complicarán aún más la gestión de los riesgos cibernéticos y sus socios probablemente no le contarán sus problemas más críticos.

Los métodos tradicionales de evaluación de riesgos por parte de terceros se basan en resultados estáticos, como autoevaluaciones, auditorías financieras, informes mensuales sobre nuevas vulnerabilidades descubiertas en los sistemas que utiliza una organización e informes ocasionales sobre el estado de cumplimiento de los controles de seguridad. Sin embargo, las evaluaciones estáticas se quedan obsoletas rápidamente, porque no reflejan la naturaleza dinámica de un negocio cambiante. En resumen, no tienen la información que necesitan para tomar decisiones informadas sobre la gestión de los riesgos de terceros para su organización.

En cambio, la inteligencia en tiempo real sobre terceros le permite evaluar con precisión el riesgo que suponen esas organizaciones y mantener las evaluaciones actualizadas a medida que cambian las condiciones y surgen nuevas amenazas.

Las evaluaciones de riesgo tradicionales se quedan cortas

Muchas de las prácticas de gestión de riesgos de terceros más comunes que se emplean hoy en día van por detrás de los requisitos de seguridad. Las evaluaciones estáticas del riesgo, como las auditorías financieras y las verificaciones de los certificados de seguridad, siguen siendo importantes, pero a menudo carecen de contexto y oportunidad.

Las organizaciones que siguen los enfoques tradicionales para gestionar el riesgo de terceros suelen utilizar estos tres pasos:

1. Intentan comprender la relación comercial de su organización con un tercero y cómo expone a su organización a las amenazas.
2. A partir de ese conocimiento, identifican los marcos para evaluar la salud financiera del tercero, los controles corporativos y la seguridad e higiene de las TI, así como la forma en que estos factores se relacionan con el enfoque de seguridad de su propia organización.

3. Utilizando esos marcos, evalúan al tercero para determinar si cumple con las normas de seguridad como SOC 2 o FISMA. A veces realizan una auditoría financiera del tercero.

Aunque estos pasos son esenciales para evaluar el riesgo de terceros, no lo dicen todo. Los resultados son estáticos y no pueden reflejar las condiciones rápidamente cambiantes y las amenazas emergentes. El análisis es a menudo demasiado simplista como para producir recomendaciones prácticas. A veces, el informe final es opaco, lo que impide profundizar en la metodología del análisis. Todos estos factores crean puntos ciegos que dejan a los responsables de la toma de decisiones sin saber si se han pasado por alto elementos de información cruciales.



A la hora de evaluar el riesgo de terceros, no se debe confiar únicamente en los cuestionarios de autoinforme o en la visión interna de un proveedor sobre sus propias defensas de seguridad. Completa todo esto con una perspectiva externa e imparcial sobre el panorama de amenazas del proveedor.

Un experimento mental

Imagínese que ha seguido los pasos tradicionales de una evaluación de riesgos, tal y como se ha descrito anteriormente. Ha llegado a la conclusión de que es seguro trabajar con un proveedor de su cadena de suministro.

Ahora, este proveedor experimenta un ataque de ransomware que

puede o no haber expuesto los datos internos de su organización. ¿Cuánto tiempo tardaría su proveedor en revelar el ataque? ¿Es capaz de determinar con precisión qué medidas de seguridad proactivas debe tomar, si es que debe tomar alguna, y con qué rapidez debe actuar?

Qué buscar en la inteligencia de terceros

Para evaluar con precisión el riesgo de terceros en tiempo real, se necesita una solución que ofrezca un contexto inmediato sobre el panorama actual de las amenazas. La inteligencia de terceros proporciona indicadores de riesgo críticos que le permiten determinar qué deficiencias en las defensas de sus socios de la cadena de suministro representan riesgos significativos para su

organización. En ellos se incluyen no solo los riesgos actuales presentes en el momento de la evaluación, sino también una visión histórica, lo que proporciona aún más información para detectar, prevenir y resolver los riesgos.

Para evaluar eficazmente el riesgo de terceros, una solución de inteligencia de terceros debe ofrecer:

1. Acceso a una amplia gama de datos sobre riesgos procedentes de la open web, la dark web y fuentes técnicas
2. Automatización y análisis para clasificar de forma rápida y exhaustiva los datos masivos en una puntuación de riesgo fácilmente consumible con recomendaciones procesables
3. Pruebas transparentes para agilizar el análisis y la reducción de riesgos
4. Alertas en tiempo real sobre cambios y nuevos riesgos
5. Visibilidad continua de los entornos en constante cambio de sus socios

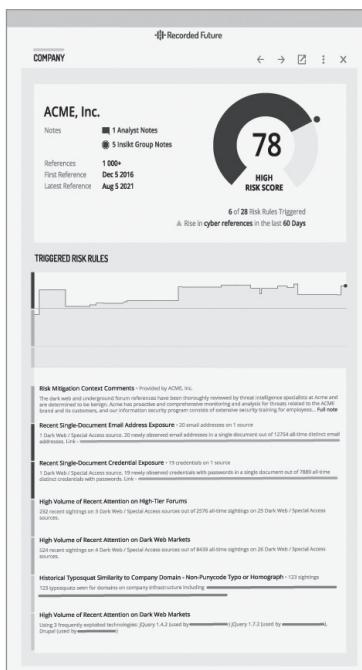


Figura 9-2: La inteligencia de terceros proporciona un contexto para identificar las deficiencias en las defensas de los socios de la cadena de suministro. (Fuente: Recorded Future)

Supervise a los terceros en relación con estos cinco riesgos críticos

Ransomware

Los ataques de ransomware han crecido dramáticamente en alcance e impacto. Algunos ataques recientes han perturbado sectores enteros de la economía estadounidense. Un ataque al sistema de oleoductos Colonial en mayo de 2021 provocó el caos en las gasolineras y los automovilistas y problemas importantes en las refinerías, las aerolíneas y otras industrias que producen y consumen combustible. Ese mismo mes, un atentado contra el procesador de carne JBS puso en jaque a grandes segmentos de la industria ganadera y de la restauración.

En julio de 2021 salió a la luz un ejemplo de riesgo de terceros aún más atroz a escala mundial. El grupo de ciberdelincuentes REvil infectó el software de Kaseya, una empresa que ofrece una solución para gestionar estaciones de trabajo y servidores en ubicaciones remotas. La mayoría de los aproximadamente 60 clientes de Kaseya comprometidos eran proveedores de servicios gestionados. Como cada proveedor de servicios accedía a las redes de muchos clientes, REvil pudo lanzar ataques de ransomware contra más de 1500 empresas de todo el mundo, y afirmó haber cifrado archivos en más de un millón de sistemas.

Recientemente, las organizaciones de ciberdelincuentes que están detrás de muchas campañas de ransomware han añadido una nueva arma a su caja de herramientas: “el ransomware de doble extorsión”. En los ataques de ransomware de doble extorsión, antes de que el malware cifre los datos de los sistemas de la víctima, exfiltra las copias a servidores controlados por los ciberdelincuentes. A continuación, los atacantes publican muestras de la información sensible de la víctima en un sitio web de extorsión de ransomware, junto con las demandas de rescate y las instrucciones de pago. La amenaza de exponer la propiedad intelectual o los datos financieros y de clientes sensibles da a los ciberdelincuentes aún más ventaja en las negociaciones del rescate.

Si uno de sus socios se ve afectado por un ataque de ransomware de doble extorsión, eso es definitivamente una mala noticia para ellos. Sin embargo, hay un resquicio de esperanza para usted. Si supervisa los sitios web de extorsión de ransomware, recibirá un aviso temprano de que el socio ha sido comprometido. Cuando esto ocurre, puedes:

- Evaluar la naturaleza de su relación con la organización y determinar qué tipo de respuesta es necesaria
- Notifique a su socio para que pueda determinar qué sistemas se han visto afectados y aislarlos
- Cambiar las credenciales o cortar el acceso a la VPN para asegurar que el atacante no pueda acceder a sus sistemas
- Identifique el tipo de malware utilizado contra el tercero y asegúrese de que sus defensas pueden contrarrestarlo
- Cambie a una fuente alternativa para garantizar la continuidad del negocio en caso de que las operaciones de su socio se vean afectadas

La rapidez de respuesta es fundamental. Si puede actuar mientras las negociaciones entre el atacante y la víctima todavía están en marcha, puede ser capaz de endurecer sus defensas antes de que los atacantes dirijan su atención hacia usted.

Filtración de datos

¿Y si sus socios externos tardan en informarle sobre los incidentes de seguridad? ¿Y si tardan semanas o meses en darse cuenta de que han sido vulnerados?

No tiene que permanecer en la oscuridad. Los sitios web en la open web y la dark web pueden proporcionar pruebas de que sus socios han sido comprometidos. Estas pruebas incluyen documentos de diseño y otra propiedad intelectual, información personal identificable sobre clientes y empleados, código de software propietario y credenciales e información técnica sobre los sistemas de información de los socios. La información puede aparecer en mercados de la dark web y en foros de hackers, sitios de pasta y repositorios de código.

Además, muchas infracciones se divultan en sitios de noticias en la open web y en los medios sociales. Por supuesto, es posible que necesite amplios conocimientos lingüísticos para aprovechar estos recursos.

Si encuentra alguno de estos indicadores de que un socio ha sido comprometido, puede:

- Informar a su interlocutor para que contenga el ataque y determine las causas de fondo

- Trabajar con el socio para descubrir si alguno de sus datos se perdió en la brecha
- Reevaluar los términos de su relación con el socio y, si es necesario, exigirle que mejore sus controles y procesos de seguridad

Actividad maliciosa en la red

Los modelos de ciberamenazas como el Lockheed Martin Cyber Kill Chain® ilustran que los ciberataques avanzados implican mucha comunicación en red entre los sistemas controlados por el atacante y las organizaciones objetivo. Los actores de la amenaza utilizan servidores y bots para enviar correos electrónicos de phishing que contienen malware o enlaces a sitios web falsos que capturan credenciales. El malware y los scripts plantados en la red del objetivo crean canales de comando y control (C&C) para intercambiar información sobre el entorno de la víctima e instrucciones sobre cómo encontrar y recopilar datos sensibles. Como paso final, los datos capturados se exfiltran a los servidores del atacante.

Muchos de los servidores y bots utilizados por los adversarios son “malos conocidos”. Es decir, durante las investigaciones de ataques anteriores sus direcciones IP han sido asociadas a actividades maliciosas o sospechosas. Estas direcciones IP han sido recopiladas y publicadas por proveedores de ciberseguridad, consorcios industriales y agencias gubernamentales, y muchas empresas bloquean el tráfico web entre ellas y su propio entorno.

Pero, ¿qué pasa con la supervisión del tráfico de red de sus proveedores, contratistas, proveedores de servicios y otras personas que tienen acceso a sus sistemas? La actividad maliciosa de la red permite conocer los ataques planificados y en curso contra terceros. Si encuentra estos indicadores puede:

- Registrar las direcciones IP maliciosas y compartirlas con su socio, para que pueda bloquear el tráfico a los sitios web maliciosos
- Trabajar con el socio para determinar si ya han sido comprometidos y mejorar sus controles para detener el spam, el malware y el tráfico de C&C
- Cambiar las credenciales del socio para sus sistemas

- Compruebe que ha bloqueado el tráfico de sus propias redes hacia los sitios web maliciosos y que sus defensas pueden contrarrestar los ataques que se utilizan contra el socio

Credenciales expuestas

Usted da a los socios credenciales para que puedan integrar sus operaciones con las suyas. Pero las credenciales son literalmente “las llaves del reino”. Los actores de amenazas que obtienen credenciales para uno de los sistemas de información de su socio tienen el poder de robar su información que reside allí, cerrar las operaciones del socio y hacerse pasar por él para acceder a sus sistemas. Dado que las credenciales son tan valiosas, muchos atacantes hacen un esfuerzo especial para encontrarlas y exfiltrarlas durante las violaciones de datos.

Lo que nos lleva a otro ejemplo de dark clouds con un lado positivo.

Los ciberdelincuentes han creado una economía de nicho para comprar y vender credenciales. Algunos hackers se especializan en la adquisición de credenciales a través de ataques de phishing, keyloggers y otros programas maliciosos, ingeniería social, y spraying de contraseñas (prueba de fuerza bruta de contraseñas comunes). Algunas filtraciones de datos dirigidas principalmente a la propiedad intelectual o a la información personal arrasan con las credenciales al mismo tiempo. En ambos casos, los atacantes pueden utilizar los mercados de la dark web para vender las credenciales robadas a otros ciberdelincuentes especializados en ataques avanzados. Los vendedores suelen proporcionar información sobre las organizaciones específicas que emitieron las credenciales.

Estos mercados de la dark web hacen más eficiente la ciberdelincuencia. Sin embargo, puedes vigilar los foros y mercados de la dark web, así como los sitios de pasta, los sitios de descarga y otros lugares donde se exponen las credenciales robadas. Si encuentra credenciales que dan acceso a uno de sus socios, puede hacerlo:

- Ofrezca sus hallazgos al socio para que pueda desactivar las cuentas con las credenciales robadas
- Cambiar las credenciales del socio para sus sistemas
- Ayudar al socio a analizar cómo se robaron las credenciales y cómo se pueden prevenir robos similares

- Trabajar con el socio para determinar si las credenciales robadas se están utilizando en un ataque en curso, y si es necesario ayudarles a contener el ataque

Tramar en la dark web

En la dark web, los ciberdelincuentes y los piratas informáticos se comunican y hacen negocios de forma anónima (y, para ser justos, también lo hacen los periodistas y los disidentes que viven bajo gobiernos represivos). Los usuarios de la dark web suelen esconderse detrás de apodos (“handles”) para ocultar su identidad y utilizan navegadores y redes TOR para ofuscar sus direcciones IP. Muchos foros y mercados de la dark web implementan el equivalente digital de una línea de cuerda de un club nocturno con un portero: los posibles miembros son rechazados a menos que hayan sido invitados o puedan pasar una prueba.

Los actores de las amenazas suelen utilizar los foros de la dark web para planificar los ataques y reclutar a otros ciberdelincuentes, y a veces a personas corruptas de la empresa, para que les ayuden. Los actores con motivaciones políticas y los “hacktivistas” utilizan a veces los mismos foros para justificar sus acciones o presumir de sus proezas. Los participantes en estos foros suelen nombrar sus objetivos.

Si supervisa los foros de la dark web, puede descubrir conspiraciones contra sus socios (así como contra su empresa). La observación de la actividad en estos foros proporciona una alerta temprana de los ataques e información sobre las tácticas, técnicas y procedimientos que se utilizarán.

Con esta información puede:

- Avise a sus socios para que puedan configurar o mejorar sus defensas para frustrar las tácticas y técnicas de los atacantes
- Asegúrese de que sus defensas son capaces de proteger contra los mismos ataques
- Notificar a las fuerzas del orden para que puedan eliminar o impedir a los actores de la amenaza

Respuesta a las puntuaciones de riesgo elevadas de terceros

¿Qué hacer cuando se enfrenta a puntuaciones de alto riesgo para un tercero? No todas las violaciones de datos justifican el cese de los negocios con ese socio. Casi todas las organizaciones se enfrentan a ciberataques y tiempos de inactividad inesperados, y los socios no son una excepción. Lo más importante es la forma en que ellos (y usted) afrontan los incidentes y toman medidas para reducir los riesgos futuros.

Un cambio en las puntuaciones de riesgo puede suponer una oportunidad para hablar con sus socios comerciales sobre su enfoque de la seguridad. Por su parte, es importante examinar más detenidamente si las reglas de riesgo que se activaron afectarán a la red de su organización. Por ejemplo, la puntuación de riesgo de un socio puede aumentar porque se han descubierto sitios web de typosquatting muy parecidos a los sitios web legítimos operados por el socio. Poner esos sitios en la lista de denegación en su propia red es una forma de frustrar las campañas de phishing mientras investiga qué medidas piensa tomar ese socio para proteger su identidad de marca.

Para tomar decisiones de seguridad inteligentes que impliquen a sus terceros, necesita un contexto actualizado y pruebas proporcionadas por la inteligencia de terceros.

Capítulo 10

Inteligencia de marca

En este capítulo

- Revisar las múltiples formas de riesgo digital para las marcas
- Conozca cómo la inteligencia identifica y remedia los ataques contra las marcas en línea

La protección de la marca implica salvaguardar la imagen, la reputación y los clientes de una organización frente a ataques que, en principio, nunca llegan a su red o sistemas. La mayoría de las organizaciones carecen de visibilidad sobre este tipo de ataques. Las amenazas incluyen:

- Sitios web y cuentas de redes sociales falsos utilizados para suplantar la identidad de la organización o de sus empleados con fines de fraude y ataques de suplantación de identidad
- Contenido malicioso e información falsa sobre la organización y sus productos publicada en sitios web y plataformas de medios sociales
- Productos y programas informáticos falsificados ofrecidos en mercados digitales y tiendas de aplicaciones
- Filtraciones de datos y credenciales de empleados y ejecutivos

La mayoría de estas amenazas provienen de delincuentes con motivaciones financieras, pero también pueden implicar a hacktivistas, clientes insatisfechos, competidores y empleados descuidados o descontentos que revelan información en línea.

Proteja su marca y a sus clientes

Para proteger realmente su marca, debe preocuparse por las amenazas que la aprovechan para perjudicar o influir en sus clientes. Los clientes que son atraídos a una estafa o fraude desde una imitación de su sitio web pueden hacer responsable a su organización. Los que compran una versión falsificada y de baja calidad de su producto en un mercado en línea pueden perder la confianza en su marca. Quienes piensen que uno de sus ejecutivos ha publicado contenido ofensivo en la web pueden boicotear sus productos, aunque no haya sido su ejecutivo quien lo haya publicado. Alegar “no fue nuestra culpa” no restablecerá su confianza ni tu reputación en ninguno de estos escenarios.

Un tipo diferente de detección

La mayoría de las actividades que hemos estado discutiendo en este manual implican la creación de inteligencia sobre los atacantes y sus herramientas. La inteligencia de marca también incluye algo de eso, pero el énfasis está en detectar el nombre y la marca de su organización en todos los lugares en los que aparecen en Internet.

Debe ser riguroso a la hora de enumerar y buscar las menciones de todos los nombres de sus marcas y productos, así como las palabras clave que se asocian a ellos. Estos incluyen los nombres de:

- Su organización matriz
- Filiales y unidades de negocio
- Productos
- Ejecutivos
- Directivos y empleados que se relacionan con el público en foros web y a través de las redes sociales

También incluye los logotipos, las marcas comerciales, las marcas de servicio y los eslóganes publicitarios que aparecen en los sitios web autorizados de su organización, ya que se utilizan con frecuencia en sitios web falsos.

Descubrimiento de pruebas de suplantación y abuso de marca

Saber lo que hay que buscar le permite encontrar pruebas de suplantación de identidad y de abuso de la marca en lugares en los que muchas organizaciones nunca buscan. Por ejemplo, una solución de inteligencia de marca le permite:

- Busque en los registros de dominios para encontrar nombres de dominio que incluyan el nombre de su organización o producto, o variaciones de los mismos
- Rastree la web para encontrar dominios con typosquatting
- Supervise las redes sociales para que le avisen de los hashtags que incluyan el nombre de su organización o producto, o variaciones de los mismos
- Escanee las redes sociales para detectar las cuentas que dicen pertenecer a su organización, a sus ejecutivos o a sus empleados
- Compruebe las tiendas de aplicaciones para descubrir aplicaciones móviles no autorizadas que utilicen su marca
- Rastree los foros de la web en busca de actores de amenazas que planeen suplantar su marca

Caso práctico: La “typosquatting” y los dominios fraudulentos

La “typosquatting” consiste en manipular los caracteres del nombre de dominio de una organización en dominios casi idénticos. Por ejemplo, los actores de la amenaza que tienen como objetivo example.com podrían crear una URL typosquat de example.com. Los atacantes suelen registrar miles de dominios que difieren en un solo carácter de las URL de sus organizaciones objetivo. Lo hacen por razones que van desde lo sospechoso hasta lo totalmente malicioso.

Los sitios web fraudulentos que utilizan estos nombres de dominio modificados se construyen para que parezcan sitios web legítimos. Los dominios y sitios web falsos se utilizan a menudo en campañas de spear-phishing contra empleados o clientes, ataques de watering-hole y ataques de drive-by download.

Estar alerta en tiempo real de los nuevos dominios registrados de phishing y typosquatting es la mejor manera de reducir la ventana de oportunidad para que los actores de la amenaza se hagan pasar por su marca y estafen a los usuarios desprevenidos. Una vez identificada la infraestructura maliciosa, podrá emplear un servicio de eliminación para anular la amenaza.

Descubrir pruebas de infracciones en la web

Al supervisar la web, incluidos los foros privados de la dark web, las soluciones de inteligencia de marca le permiten descubrir pruebas de violaciones de datos dentro de su organización y su ecosistema de socios. Puede encontrar:

- Los nombres y datos de sus clientes
- Datos de cuentas financieras y números de la Seguridad Social
- Filtración o robo de credenciales de sus empleados
- Pegar y tirar a la papelera los sitios que contienen su código de software propietario
- Foros en los que se menciona a su organización y se anuncian las intenciones de atacarla
- Foros de venta de herramientas y discusión de técnicas para atacar a organizaciones como la suya

El descubrimiento oportuno de estos indicadores le permite:

- Asegurar las fuentes de los datos
- Encuentre y solucione las vulnerabilidades y desconfiguraciones de su infraestructura
- Mitigar los riesgos futuros mejorando los controles de seguridad
- Identificar formas de mejorar la formación de los empleados y las prácticas de codificación
- Permita que sus equipos de SecOps y de respuesta a incidentes reconozcan los ataques más rápidamente



A menudo es posible acotar el origen de una filtración observando exactamente qué información y artefactos se encuentran en la web, dónde se encuentran y qué otras cosas se encuentran en el mismo lugar. Por ejemplo, si encuentra diseños de productos o códigos de software en un sitio de dark web y reconoce que fueron compartidos solo con unos pocos proveedores, sabrá que debe investigar los controles de seguridad de esos proveedores como parte de su programa de gestión de riesgos de terceros. Si el nombre de su organización ha sido mencionado en un foro clandestino cuyos miembros son conocidos por atacar ciertas aplicaciones, podría aumentar la protección de las aplicaciones objetivo parcheando los sistemas en los que se ejecutan, supervisándolos más de cerca y añadiendo controles de seguridad.

Caso práctico: Datos comprometidos

Los actores de las amenazas ganan dinero con muchos tipos de información personal y propiedad intelectual corporativa comprometida. Entre los ejemplos de datos comprometidos a la venta en la dark web se encuentran los historiales médicos, las tarjetas de regalo clonadas y comprometidas, y las credenciales robadas para “pagar” servicios como los proveedores de streaming de música o las aplicaciones de transporte, y los artículos cobrados a través de los proveedores de pago en línea, como se ilustra en la figura 10-1.

Figura 10-1: Datos comprometidos: credenciales de un servicio de streaming de música en línea reveladas en la dark web. (Fuente: Recorded Future)

Un alto porcentaje de las infracciones relacionadas con la piratería informática aprovechan las contraseñas robadas o débiles. Los actores de las amenazas suben regularmente cachés masivos de nombres de usuario y contraseñas a sitios de pasta y a la dark web, o los ponen a la venta en mercados clandestinos. Estos volcados de datos pueden incluir direcciones de correo electrónico y contraseñas corporativas, así como datos de acceso a otros sitios.

La supervisión de fuentes externas para este tipo de información aumentará drásticamente su visibilidad, no solo de las credenciales filtradas, sino también de las posibles violaciones de los datos corporativos y del código propietario.

La desinformación es alarmantemente sencilla y barata

Difundir mentiras sobre una organización en la web es fácil y barato. Como ejercicio de aprendizaje, el Insikt Group® de Recorded Future utilizó un proveedor de servicios de desinformación para lanzar una campaña negativa contra una empresa ficticia por solo 4200 dólares.

El ejercicio

El Grupo Insikt creó una empresa ficticia. A continuación, encontró a dos proveedores de servicios de desinformación en foros clandestinos de habla rusa y les encargó que generaran narrativas intencionadamente falsas en la red. A uno se le pidió que creara propaganda positiva para que la empresa pareciera atractiva. El otro fue encargado de difundir material malicioso acusando a la misma empresa de prácticas comerciales poco éticas.

Los resultados

El Grupo Insikt descubrió que lanzar campañas de desinformación es alarmantemente sencillo y barato. Ambas campañas de desinformación produjeron resultados en menos de un mes por solo unos pocos miles de dólares: 1850 dólares para el esfuerzo de propaganda positiva

y 4200 dólares para la campaña de desinformación negativa. Los proveedores de servicios difundieron sus mensajes con éxito colocando artículos en sitios web de renombre y creando cuentas en las redes sociales de personas aparentemente reales.

Las conclusiones

- Los servicios de desinformación están disponibles públicamente en foros clandestinos.
- Por unos pocos miles de dólares, los proveedores de servicios de desinformación publican artículos en medios de comunicación que van desde sitios web dudosos hasta medios de comunicación de renombre.
- Estos proveedores de servicios utilizan una combinación de cuentas de redes sociales establecidas y nuevas para propagar contenidos sin activar los controles de moderación de contenidos.

Conozca los métodos utilizados por los proveedores de servicios de desinformación en el informe de análisis de ciberamenazas del Grupo Insikt: “[El precio de la influencia: Desinformación en el sector privado](#).”

Cualidades críticas para las soluciones de inteligencia de marca

Por supuesto, mitigar el riesgo digital para su marca no es simplemente una cuestión de tropezar con un dominio de typosquatting o con algún dato aislado robado. Alguien, o algo, tiene que hacer el trabajo más amplio de recopilar masas de datos, tamizar miles de puntos de datos, analizar las relaciones entre los puntos de datos, decidir las prioridades y, finalmente, tomar medidas.

El mejor enfoque es utilizar una solución de inteligencia de marca que:

- Recoge y escanea datos de la más amplia gama y variedad de fuentes:** La automatización en la fase de recogida de datos ahorra a los analistas un tiempo precioso. Las mejores soluciones recopilan datos no solo de fuentes de open web, sino también de la dark web y de fuentes técnicas.
- Traza, supervisa y puntúa el riesgo de las marcas:** Mediante la automatización, la ciencia de datos avanzada y las técnicas analíticas como el procesamiento del lenguaje natural, las herramientas eficaces de inteligencia de marca permiten a los analistas vincular los atributos empresariales con los activos digitales relacionados y detectar, puntuar y priorizar los eventos relacionados con el riesgo de la marca.
- Coordina la reparación:** Las sólidas soluciones de inteligencia de marca generan alertas e informes que proporcionan información sobre cómo solucionar los problemas. Las alertas actualizan automáticamente a los equipos de seguridad o de marketing cuando surge nueva información. Las soluciones también ofrecen servicios para acabar con varios tipos de ataques a la marca.

Caso práctico: La derrota de la tipografía en un gran proveedor de soluciones de recursos humanos

Un gran proveedor de servicios de recursos humanos, salud y prestaciones patrimoniales permite a otras organizaciones gestionar sus recursos humanos. Esta empresa maneja mucha información personal identificable (PII), incluyendo datos sensibles de salud y financieros. Para proteger esos datos, cuentan con un amplio centro de operaciones de seguridad, que ofrece supervisión 24/7/365, respuesta a incidentes, investigación y análisis forense, y mucho más.

Su vicepresidente de operaciones de seguridad dice que en un momento dado se necesitaba un equipo de unas 100 personas para gestionar estas funciones. Con Recorded Future, se necesitan 10. “Obtener una lista de todas las menciones de nuestra empresa en Internet al final del día era totalmente inviable, aunque tuviera 10 o 20 personas trabajando en ello”, dice el vicepresidente.

El vicepresidente añade: “Seguro que podríamos gastar mucho dinero para que la gente tenga cuentas de quemador y acceso a estos espacios privados, pero iqué desperdicio! Cualquier cosa más allá de dos personas no tiene sentido en comparación con el uso de Recorded Future. El coste es inferior a dos personas, frente a las 10 o 20 que necesitaría para intentar hacer algo similar.”

Por ejemplo, una mañana saltó una alerta sobre un posible dominio de typosquatting. La alerta se activó gracias a una regla de supervisión que el equipo había configurado en Recorded Future para buscar dominios fraudulentos que se parecieran a los de la organización. El registro de estos dominios suele ser el primer paso en un ataque de phishing.

En cuanto el equipo recibió la alerta, investigó y encontró intentos de phishing dirigidos a su organización y a algunos de sus clientes. Inmediatamente enviaron un informe flash a toda su organización y a todos sus clientes y socios. El informe ofrecía recomendaciones prácticas sobre cómo contrarrestar el ataque: Bloquee el dominio en su proxy y utilice los registros de eventos para buscar la amenaza con su SIEM. Muchos de sus socios informaron de visitas al sitio, pero pudieron bloquear el acceso antes de que se produjera ningún daño.

Gracias a la inteligencia de marca en tiempo real, la empresa pudo mitigar la amenaza en cuestión de horas, en lugar de semanas, o nunca.

Capítulo 11

Inteligencia geopolítica

En este capítulo

- Comprender los factores que provocan el riesgo geopolítico
- Descubra todos los grupos que utilizan la inteligencia geopolítica
- Explorar los tipos de eventos de geofencing y riesgo geopolítico

¿Qué es el riesgo geopolítico?

El riesgo geopolítico es la exposición al riesgo derivado de los cambios en las tendencias globales estratégicas y tácticas en cada región geográfica que podrían afectar a su organización.

Piense en un país o ciudad donde su organización tenga una oficina o unas instalaciones como una fábrica, una oficina, un almacén, o quizás una clínica, un consulado o una base militar. Las operaciones de esa instalación podrían verse afectadas por:

- Decisiones y acciones de los órganos y organismos gubernamentales: desde la aprobación de leyes, pasando por la introducción de reglamentos, hasta la movilización de fuerzas policiales o militares en estado de emergencia.
- Acciones de partidos políticos, sindicatos, grupos de activistas y otras organizaciones, como huelgas, manifestaciones, protestas, boicots, campañas en las redes sociales e incluso disturbios y ataques selectivos contra lugares y propiedades.
- Catástrofes naturales o provocadas por el hombre, como brotes de enfermedades, huracanes y terremotos, acciones militares y atentados terroristas

Los efectos de estos sucesos van desde interrupciones temporales, pasando por millones de dólares en costes directos e indirectos, hasta la pérdida de vidas.

Alto impacto

Una reciente encuesta realizada a organizaciones mundiales con ingresos de 250 millones de dólares o más reveló que más del 90 % de los ejecutivos de todo el mundo creen que su empresa se ha visto afectada por riesgos políticos inesperados en los últimos 12 meses. Los cambios en las políticas comerciales e industriales están afectando a las decisiones operativas en áreas como la diversificación de la base de proveedores, la modificación de las estrategias de fusión y adquisición, el ajuste de la longitud de las cadenas de suministro y la evolución hacia la deslocalización cercana y la deslocalización. (Fuente: EY-Parthenon: “[La geoestrategia en la práctica 2021](#)”)

Los autores de una versión anterior del estudio (Geoestrategia en la

práctica 2020) destacaron cuatro tipos de riesgo político:

- Riesgos derivados de los conflictos entre países y los cambios en los sistemas internacionales
- Riesgos relacionados con el entorno político nacional, la estabilidad de los gobiernos e instituciones y la legislación
- Riesgos que surgen cuando los gobiernos cambian la normativa medioambiental, de salud y seguridad, del mercado financiero, etc.
- Riesgos creados por el activismo de grupos como los sindicatos y las organizaciones de consumidores

Inteligencia geopolítica

Consideré las ventajas de ser advertido días antes de que este tipo de eventos afecten a su organización, o de ser alertado en tiempo real cuando se produzcan. Ese conocimiento puede permitirle evitar que los sucesos afecten a su organización, o puede ponerle en situación de responder más rápidamente a la hora de mitigar sus efectos.

Además, la información sobre las actitudes locales y las tendencias a largo plazo le proporciona la información que necesita para tomar decisiones más inteligentes sobre la expansión de las operaciones en países y ciudades específicas.

Ubicación, ubicación, ubicación

La inteligencia geopolítica utiliza el ciclo de vida de la inteligencia descrito en el capítulo 3. La principal diferencia entre la inteligencia geopolítica y otros tipos de inteligencia para los equipos de seguridad es el punto de partida.

Las actividades de inteligencia para las operaciones de seguridad, la respuesta a incidentes, la gestión de vulnerabilidades, el análisis de amenazas y los equipos de riesgo de terceros se organizan principalmente en torno a las amenazas y los actores de las mismas. La inteligencia de marca se centra en nombres y palabras clave relacionados con las marcas y productos de la organización.

En cambio, la inteligencia geopolítica comienza con las ubicaciones geográficas y las tendencias geopolíticas, normalmente en las ciudades, países y regiones donde su organización tiene activos físicos e instalaciones. Su resultado son datos y conocimientos sobre los acontecimientos específicos de cada lugar que tienen un impacto potencial en las operaciones de esas instalaciones y en el personal de las mismas.

Cadenas de suministro, clientes y riesgo geopolítico

El riesgo geopolítico no se limita a las oficinas e instalaciones de su organización. Como se ilustra en 2020 y 2021, durante la pandemia de COVID-19, las interrupciones que afectan a los socios de la cadena de suministro y las redes de transporte también tienen un efecto dramático en las operaciones de una organización. Esto es así incluso en regiones donde la organización no tiene activos físicos ni personal. Cuando los acontecimientos específicos de un lugar afectan a un gran número de sus clientes o consumidores, una organización puede sufrir las consecuencias.

¿Quién utiliza la inteligencia geopolítica?

La inteligencia geopolítica es valiosa para muchos grupos dentro de las organizaciones que son globales o que aspiran a expandirse globalmente. Los nombres de los grupos suelen variar según las organizaciones, pero pueden incluir los siguientes equipos:

- Seguridad física
- Operaciones de seguridad
- Seguridad mundial
- Continuidad de la actividad
- Gestión de la cadena de suministro

- Gestión de riesgos
- Relaciones con el gobierno
- Inteligencia estratégica
- Política pública o asuntos públicos
- Oficina del consejero general
- Gestión regional y nacional

Estos grupos tienen diversas responsabilidades relacionadas con los riesgos geopolíticos, entre ellas

- Anticipación y prevención de daños (por ejemplo, cierre de una instalación antes de una manifestación masiva)
- Responder rápidamente para mitigar los efectos de los acontecimientos (por ejemplo, proporcionar ayuda a los empleados o encontrar fuentes de suministro alternativas después de un desastre natural)
- Comunicar los datos clave a los empleados, clientes, socios comerciales y organismos gubernamentales
- Evaluar los riesgos de localización en el futuro para orientar las decisiones de inversión y expansión



Para sacar el máximo provecho de la inteligencia geopolítica, hay que consultar a estos grupos sobre sus necesidades de información, y utilizar esa aportación para establecer las prioridades de la recogida y el análisis de información. Adapte sus resultados para que sean fácilmente comprensibles y procesables por estos públicos. Véanse las secciones “Dirección” y “Difusión” del análisis del ciclo de vida de la inteligencia en el capítulo 3.

Recogida de datos con Geofencing

Para que su organización pueda anticiparse y hacer frente a los eventos específicos de cada lugar, tiene que empezar por seleccionar los lugares y tipos de eventos que son importantes para su organización. La solución de inteligencia geopolítica controlará y filtrará los datos por ubicación, lo que se denomina “geofencing”.



Si su organización cuenta con un departamento de seguridad física, seguridad global o continuidad del negocio, es probable que ese equipo mantenga una lista de todas las ubicaciones de sus oficinas e instalaciones en todo el mundo.



Profundice más allá de su lista de oficinas e instalaciones preguntando a los diferentes grupos de su organización sobre los socios de la cadena de suministro, las redes de transporte, los clientes y otras entidades que puedan afectar a sus operaciones. Documentar los lugares en los que podrían ser susceptibles de sufrir acontecimientos geopolíticos, y vigilarlos.

También es necesario especificar los tipos de eventos a supervisar. La figura 11-1 es un ejemplo de categorías de eventos geopolíticos de alto nivel y algunos de los elementos específicos que podrían ofrecerse dentro de una categoría.

Geo-political	
<input type="checkbox"/>	Protest
<input type="checkbox"/>	Military
<input type="checkbox"/>	Political
<input type="checkbox"/>	Environmental
<input type="checkbox"/>	Crime and Disasters
<input type="checkbox"/>	Arms and Nuclear
<input type="checkbox"/>	Political Relations
<input type="checkbox"/>	Calendar Event

Political	
<input checked="" type="checkbox"/>	Political
<input type="checkbox"/>	Coup
<input type="checkbox"/>	Election
<input type="checkbox"/>	Legislation
<input type="checkbox"/>	Political Endorsement
<input type="checkbox"/>	Political Event
<input type="checkbox"/>	Poll Result
<input type="checkbox"/>	Voting Result

Figura 11-1: Ejemplos de categorías de acontecimientos geopolíticos y los elementos específicos dentro de una categoría. (Fuente: Recorded Future)

Fuentes de datos e información

Las fuentes de datos e información utilizadas para producir inteligencia geopolítica se solapan con las utilizadas para otros tipos de inteligencia. Las fuentes técnicas, como las fuentes de amenazas, suelen desempeñar un papel menor en la inteligencia geopolítica, porque la mayoría de las ciberamenazas no son específicas de un lugar. Las fuentes de inteligencia geopolítica más valiosas suelen ser específicas de un país o ciudad, por ejemplo:

- Sitios web de noticias y medios de comunicación públicos de todo el mundo
- Publicaciones en las redes sociales
- Blogs
- Foros y mercados tanto en la open web como en la dark web

La mayoría de estas fuentes incluyen datos e información de gobiernos nacionales y locales, agencias reguladoras, organizaciones de medios de comunicación, sindicatos, grupos de consumidores y particulares. Sin embargo, los activistas y los delincuentes también utilizan la dark web para planificar actividades peligrosas e ilegales dirigidas a lugares específicos, lo que hace que las fuentes de la dark web sean valiosas para la inteligencia geopolítica.

Automatización, análisis y experiencia

Se necesita una enorme cantidad de trabajo para determinar qué sitios, y qué artículos, vídeos, mensajes y mensajes específicos son relevantes para una ubicación y un tipo de amenaza concretos. Por eso, las organizaciones que se toman en serio la gestión del riesgo geopolítico deben utilizar una plataforma de inteligencia que combine la analítica, la automatización y la experiencia humana para procesar y analizar los datos y la información.

La automatización reduce, y a menudo elimina, la investigación manual, que requiere muchos recursos y tiempo. También acelera los procesos de cálculo y actualización de las puntuaciones de riesgo, la difusión de alertas, la creación de representaciones visuales de los datos y muchas otras tareas.

La analítica es lo que permite a una solución de inteligencia recopilar millones de piezas de información procedentes de la open web, la dark web y las fuentes técnicas, y vincularlas y categorizarlas dinámicamente para generar inteligencia sobre lugares específicos y tipos de eventos geopolíticos. Gracias a la analítica, los analistas no necesitan peinar manualmente volúmenes masivos de contenido, descubrir patrones y conectar los puntos entre los hechos y los conocimientos relacionados con lugares específicos y tipos de amenazas.

Las herramientas analíticas especializadas también ayudan en otras áreas. Aunque la mayor parte de la comunicación entre los actores de las amenazas se lleva a cabo en inglés o en ruso, los anuncios gubernamentales, las noticias y las publicaciones en las redes sociales y en los blogs se escriben naturalmente en varios idiomas locales. El procesamiento del lenguaje natural (PLN) es una herramienta analítica que identifica piezas de contenido que contienen palabras y frases clave en todos los idiomas. Por ejemplo, la PLN permite que una solución de inteligencia encuentre artículos de noticias relevantes, publicaciones en blogs

y charlas en la dark web relacionadas con un mensaje en un foro en ruso que menciona “В Киеве будет протестный марш” (una marcha de protesta en Kiev).

Por supuesto, la inteligencia geopolítica no se limita a la automatización y el análisis. A menudo, no hay sustituto para la experiencia humana. Esto es especialmente cierto cuando se abordan cuestiones relacionadas con regiones y países concretos, en los que son fundamentales los conocimientos lingüísticos (incluido el conocimiento de la jerga local) y la familiaridad con la historia y la política. Por ello, también debe evaluar las soluciones de inteligencia en función de su capacidad para proporcionar inteligencia acabada, especialmente inteligencia geopolítica acabada.

La inteligencia terminada puede incluir informes de investigación personalizados que evalúen los riesgos en regiones específicas, conocimientos personalizados sobre las últimas amenazas que afectan a esas zonas y paquetes de caza que aceleran la investigación de sus equipos de respuesta a incidentes, caza de amenazas y riesgos geopolíticos.



Para un debate técnico sobre cómo una plataforma de inteligencia combina el análisis con la experiencia humana y la automatización para categorizar y conectar enormes volúmenes de datos de seguridad, lea la documentación técnica de Recorded Future, “[El gráfico de inteligencia de seguridad: dentro de la metodología y la tecnología patentada de Recorded Future.](#)”

Interacción con la inteligencia geopolítica

Las soluciones de inteligencia le permiten acceder e interactuar con la inteligencia geopolítica en varios formatos, como por ejemplo

- Cuadros de mando y mapas que muestran los niveles de riesgo por país y ciudad
- Alertas activadas por eventos o cambios en las puntuaciones de riesgo
- Informes en los que se detallan los acontecimientos y los problemas relacionados con los lugares especificados
- Documentos de referencia y perspectivas que resumen las principales conclusiones para los países y las ciudades
- Integraciones con otras herramientas de inteligencia, por ejemplo, el proveedor de inteligencia de localización Esri

Además, algunas soluciones de inteligencia geopolítica pueden integrarse con herramientas de seguridad más tradicionales, como los SIEM y los sistemas de tickets, y utilizar etiquetas geográficas para garantizar que las personas relacionadas con ciudades, países y regiones específicas reciban alertas inmediatas de los acontecimientos que se produzcan allí.

La figura 11-2 es un ejemplo de tablero de inteligencia geopolítica que destaca las zonas de alto riesgo en un mapa del mundo.

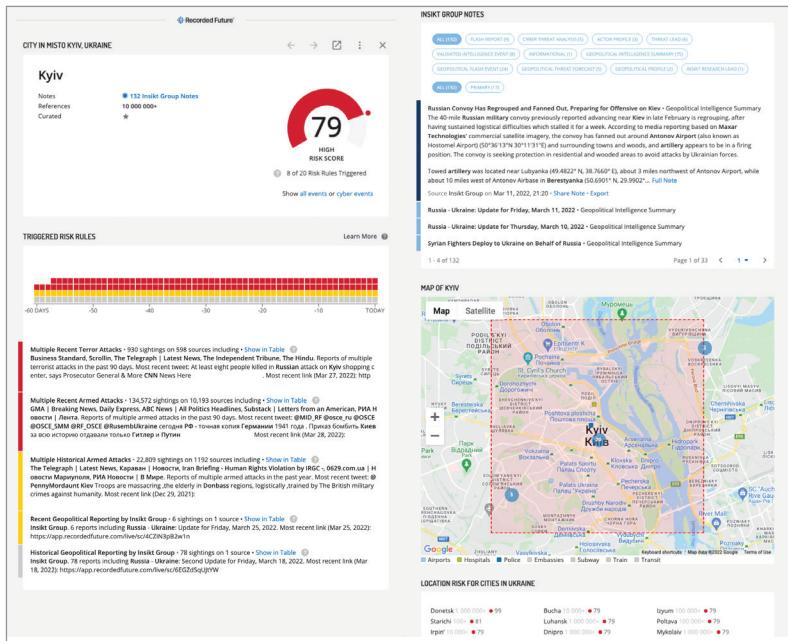


Figura 11-2: Ejemplo de panel de control que destaca las áreas de alto riesgo. (Fuente: Recorded Future)

Geopolítica y ciberamenazas

Este capítulo se ha centrado en las amenazas y eventos que se originan en los mismos países que las instalaciones que se quieren proteger. Sin embargo, el riesgo geopolítico también implica, bueno, geopolítica: Conflictos políticos, económicos e ideológicos entre naciones y alianzas mundiales.

En los últimos años, el mundo ha sido testigo de ciberataques contra Internet, las finanzas y las infraestructuras físicas. Entre ellos se encuentran los intentos de sobrecargar o inutilizar los

sitios web de organismos gubernamentales, organizaciones no gubernamentales (ONG) y medios de comunicación independientes, así como las campañas de desinformación dirigidas a gobiernos, elecciones y empresas.

La mayoría de estos ataques se han atribuido a misteriosos grupos de piratas informáticos, a veces vinculados a gobiernos, y en ocasiones incluso a departamentos de un gobierno o un servicio militar. Muchos organismos gubernamentales, empresas comerciales y ONG quedan atrapados en el fuego cruzado, incluso cuando tienen poca o ninguna relación con la disputa entre las naciones que iniciaron el conflicto. Esto hace que entender la intersección entre el riesgo físico y el cibernetico sea ahora más importante que nunca.

La defensa de su organización contra este tipo de amenazas requiere un programa de inteligencia integral que abarque todos los temas tratados en este manual, desde las operaciones de seguridad y la inteligencia sobre amenazas hasta la protección de la marca, y desde la gestión de vulnerabilidades y riesgos de terceros hasta la inteligencia geopolítica.

Para saber más sobre la relación entre los conflictos geopolíticos y las ciberamenazas, lea el artículo del blog Recorded Future, “[Geopolítica: una influencia ignorada en las operaciones cibernéticas](#).” Para saber más sobre la conexión entre las rivalidades nacionales y el hacktivismo, lea, “[Vuelta a la normalidad: Las falsas banderas y el declive del hacktivismo internacional](#).”



Capítulo 12

Inteligencia sobre el fraude

En este capítulo

- Revise los desafíos especiales para prevenir el fraude en línea
- Aprenda cómo se puede utilizar la inteligencia para anticipar y frustrar las campañas de fraude

Inteligencia sobre el fraude y evaluación del riesgo

La inteligencia del fraude se ocupa principalmente de prevenir el fraude en los pagos con tarjeta de crédito, así como otros tipos de fraude relacionados con las transacciones en línea. Aunque la inteligencia sobre el fraude es más importante para las instituciones financieras y los minoristas, también es valiosa para la sanidad, la administración pública, los viajes, el entretenimiento, los juegos en línea y otras organizaciones que aceptan pagos en línea por bienes y servicios.

La inteligencia contra el fraude difiere en un aspecto importante de la mayoría de los tipos de inteligencia que hemos analizado. Cuando la inteligencia proporciona una lista de vulnerabilidades o desconfiguraciones que representan amenazas reales para la empresa, el objetivo es eliminarlas. Sin embargo, cuando la inteligencia del fraude apunta a un lote de cuentas de tarjetas de pago que pueden haber sido comprometidas, los bancos, los comerciantes, los hospitales y las agencias gubernamentales probablemente no bloquearán automáticamente las transacciones o cerrarán las cuentas. En su lugar, adoptarán un enfoque basado en el riesgo para autorizar las transacciones (véase el cuadro de texto). En estas situaciones, la inteligencia sobre el fraude se utiliza para ayudar a evaluar el riesgo en lugar de crear una lista de vulnerabilidades y problemas que deben ser remediatos.

Autorización basada en el riesgo

Hoy en día, la mayoría de las instituciones financieras y muchos sitios web de comercio electrónico adoptan un enfoque basado en el riesgo para autenticar a los usuarios y autorizar las transacciones. Por ejemplo, cuando un usuario solicita una transacción, la aplicación evaluará su riesgo basándose en factores como el valor de la transacción, el dispositivo del usuario y su ubicación, el comportamiento del usuario en línea y sus similitudes con comportamientos anteriores, y los problemas conocidos relacionados con el usuario o el método de

pago. Dependiendo del cálculo del riesgo, se puede pedir al usuario que proporcione una contraseña, que responda a preguntas de seguridad o que introduzca un código de un solo uso enviado a un smartphone. Algunas transacciones pueden quedar en suspenso a la espera de una aprobación especial o ser bloqueadas por completo.

La inteligencia sobre el fraude que mejora la precisión de las evaluaciones de riesgo puede tener un gran impacto en la reducción del fraude.

La inteligencia sobre el fraude implica la recopilación y correlación de datos fragmentarios procedentes de muchas fuentes para identificar las cuentas expuestas y señalar el origen de las infracciones. A continuación, examinaremos las formas concretas en que puede utilizarse para anticiparse a las campañas de fraude y frustrarlas.

Vigilar la exposición de la cartera de tarjetas y la filtración de credenciales

Al igual que muchos otros tipos de información, la información sobre el fraude puede obtenerse en foros y mercados de la dark web. El tipo de pruebas que se pueden encontrar incluye:

- Los números de las tarjetas de pago y otros datos a menudo asociados a las cuentas de las tarjetas de pago, como los nombres, las direcciones, los números de teléfono y los códigos postales.
- Números de la Seguridad Social, números del carné de conducir, fechas de nacimiento, números de usuario frecuente y otros datos que suelen estar asociados a cuentas sanitarias, gubernamentales, de viajes y otras.

- Filtración de credenciales con direcciones de correo electrónico de empleados y otros identificadores
- “Charla” sobre sitios vulnerables al fraude y métodos para eludir las protecciones antifraude
- En raras ocasiones, los números reales de las cuentas de las tarjetas de pago

Los ciberdelincuentes de la dark web rara vez revelan los números de las cuentas de las tarjetas de pago. A veces es posible adquirir alguna información de la cuenta haciéndose pasar por un comprador criminal. Sin embargo, normalmente esto requiere una identidad establecida en la dark web y conocimientos idiomáticos en ruso, chino y otras lenguas no inglesas.

Más a menudo, es necesario recopilar datos relacionados con el fraude de múltiples fuentes y juntar las piezas para crear una inteligencia de fraude procesable. Y como parte de la información puede ser engañosa o simplemente falsa, hay que trabajar para limpiar los datos.

Aun así, los resultados pueden ser muy valiosos para los grupos de protección contra el fraude y de gestión de riesgos. Con frecuencia pueden señalar las cuentas comprometidas y ajustar los controles de riesgo de su organización antes de que se produzca el fraude.

Identificar los puntos comunes de compra comprometidos

Una técnica clave de protección contra el fraude es la correlación de muchas transacciones fraudulentas para identificar los puntos comunes de compra (CPP) comprometidos. Por lo general, se trata de sitios web de comerciantes (y a veces de locales físicos) con una vulnerabilidad que ha sido explotada para capturar los números de las tarjetas de crédito y la información de los usuarios de muchas cuentas.

La identificación de los CPP comprometidos ofrece varios beneficios:

- Todos los clientes que hayan visitado el CPP comprometido dentro del periodo de exposición pueden ser colocados en una categoría de mayor riesgo para reducir o eliminar la posibilidad de que sus cuentas puedan ser utilizadas para el fraude

- La vulnerabilidad en el sitio puede ser remediada para prevenir futuros compromisos
- Los TTP del atacante pueden ser analizados para mejorar las defensas de otros sitios web

Cuantos más datos sobre las transacciones fraudulentas estén disponibles, más fácil será identificar los CPP comprometidos. Sin embargo, muchas instituciones financieras son reacias a compartir este tipo de información con otras empresas del mismo ámbito. Por ello, las organizaciones del sector y los proveedores de servicios de inteligencia contra el fraude suelen poder recopilar más datos y hacer un mejor trabajo para encontrar los sitios comprometidos.

Vigilar los sitios web en busca de Magecart y otros ataques

Otra técnica para adquirir información sobre el fraude consiste en vigilar los sitios web de los comerciantes y de otros comercios electrónicos para detectar ataques de skimming digital, como las inyecciones de Magecart e iFrame. Normalmente es posible identificar los sitios web que han sido comprometidos por estos ataques inspeccionando el código del sitio en un navegador, sin requerir ninguna acción por parte del comerciante. Esta supervisión puede revelar datos comprometidos incluso antes de que se hayan puesto a la venta en la dark web o se hayan utilizado para cometer fraudes.

Una vez detectados los sitios web comprometidos, a menudo es posible:

- Identificar numerosos COI relacionados con el ataque
- Crear una imagen completa de la infraestructura y los métodos del atacante, incluidos los dominios de phishing, los dominios de exfiltración y el código malicioso
- Reconstruir cuando las cuentas fueron expuestas

Esta información puede utilizarse para encontrar otros sitios web que hayan sido víctimas del mismo atacante, proteger otros sitios web de comercio electrónico e identificar cuentas que puedan haber sido robadas y que, por tanto, deban colocarse en una categoría de alto riesgo.



Magecart es una alianza informal de piratas informáticos que empezaron a atacar los sistemas de carritos de la compra en línea para inyectar malware de robo de tarjetas y capturar los datos de las tarjetas de pago. Desde entonces, se han ramificado con técnicas adicionales para desplegar los skimmers y capturar los datos de las tarjetas. Los ataques Magecart han cobrado importancia desde el comienzo de la pandemia de COVID-19 porque facilitan el fraude con tarjeta no presente (CNP) (fraude cometido sin la tarjeta física, normalmente en línea).



Para obtener más información sobre la evolución de los ataques a Magecart, consulte dos entradas del blog de Gemini Advisory: “[El grupo “Keeper” Magecart infecta 570 sitios y el informe anual de Gemini 2021](#)”. (Gemini Advisory es una empresa de Recorded Future).

Identificar las señales

La dark web incluye mercados clandestinos en los que los ciberdelincuentes compran y venden programas informáticos, servicios e información de cuentas utilizadas para las campañas de fraude. La vigilancia de estos mercados puede proporcionar señales de que los ataques son inminentes.

Por ejemplo, los delincuentes están dispuestos a pagar más por la información de las cuentas de las tarjetas de pago cuando saben que es probable que los intentos de fraude tengan éxito. Un aumento en el precio de las cuentas de una tarjeta de pago puede indicar que se ha dado a conocer una debilidad en los controles de prevención del fraude de esa tarjeta o del banco que la emitió y que los ataques son inminentes. Esta información alerta a la institución emisora de que debe aumentar sus niveles de riesgo y revisar sus controles de seguridad.

A los defraudadores les gusta utilizar las credenciales de las tarjetas en el lugar donde vive el titular de la cuenta porque el uso local reduce la posibilidad de que una transacción sea marcada como sospechosa. Por lo tanto, un aumento de las solicitudes de cuentas en la dark web en una ciudad o región específica puede indicar que un grupo criminal está planeando lanzar ataques allí. Las instituciones financieras y los comerciantes pueden responder aumentando los controles de riesgo para las transacciones en esa área.

Superar al otro

Hay un viejo chiste sobre dos amigos que van de excursión por el bosque y son sorprendidos por un oso que se acerca. Uno de los amigos empieza a huir inmediatamente. El otro abre su mochila y empieza a cambiar sus botas de montaña por las zapatillas de correr. “¿Estás loco?” grita el primer amigo, “¡No puedes dejar atrás a un oso!” “No tengo que correr más que el oso”, dice el segundo amigo, “solo tengo que correr más que tú”.

Esta lógica se aplica a muchos escenarios de prevención del fraude. Incluso una ligera mejora en los modelos de riesgo de las instituciones financieras y los comerciantes en línea puede suponer una enorme reducción de

los índices de fraude. Los grupos de ciberdelincuentes son diligentes a la hora de hacer un seguimiento del retorno de la inversión de sus campañas. Si ven un rendimiento inusualmente bajo en los ataques contra una tarjeta de pago o un comerciante específico, dirigen su atención a víctimas más fáciles. La inteligencia sobre el fraude puede proporcionar la ventaja que lo hace posible.

A veces se puede observar el efecto de una mejor prevención del fraude en los mercados de la dark web. Cuando se observa la disminución de la demanda y la caída de los precios de la información de ciertas tarjetas, en realidad se está viendo cómo el oso se vuelve para perseguir al otro.

El retorno de la inversión en inteligencia sobre el fraude

La inteligencia en materia de fraude suele producir un alto rendimiento de la inversión para los bancos que emiten tarjetas de pago. El uso proactivo de la inteligencia del fraude:

- Evita el fraude
- Mejora la satisfacción y la retención de los clientes al reducir las señales falsas positivas en las transacciones de compra
- Aumenta la retención de los comerciantes y los ingresos subyacentes

Capítulo 13

Inteligencia de la identidad

En este capítulo

- Examinar la idea de recoger y analizar las credenciales comprometidas para proteger a los empleados, socios y clientes
- Comprender la necesidad de una amplia cobertura y de un triaje de gran volumen
- Explore cómo utilizar la inteligencia para proteger las identidades

Protección de la autenticación

Una autenticación de identidad sólida es esencial para frustrar el fraude en línea, la toma de posesión de cuentas (ATO) y los ataques de ransomware, los robos de PII y propiedad intelectual, los ataques de compromiso de correo electrónico empresarial (BEC) y otras amenazas.

Los ciberdelincuentes llevan tiempo reconociendo que las credenciales de los usuarios son las proverbiales llaves del castillo. Han desarrollado muchas formas innovadoras de obtenerlos, como el skimming y el malware de registro de claves, los ataques de phishing y de ingeniería social dirigidos a los usuarios finales, y las violaciones de datos de sitios web corporativos, gubernamentales, minoristas y de medios sociales. Las personas que reutilizan las contraseñas en varias cuentas juegan a su favor, porque las credenciales robadas en una violación de datos a menudo pueden utilizarse para penetrar en muchos sitios web.

¿Cuál es la gravedad de este problema? En el informe de *2021Tendencias en la seguridad de las identidades digitales* de la Identity Defined Security Alliance y Dimensional Research, el 95 % de las empresas encuestadas reconoció haber sufrido una brecha relacionada con la identidad en algún momento, y el 79 % dijo haber experimentado una brecha relacionada con la identidad durante los últimos dos años. En su informe sobre investigaciones de fugas de datos de 2021, Verizon descubrió que las credenciales eran el tipo de datos más buscado durante las fugas.



El panorama del robo de credenciales ha empeorado aún más con la aparición del malware ladrón. Un ejemplo claro es el malware RedLine Stealer vendido en varios foros de la dark web por un ciberdelincuente de habla rusa que se hace llamar “REDGLade”. RedLine Stealer captura nombres de usuario, contraseñas, cookies, credenciales de tarjetas de pago e información de carteras de criptomonedas de navegadores, clientes FTP y clientes de mensajería instantánea. Puede distribuirse a través de correos electrónicos de phishing, redes sociales y aplicaciones de mensajería, o incrustado en una aplicación aparentemente legítima. Para una descripción detallada, lea [RedLine Stealer es una fuente clave de datos de identidad para las tiendas de productos delictivos](#), un informe publicado por el Grupo Insikt de Recorded Future.

Un plan para proteger las identidades

Pero no todo está perdido. La información en tiempo real sobre las credenciales comprometidas puede desbaratar a los adversarios antes de que sus ataques causen algún daño. Imagine que pudiera compilar una base de datos de todas las identidades robadas publicadas y vendidas en la dark web. Serías capaz de hacerlo:

- Analice las cuentas de usuario de sus empleados, así como de los contratistas y socios comerciales que tengan acceso a sus sistemas, para identificar y cambiar las credenciales que hayan sido comprometidas
- Realice comprobaciones de riesgo automáticas durante eventos críticos, como la creación y el restablecimiento de contraseñas, para evitar que la gente reutilice las contraseñas expuestas
- Identificar las credenciales de los clientes que habían sido comprometidas, y pedir una verificación adicional de sus identidades antes de permitir las transacciones
- Supervisar los correos electrónicos y los intentos de inicio de sesión para evitar el uso de credenciales robadas para el fraude, los ataques de BEC y ransomware, y las violaciones de datos

Pero la ejecución de esa sencilla idea plantearía algunos problemas importantes. Tendrías que hacerlo:

- Recoger con frecuencia las credenciales expuestas de muchas fuentes de difícil acceso
- Clasifique cantidades masivas de datos para encontrar las credenciales expuestas que representan amenazas reales para su empresa
- Facilitar el uso de la base de datos de identidades robadas tanto a los profesionales de la seguridad como a las herramientas de autenticación y seguridad automatizadas

Veamos de qué se trata.

Fuentes de identidades robadas

Las credenciales expuestas están disponibles en muchas fuentes de código abierto, dark web y técnicas. Entre ellas se encuentran:

- Bases de datos públicas y de hackers de credenciales expuestas
- Foros y mercados de la dark web
- Salas de chat de retransmisión por Internet y plataformas de medios sociales
- Repositorios de código como GitHub y sitios de pegado como Pastebin

La creación de una base de datos completa de credenciales expuestas requiere la recopilación continua de actualizaciones y nuevas publicaciones de estas fuentes, incluidos los foros y mercados por invitación en la dark web.



Gol en propia meta GitHub es ampliamente utilizado por los ingenieros de software para compartir el código del software, la documentación y otros archivos de trabajo. Por desgracia, a veces contienen contraseñas, claves secretas, tokens de la API y otros elementos de seguridad. Los repositorios de GitHub son públicos por defecto. Los desarrolladores a menudo se olvidan de restringir el acceso, y los malos los escanean regularmente. En esta entrada del blog de Comparitech, puede leer cómo un equipo de seguridad expuso intencionadamente un conjunto de credenciales de AWS en GitHub y vio cómo los hackers maliciosos se abalanzaban sobre ellas literalmente en un minuto: **Los hackers tardan 1 minuto en encontrar y abusar de las credenciales expuestas en GitHub.**

Triaje de gran volumen

La gran mayoría de las credenciales expuestas disponibles en fuentes de código abierto y de la dark web son duplicados o falsificaciones, o no suponen una amenaza para su empresa. Clasificarlos todos es una tarea ingente. ¿Qué hay que reducir?

Duplicados y falsificaciones

La mayoría de los analistas estiman que dos tercios o más de las entradas en las bases de datos de credenciales expuestas son duplicados. A menudo, las mismas entradas aparecen tres, cuatro o muchas más veces porque:

- Las mismas credenciales pueden haber sido comprometidas en múltiples violaciones de datos o ataques de phishing
- Las bases de datos y las listas de credenciales para la venta se copian unas a otras

Los malos actores que venden información robada no son escrupulosos a la hora de copiar y revender los datos de los demás. Y no solo eso, sino que a veces engrosan sus listas creando usuarios falsos con direcciones de correo electrónico de dominios populares. Demasiado para el honor entre ladrones.

Amenazas no amenazantes

Suponga que encuentra una entrada con la dirección de correo electrónico correcta de uno de sus empleados (jane.smith@mycompany.com) y una contraseña, “genius1”. ¿Está usted expuesto? No si su organización ha aplicado una política de contraseñas que exige un mínimo de ocho caracteres, o el uso de al menos una letra mayúscula o un carácter especial. Es probable que Jane Smith utilizara su dirección de correo electrónico de empresa y “genius1” para un sitio web o una cuenta de redes sociales que fue hackeada, pero sabes que debe tener una contraseña diferente para el inicio de sesión de su empresa.

Credenciales obsoletas

Hay otros tipos de credenciales que no representan una amenaza significativa, por ejemplo, las credenciales de:

- Personas que han cambiado sus contraseñas recientemente porque han sido alertadas de una brecha, o han sido obligadas por las políticas de acceso de su organización, o simplemente están preocupadas por la seguridad
- Personas que ya no trabajan para la empresa (suponiendo que se desactiven las cuentas cuando la gente se vaya)
- Clientes cuyas cuentas han sido canceladas

Está claro que necesitamos herramientas automatizadas de filtrado y triaje para evitar gastar la mayor parte de nuestro tiempo en los duplicados, las falsificaciones, las no amenazas y los problemas que ya se han solucionado solos.

¿Las contraseñas con hash tienen un pase?

Un número importante de contraseñas robadas se convierten en hash (codificadas mediante una transformación unidireccional) antes de ser almacenadas. ¿Significa eso que están seguros? No necesariamente. Una contraseña (digamos, Qwerty123) transformada por un algoritmo hash específico (digamos, MD5) siempre tendrá el mismo valor hash (en este caso, 2AF9B1BA42D-C5EB01743E6B3759B6E4B).

Los atacantes utilizan tablas con los valores hash de las contraseñas más comunes para devolver esas contraseñas a su forma original. Así que una versión con hash de “!!A1nt!\$martXO%%^” es probablemente segura, pero un hash de “Qwerty123” definitivamente no lo es. Las contraseñas codificadas pueden ser menos prioritarias que las claras, pero no deben ser ignoradas.

Uso de la información sobre la identidad

Hay varias maneras de utilizar los datos de identidad para prevenir el fraude y las violaciones de datos y mejorar los controles de seguridad.

Escaneo de cuentas de usuario

Una organización puede aprovechar la recopilación de información de identidad en tiempo real escaneando las cuentas de los usuarios para encontrar y cambiar las credenciales comprometidas.

Se puede aplicar una vigilancia especial a los usuarios más arriesgados:

- Ejecutivos y miembros del consejo de administración
- Administradores de sistemas informáticos, profesionales de la seguridad y otras personas con amplios privilegios y permisos de cuenta
- Responsables de las funciones de tesorería y finanzas y otras personas con poder para transferir fondos
- Socios comerciales y proveedores que tienen credenciales para acceder a las aplicaciones de la organización
- Clientes clave
- Usuarios de todo tipo cuyas credenciales han sido comprometidas con mayor frecuencia



No supervise solo las credenciales de las personas reales. Los ciberdelincuentes también valoran las contraseñas asociadas a direcciones de correo electrónico basadas en roles. Busque credenciales comprometidas que incluyan direcciones con palabras relacionadas con las finanzas, la administración y la gestión de la cadena de suministro, como “factura”, “pagos”, “administración”, “soporte” y “socios”.

Por supuesto, el hallazgo de credenciales comprometidas debería desencadenar solicitudes de restablecimiento de la contraseña. Pero se puede ir más allá en el caso de los usuarios de alto riesgo y frecuentemente comprometidos, exigiendo:

- Contraseñas más fuertes
- Restablecimiento más frecuente de las contraseñas
- El uso de MFA para acceder a aplicaciones críticas

El AMF no es una panacea

La autenticación multifactor (MFA) es una técnica valiosa para proteger las cuentas de alto riesgo, pero no es una panacea. En algunas situaciones, las organizaciones no están dispuestas a imponer a los usuarios los inconvenientes de configurar y utilizar la AMF. Además, los actores de las amenazas pueden eludir la AMF mediante:

- Intercambio de SIM: convencer a un proveedor de servicios de telefonía móvil para que transfiera una cuenta de móvil de la tarjeta SIM del usuario (y del smartphone) a otra controlada por el atacante.
- Suplantación de identidad en tiempo real: una técnica de “hombre en el medio” que utiliza un enlace de correo electrónico para enviar a un usuario a un

sitio web controlado por el atacante, donde el usuario envía un formulario a un sitio web legítimo, que devuelve una contraseña de un solo uso a las manos del atacante, que puede utilizarla para iniciar sesión y hacerse con la cuenta.

- Extensiones maliciosas del navegador: software espía que supervisa las sesiones de MFA entre el navegador y el servidor y captura información sobre los factores de autenticación adicionales.

La AMF sigue siendo una práctica recomendada importante, pero no elimina la necesidad de defensas adicionales, como las comprobaciones de riesgo contra las credenciales comprometidas.

Realización de controles de riesgo automáticos

Puede realizar comprobaciones automáticas de credenciales comprometidas durante eventos críticos como la creación y el restablecimiento de contraseñas. Dependiendo de las políticas y la cultura de su organización, esto podría implicar cambiar las contraseñas automáticamente o informar a los usuarios y pedirles que realicen el cambio (quizás dentro de un límite de tiempo).

SUGERENCIA



Aproveche esta oportunidad para educar a los usuarios. Explíquenes claramente lo sucedido y recuérdoles la importancia de no utilizar su dirección de correo electrónico o contraseña de la empresa para las redes sociales, el comercio, el ocio u otras cuentas no comerciales.

Supervisión de los correos electrónicos y los inicios de sesión

Los productos de seguridad del correo electrónico suelen capturar las direcciones de correo electrónico y las contraseñas contenidas en los correos electrónicos entrantes. Las herramientas de autenticación evalúan las entradas de personas (y bots) que intentan entrar en las aplicaciones. En ambos casos, estas soluciones pueden integrarse con una base de

datos de inteligencia de identidad para señalar las credenciales comprometidas y prevenir las etapas iniciales de las campañas de fraude en línea, los ataques de BEC y ransomware, y las violaciones de datos.

Determinación de las causas profundas

Analizar la incidencia de credenciales comprometidas en su base de usuarios puede ayudarle a descubrir problemas sistémicos como:

- El uso de contraseñas débiles y comunes que son susceptibles de ataques de fuerza bruta
- Socios de la cadena de suministro y otros terceros con controles de seguridad deficientes
- Unidades de negocio o regiones geográficas especialmente susceptibles de pérdida de credenciales

Este tipo de análisis puede poner de manifiesto la necesidad de tomar medidas como:

- Reforzar las políticas de contraseñas en determinados ámbitos o de forma global
- Refuerzo de los controles de acceso de terceros
- Salado y hashing de contraseñas almacenadas
- Aumentar el uso de la autenticación multifactorial

Inteligencia de identidad como servicio

La inteligencia de la identidad es un campo especializado. La mayoría de las empresas querrán investigar las ofertas de servicios de inteligencia de identidad en lugar de crear sus propias capacidades. Un proveedor de servicios debe ser capaz de ofrecer inteligencia de identidad con:

- Recopilación de información de identidad en tiempo real
- Amplia cobertura de fuentes técnicas, de código abierto y de la dark web

- Clasificación eficiente y precisa de los datos para eliminar los duplicados, las falsificaciones y las credenciales que no son una amenaza para su organización
- Búsqueda automática de credenciales expuestas
- Herramientas para consultar y analizar datos de usuarios individuales, lotes de usuarios y unidades de negocio enteras

Capítulo 14

Inteligencia de superficie de ataque

En este capítulo

- Conozca qué comprende la superficie de ataque digital de una organización
- Explore cómo los servicios de inteligencia de la superficie de ataque descubren dominios desconocidos y activos expuestos en Internet
- Comprenda cuántos grupos dentro y fuera de TI pueden utilizar la inteligencia de la superficie de ataque

Su superficie de ataque digital es más grande de lo que cree

Hoy en día, la mayoría de las organizaciones de tamaño medio tienen cientos de activos orientados a Internet que son potencialmente susceptibles de ser atacados. Las grandes empresas tienen miles. Y muy pocas organizaciones pueden identificar, y mucho menos controlar, a la mayoría.

Por supuesto, la mayoría de las empresas y organismos públicos solo tienen unos pocos dominios de primer nivel (por ejemplo, www.recordedfuture.com) y quizás unas cuantas docenas de subdominios (blog.recordedfuture.com, support.recordedfuture.com, etc.). Pero, ¿cuántos activos tienen una dirección IP y se conectan a Internet? Sume:

- Todos los portátiles, ordenadores de sobremesa y dispositivos móviles utilizados por los empleados
- Cada servidor, dispositivo de red, dispositivo de seguridad e impresora en red en cada centro de datos y oficina
- Todos los servidores virtuales, bases de datos, servicios y otras cargas de trabajo en plataformas de nube

- Todo el inventario de sensores, cámaras, robots y otros dispositivos IoT conectados a la web

La mayoría de ellos están protegidos por algún tipo de cortafuegos o sistema de control de acceso. Pero algunos no lo son, y solo hace falta uno o unos pocos sistemas expuestos para dar a los atacantes una vía de entrada a una organización.

La inteligencia de la superficie de ataque es la información sobre las redes y los sistemas a los que se puede acceder a través de Internet y los riesgos que generan. Las soluciones y servicios de inteligencia de la superficie de ataque ayudan a los equipos de seguridad:

- Descubrir todos los activos de la organización en Internet
- Analizar los activos expuestos para determinar cuáles son los más propensos a tener vulnerabilidades o problemas de seguridad
- Supervisar continuamente la superficie de ataque de la organización para detectar nuevos dominios y activos que puedan crear riesgos

Riesgos ocultos

¿Cómo es posible que los equipos de seguridad no conozcan los activos orientados a Internet o no sean conscientes de los problemas graves de seguridad? Las causas típicas son:

- Proyectos de desarrollo de aplicaciones abandonados y entornos de demostración de marketing que dejan en su lugar dominios y subdominios no utilizados
- Dominios y activos olvidados pertenecientes a entidades adquiridas

- “Sistemas de TI en la sombra” y suscripciones a aplicaciones en la nube fuera de los controles de seguridad de la organización
- Configuraciones erróneas del servidor, como puertos abiertos que permiten el acceso no autorizado a las redes internas
- Nombres de host y certificados autofirmados que apuntan a direcciones IP internas
- Los servicios de alojamiento en la nube carecen de los controles necesarios para la seguridad o el cumplimiento de la normativa

Descubrir los activos de cara a Internet

La primera tarea de un servicio o solución de inteligencia de superficie de ataque es descubrir todos los activos de una organización que podrían ser explotados por los actores de la amenaza. Este proceso implica la comprobación de diversas bases de datos y fuentes de terceros y la realización de exploraciones en Internet.

El proceso de descubrimiento incluye:

- Comprobación de los registros de dominios y de la base de datos WHOIS para todos los dominios y subdominios de primer nivel asociados a la organización
- Realización de búsquedas DNS inversas para descubrir todas las direcciones IP a las que apuntan los dominios y subdominios
- Comprobación de los registros regionales de Internet (RIR) para encontrar todas las direcciones IP registradas en la organización
- Encontrar certificados autofirmados con punteros a direcciones IP internas

Los datos pueden utilizarse para crear un inventario de toda la cartera de dominios de la organización y de todas las direcciones IP a las que se puede acceder desde el exterior.



No se sorprenda si el proceso de descubrimiento arroja cientos o incluso miles de dominios, subdominios y sistemas conectados a Internet previamente desconocidos. Es un resultado típico, aunque bastante aleccionador. Utilice las conclusiones para determinar y abordar las causas de fondo, como el descuido por parte de los grupos de desarrollo de aplicaciones o de marketing, las actividades de TI en la sombra, la investigación inadecuada de los sistemas de TI de las organizaciones adquiridas y la supervisión incompleta de los entornos en la nube.

Discovery también puede encontrar adquisiciones de subdominios.

Adquisición de subdominios

A veces, una organización registra un subdominio y nunca lo utiliza, o utiliza el subdominio durante un tiempo y luego retira el host que le proporciona contenido.

Estas situaciones dan a los actores maliciosos una apertura para tomar el control del subdominio contactando con el servicio de alojamiento y conectando su propio host virtual. Un atacante puede entonces ser capaz de:

- Enviar correos electrónicos de phishing que parezcan proceder del dominio de nivel superior de la organización
- Publicar contenido controvertido o vergonzoso en el subdominio (“defacement”)

- Ejecutar ataques de secuencias de comandos en sitios cruzados (XSS) y de falsificación de solicitudes en sitios cruzados (CSRF)

Las adquisiciones de subdominios pueden utilizarse para engañar a los clientes y a los empleados de forma muy similar a los “dominios parecidos”. Si www.avaliddomain.com es el sitio web de una empresa legítima, ¿cómo puede saber un usuario que un formulario en freegift.avaliddomain.com o un correo electrónico de support.avaliddomain.com forman parte de una campaña de fraude?

Análisis de los activos expuestos

Después de crear un inventario de los activos orientados a Internet, un servicio o solución de inteligencia de superficie de ataque puede adquirir información de esos activos, analizar la información y hacer una lista de los activos con mayor probabilidad de tener vulnerabilidades o problemas de seguridad.

Posibles vulnerabilidades

Uno de los problemas típicos son los servidores con configuraciones erróneas, como puertos abiertos y parámetros de acceso remoto que podrían permitir a los malintencionados obtener acceso no autorizado a las redes y aplicaciones.

Otro ámbito de preocupación son los sistemas orientados al exterior con herramientas y aplicaciones de software que se sabe que son objetivo frecuente de los agentes de amenazas. Algunos ejemplos son los sitios web con un sistema de gestión de contactos (CMS), las plataformas de comercio electrónico, los servidores de bases de datos y las bibliotecas de JavaScript.

Una solución de inteligencia de la superficie de ataque también puede analizar los registros DNS y los certificados SSL para ver si apuntan a la infraestructura interna y a las direcciones IP de los sistemas internos que podrían ser explotados por los atacantes.

Infracciones de la política

Una solución de inteligencia de la superficie de ataque puede identificar los sistemas que podrían violar las políticas de la empresa, como los sistemas que deberían estar protegidos por controles de seguridad especiales, pero no están. Un ejemplo es un sistema que maneja información de tarjetas de crédito pero que está fuera del entorno de datos de titulares de tarjetas (CDE) designado por la organización. Otro ejemplo sería el de los certificados digitales registrados con una autoridad certificadora gratuita cuando eso viola la política de seguridad de la organización.

Las infracciones de las políticas también pueden ocurrir cuando las cargas de trabajo se ejecutan en plataformas de alojamiento en la nube que no proporcionan todos los controles de seguridad necesarios para cumplir con los estrictos requisitos reglamentarios, como el GDPR y algunas de las normas de alto nivel del NIST.

Defensas en su sitio

En la otra cara de la moneda, un análisis también puede mostrar qué sistemas están protegidos por defensas como los cortafuegos de aplicaciones web (WAF). Esta información es útil porque a estos sistemas se les puede asignar una prioridad de corrección menor que a los equivalentes que están más expuestos.



Las soluciones de inteligencia de la superficie de ataque no sustituyen a los escáneres de vulnerabilidades, sino que los complementan. Cuando la solución descubre y analiza todos los activos orientados a Internet, una organización puede centrar sus esfuerzos de exploración de vulnerabilidades en las aplicaciones y sistemas de mayor riesgo.

Supervisión continua de la superficie de ataque

Hoy en día, las superficies de ataque digitales evolucionan y se transforman a un ritmo rápido. Las organizaciones amplían continuamente su presencia en la web con nuevos proyectos de marketing, comercio electrónico, seguimiento de pedidos, atención al cliente, cadena de suministro, redes sociales y otros proyectos web. Las aplicaciones dinámicas en la nube crean y mueven con frecuencia las cargas de trabajo de las aplicaciones. Cientos de nuevos dispositivos con direcciones IP pueden

ponerse en línea en cualquier momento. Estas actividades crean las condiciones para que surjan nuevos problemas de seguridad, a menudo en áreas invisibles para las herramientas de seguridad convencionales.

Las soluciones de inteligencia de la superficie de ataque pueden ayudar a las organizaciones a mantenerse al tanto de la situación mediante la supervisión de estos cambios y destacando los activos afectados que deben ser investigados, como, por ejemplo:

- Nuevos dominios y subdominios registrados asociados a la organización y sus marcas
- Nuevos servidores y sistemas con software de alto riesgo
- Sistemas pertenecientes a los objetivos de adquisición y a los socios de terceros con configuraciones erróneas e infracciones de las políticas

Con la inteligencia de la superficie de ataque, los equipos de seguridad pueden trabajar con un inventario dinámico de activos orientados a la web, en lugar de listas estáticas y obsoletas de direcciones IP.

¿Quién utiliza la inteligencia de superficie de ataque?

La inteligencia de la superficie de ataque es valiosa para bastantes grupos dentro y fuera de las TI. Puede ayudar:

- Los equipos de gestión de vulnerabilidades priorizan la aplicación de parches, identifican los activos afectados por las nuevas CVE y comienzan a cubrir los activos hasta ahora desconocidos
- Los equipos del SOC enriquecen las alertas con datos de la superficie de ataque y priorizan la reparación de los activos de alto riesgo
- Los equipos de respuesta a incidentes, caza de amenazas y análisis forense obtienen una visión de los hackers de toda la superficie de ataque digital de la organización, incluidos los dominios desconocidos y olvidados, los activos de alto riesgo y las direcciones IP internas expuestas por los registros DNS y los certificados digitales

- Los equipos de cumplimiento y de gestión de riesgos de terceros identifican las infracciones de las políticas y señalan los puntos débiles de los entornos informáticos de terceros y de las posibles adquisiciones
- Los analistas de seguridad reducen las superficies de ataque identificando y eliminando o mitigando las causas raíz de los activos expuestos en Internet

En resumen, la inteligencia de la superficie de ataque no solo ayuda a los equipos de seguridad a ser más eficientes y eficaces, sino que puede apoyar las iniciativas corporativas de transformación digital, cumplimiento de políticas y gestión de riesgos de terceros.

Capítulo 15

Inteligencia para líderes de seguridad

En este capítulo

- Vea cómo la inteligencia apoya la gestión de riesgos y las inversiones en programas de seguridad
- Explore los tipos de información que los CISO consideran más valiosos
- Revise cómo la inteligencia mitiga la brecha de habilidades de seguridad

El trabajo del CISO ha experimentado cambios drásticos en los últimos años. Antes se centraba en la toma de decisiones sobre la compra e implantación de tecnologías de seguridad. Ahora, los CISO son mucho más propensos a interactuar con el director general y el consejo de administración y a realizar delicados actos de equilibrio para anticiparse al riesgo y garantizar la continuidad del negocio.

Los responsables de seguridad deben ser capaces de:

- Evaluar los riesgos empresariales y técnicos, incluidas las amenazas emergentes y las “incógnitas conocidas”, que podrían afectar a la empresa
- Identificar las estrategias y tecnologías adecuadas para mitigar los riesgos
- Comunicar la naturaleza de los riesgos a la alta dirección y justificar las inversiones en seguridad en función del valor financiero para la empresa

La inteligencia es un recurso fundamental para todas estas actividades.

Gestión de riesgos

Quizá la mayor responsabilidad del CISO moderno sea la gestión de riesgos. Se trata de asignar recursos y presupuesto para minimizar el impacto probable de las amenazas en la empresa. La figura 15-1 describe las etapas por las que suelen pasar los responsables de seguridad al abordar este reto.

Evaluar los requisitos de seguridad	Comprender los objetivos empresariales y de TI y definir las responsabilidades de la función de seguridad.
Evaluar los protocolos de seguridad existentes	Analizar el personal, los procesos y las tecnologías de seguridad actuales para desarrollar una imagen precisa de la función de seguridad.
Desarrollar iniciativas	Utilice un enfoque basado en los riesgos para identificar las deficiencias más importantes en materia de seguridad y, a continuación, defina y priorice las iniciativas para solucionarlas.
Seguimiento del progreso	Supervisar continuamente los progresos y garantizar que la función de seguridad mejore de acuerdo con los requisitos. Desarrollar métricas para medir la eficacia continua.

Figura 15-1: Un enfoque estándar para evaluar el riesgo y desarrollar una estrategia de seguridad. (Fuente: Recorded Future)

Los datos internos no son suficientes

El enfoque de la seguridad descrito en la Figura 15-1 depende de que se disponga de una buena información sobre los factores de riesgo relevantes y los posibles puntos débiles de los programas de seguridad existentes. Sin embargo, con demasiada frecuencia este tipo de información solo se obtiene a partir de auditorías internas, problemas conocidos e incidentes de seguridad anteriores. Ese enfoque produce una lista de retos que ya han afectado a su organización, pero deja fuera los retos que están en el horizonte y aún no le han alcanzado.

El contexto externo es necesario para:

- Verificar el riesgo relacionado con problemas conocidos
- Advertir sobre las amenazas emergentes e imprevistas

Los datos de tráfico de la red interna, los registros de eventos y las alertas obviamente aportan valor a la gestión de riesgos, pero no proporcionan suficiente contexto para construir un perfil de riesgo completo, y ciertamente no es suficiente para definir una estrategia completa. Los profesionales de la seguridad deben ser proactivos a la hora de descubrir riesgos desconocidos. El contexto es lo que permite a los responsables de seguridad determinar qué amenazas potenciales tienen más probabilidades de convertirse en amenazas reales para su organización.

Afinar el enfoque

La inteligencia proporciona un contexto sobre tendencias generales como:

- Los tipos de ataques que son cada vez más (o menos) frecuentes
- Los tipos de ataques más costosos para las víctimas
- TTP de los nuevos actores de la amenaza que se están presentando, y los activos y organizaciones a los que se dirigen
- Las prácticas y tecnologías de seguridad que han resultado más (o menos) exitosas para detener o mitigar estos ataques

Los datos y la información sobre estas tendencias permiten a las organizaciones de seguridad anticiparse a las amenazas que serán noticia en el futuro. Sin embargo, la inteligencia externa contextualizada es mucho más poderosa. Por ejemplo, permite a los grupos de seguridad evaluar si es probable que una amenaza emergente *afecte* a su organización específica en función de factores como:

- Industria:** ¿Afecta la amenaza a otras empresas de nuestro vertical?
- Tecnología:** ¿La amenaza implica comprometer el software, el hardware u otras tecnologías utilizadas en nuestra organización?

- Geografía:** ¿La amenaza se dirige a las instalaciones de las regiones en las que operamos?
- Método de ataque:** ¿Las técnicas utilizadas en el ataque (incluida la ingeniería social y los métodos técnicos) se han utilizado con éxito contra nuestra organización o contra otras similares?

Sin un profundo conocimiento de un conjunto extremadamente amplio de fuentes de datos externas, es imposible que los responsables de la seguridad obtengan una visión holística del panorama de los ciberriesgos e identifiquen los mayores riesgos para su organización.

La Figura 15-2 ilustra cómo un panel de inteligencia personalizado destaca la inteligencia más relevante para una organización específica.

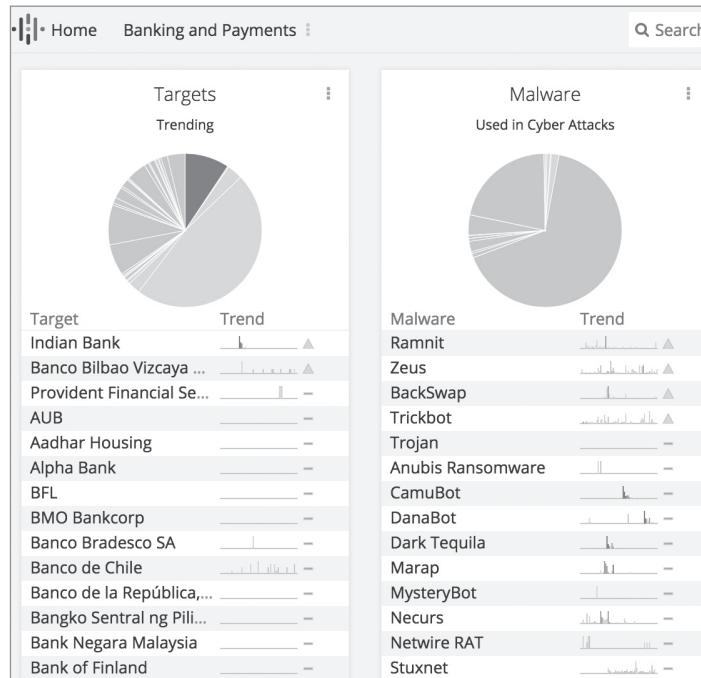


Figura 15-2: Un panel de inteligencia señala las amenazas más relevantes para una industria o tecnología específica. (Fuente: Recorded Future)

Mitigación: personas, procesos y herramientas

Los escaneos de vulnerabilidades y las técnicas como las pruebas de penetración y el “red teaming” contribuyen a la capacidad de un equipo de seguridad para comprender dónde existen brechas en sus defensas. Sin embargo, muchas organizaciones tienen muchas más vulnerabilidades en sus procesos y más debilidades en sus prácticas y políticas de seguridad de las que pueden solucionar a corto plazo.

La inteligencia permite a los responsables de la seguridad señalar los retos que deben abordarse en primer lugar indicando:

- Los actores de la amenaza que tienen más probabilidades de dirigirse a la organización
- Las TTP que utilizan esos actores de la amenaza, y las debilidades que tienden a explotar

Alertas tempranas

Los analistas encuentran actores de amenazas en la Dark Web discutiendo o anunciando malware dirigido a su pila tecnológica. En ocasiones, estos actores de la amenaza utilizan estas plataformas para reclutar a programadores con ideas afines que les ayuden. Al supervisar los foros y mercados de la Dark Web, los analistas también pueden rastrear el desarrollo y la venta de malware dirigido a vulnerabilidades específicas y otras herramientas maliciosas.

La inteligencia conecta los puntos de todas estas entidades para proporcionar un contexto sobre lo que significan para su organización. Y, como se ha comentado anteriormente en este libro, es fundamental centrarse en parchear las vulnerabilidades y mitigar los puntos débiles que realmente corren el riesgo de ser explotados antes de abordar otros en los que la explotación es meramente teórica.



Utilice una solución de inteligencia para escanear la Dark Web y otras fuentes en busca de referencias a su organización, su industria y las tecnologías específicas instaladas en su organización.

Inversión

Decidir cómo invertir en ciberseguridad se ha convertido en los últimos tiempos en un reto de enormes proporciones.

Los asesores de inversión financiera Momentum Partners identificaron más de 3500 empresas en 2021 especializadas en tecnologías y servicios de ciberseguridad. Con tantas opciones, ¿cómo se supone que los CISO identifican las soluciones más efectivas para implementar como parte de una estrategia de seguridad proactiva?

La única forma lógica es tomar decisiones de inversión basadas en el riesgo. Cada organización tiene su propio perfil de riesgo, conformado por su industria, ubicaciones físicas e infraestructura interna. La inteligencia permite a los responsables de seguridad conocer las amenazas más acuciantes para su organización, lo que simplifica las tareas de identificación y justificación de las áreas de inversión. El objetivo final es poder juzgar ese riesgo y realizar inversiones basadas en un sólido conocimiento del panorama de las amenazas.

Comunicación

Los CISO se enfrentan a menudo a la necesidad de describir las amenazas y justificar las contramedidas en términos que motiven a los líderes empresariales no técnicos, como el coste, el retorno de la inversión, el impacto en los clientes y las ventajas competitivas.

Bombardear a los altos cargos con noticias sobre cada una de las amenazas no es una buena opción. En cambio, la inteligencia proporciona poderosas ideas para orientar este tipo de debates, como por ejemplo

- Los impactos de ataques similares en empresas del mismo sector, y en organizaciones del mismo tamaño en otros sectores
- Tendencias e información cibernetica que indiquen que la organización es susceptible de ser objeto de un ataque y cuántas pérdidas pueden esperarse por incidente

Caso práctico: Inteligencia y automatización en un minorista mundial

Con casi 3600 tiendas y más de 135 000 empleados en todo el mundo, una cadena minorista global se enfrenta a retos que van desde la prevención de pérdidas y fraudes y la seguridad corporativa hasta la protección de la información personal de los clientes.

El minorista utiliza la automatización para centralizar y personalizar la inteligencia de cada función de seguridad. La automatización garantiza que la inteligencia en tiempo real que entra en su SIEM es precisa y altamente contextual, y que el resultado se presenta en formatos flexibles y fáciles de usar.

El mayor retorno de la inversión de la empresa, y la mayor ventaja de gestionar la inteligencia a través de una plataforma integral, es la mejora de las relaciones tanto entre los

equipos de ciberseguridad como con otros departamentos.

Dice un alto directivo del centro de ciberdefensa de la empresa: “Ninguno de nosotros opera en un silo. Si podemos utilizar la inteligencia para mantenernos seguros, pero también para ayudar a la visibilidad de nuestro programa, eso ayuda a justificar la necesidad de más capacidades. Contar con campeones en otros equipos que respalden los beneficios de la inteligencia realmente ayuda a nuestro retorno de la inversión.”

Para ver más ejemplos de cómo Recorded Future ahorra costes, aumenta la productividad y mejora la seguridad, lea el informe de Forrester: “[El Total Economic Impact™ de la plataforma de inteligencia Recorded Future](#).”

Apoyo a los líderes de seguridad

Hemos mencionado en varias ocasiones que la inteligencia para los equipos de seguridad debe ser completa, relevante y contextualizada para que sea útil para los miembros de la organización de seguridad. Cuando se trata de CISO y otros líderes de seguridad, también tiene que ser conciso y oportuno.

Por ejemplo, la inteligencia proporciona a los responsables de seguridad una imagen en tiempo real de las últimas amenazas, tendencias y acontecimientos. Un panel de inteligencia fácil de usar (o algún otro formato “de un vistazo”) permite a los líderes de seguridad responder a una amenaza o comunicar el impacto potencial de un nuevo tipo de amenaza a los líderes empresariales y a los miembros de la junta directiva.



La inteligencia no es solo para los equipos de SecOps y los analistas de amenazas. Los responsables de seguridad también son consumidores clave de inteligencia. Piense en los tipos de información que los responsables de la seguridad necesitan a diario (por ejemplo, un cuadro de mando y una lista de los principales hallazgos de inteligencia del día anterior), a intervalos regulares (por ejemplo, resúmenes y tendencias para un informe de riesgos trimestral) y en caso de crisis (por ejemplo, información sobre ataques que acaban de ser detectados), y asegúrese de que los procesos y las herramientas de inteligencia están en marcha para satisfacer todas estas necesidades.

El déficit de competencias en materia de seguridad

Una de las responsabilidades de un CISO es asegurarse de que la organización de seguridad y TI cuente con el personal adecuado para llevar a cabo su misión. Sin embargo, el campo de la ciberseguridad tiene una escasez de habilidades ampliamente publicitada, y el personal de seguridad existente se encuentra a menudo bajo la presión de cargas de trabajo inmanejables.

La inteligencia proporciona una respuesta parcial al automatizar las tareas más intensivas en mano de obra, pero críticas, de la ciberseguridad, lo que libera el tiempo de las personas para las tareas intensivas en habilidades para las que están capacitadas. Por ejemplo, la inteligencia ayuda a priorizar el enorme volumen de alertas generadas por los SIEM y otras herramientas de seguridad, recopila y correlaciona rápidamente el contexto de múltiples fuentes y proporciona la inteligencia necesaria para comprender los riesgos.

Hacer que la inteligencia esté disponible en todas las funciones de seguridad ahorra una gran cantidad de tiempo, ya que los equipos de operaciones de seguridad y de respuesta a incidentes, los analistas de amenazas, los especialistas en gestión de vulnerabilidades y otro personal de seguridad reciben la inteligencia y el contexto que necesitan para tomar decisiones rápidas y seguras.

La potente inteligencia también permite que el personal más joven se perfeccione rápidamente y rinda por encima de su nivel de experiencia, por lo que el CISO no tiene que contratar a tantos profesionales senior.

Ciberseguridad basada en el riesgo: Una mejor manera de gestionar

Muchos equipos de seguridad se guían por las amenazas o por el cumplimiento. Los equipos orientados a las amenazas se centran en reaccionar ante las últimas amenazas de gran repercusión, tanto si suponen un riesgo real para la organización como si no. Por su parte, los equipos orientados al cumplimiento de la normativa destacan por marcar las casillas de las normas y marcos de cumplimiento.

Ninguna de las dos cosas maximiza la seguridad, y ambas dificultan las discusiones significativas con gerentes y ejecutivos que están mucho más interesados en las ganancias y las pérdidas que en las amenazas y el cumplimiento.

En su libro “El negocio del riesgo, lo que los CISO necesitan saber sobre la ciberseguridad basada en el riesgo”, Levi Gundert ofrece una alternativa mejor. Su concepto, denominado “ciberseguridad basada en el riesgo”, postula que:

- El riesgo es la posibilidad de que un acontecimiento acabe provocando una reducción de la rentabilidad.
- El riesgo de una ciberamenaza es cuantificable en términos monetarios con relativamente poco esfuerzo.
- El impacto neto de las actividades de mitigación puede calcularse comparando el coste de la mitigación con el ahorro previsto al mitigar el riesgo.

- Estos cálculos permiten a los programas de seguridad seleccionar las actividades que maximizan el impacto positivo en la rentabilidad de la organización.

¿Se le encendió una luz amarilla en la cabeza al oír las palabras “con relativamente poco esfuerzo” en el punto 2? Basándose en el trabajo de Douglas W. Hubbard y Richard Seiersen, Gundert ilustra cómo utilizar la estimación, la simulación y un marco de riesgo de categoría de amenaza (TCR) para cuantificar fácilmente las amenazas a una organización en términos monetarios.

Además de guiar a los equipos de seguridad hacia la asignación más eficaz de recursos y personal, la seguridad basada en el riesgo permite a los líderes de seguridad comunicarse con los ejecutivos en un lenguaje que entienden y aprecian: El lenguaje de los dólares y centavos.

“El negocio del riesgo, lo que los CISO necesitan saber sobre la ciberseguridad basada en el riesgo” está disponible para su descarga en <https://go.recordedfuture.com/the-risk-business>. Para obtener información adicional sobre cómo cuantificar el riesgo de ciberseguridad, lea el libro de Hubbard y Seiersen “[Cómo medir cualquier cosa en el riesgo de ciberseguridad](#).”

Capítulo 16

Inteligencia para priorizar las amenazas emergentes

En este capítulo

- Comprender cómo el seguimiento de los ciclos de vida de los ataques ayuda a las organizaciones a anticipar y priorizar las amenazas emergentes
- Conozca tres amenazas a las que hay que prestar atención: deepfakes, reclutamiento de personal interno y nuevas formas de vender bases de datos y acceso a la red

Planificar hoy el próximo año

Gran parte de este manual trata de cómo la inteligencia nos permite detectar y prevenir los ataques actuales y prepararnos para los que vendrán en los próximos meses. Pero la inteligencia también puede desempeñar un papel único al alertarnos de amenazas que quizás no surjan del todo hasta el año que viene o el siguiente.

La información sobre las amenazas emergentes y futuras es vital cuando las estrategias de mitigación tardan meses o años en aplicarse plenamente. Prepararse para un nuevo tipo de amenaza suele requerir aprender y probar nuevas tecnologías de seguridad, desarrollar nuevos procesos de detección y respuesta, y formar a los equipos y empleados de seguridad para que reconozcan los nuevos indicadores. Empezar temprano puede marcar la diferencia entre estar preparado con antelación y tener que luchar para ponerse al día, o peor aún, convertirse en una de las primeras víctimas.

En este capítulo analizamos cómo la inteligencia puede ayudar a las organizaciones a anticipar y priorizar futuras amenazas. A continuación, veremos tres ejemplos de amenazas emergentes y lo que la inteligencia puede decirnos sobre ellas en la actualidad:

- Deepfakes
- Contratación de información privilegiada para el fraude
- Nuevas formas de ofrecer a la venta bases de datos comprometidas y acceso a la red

Uso de los ciclos de vida de los ataques para evaluar los riesgos

Cada tipo de ataque tiene un ciclo de vida, o más exactamente, una serie de ciclos de vida conectados.

Ciclos de vida de la tecnología

Las tecnologías y herramientas utilizadas por los atacantes progresan desde las teorías, a las pruebas de concepto, a las implementaciones que son funcionales pero difíciles de usar, a los paquetes con características de facilidad de uso que pueden ser utilizados por personas con habilidades limitadas. Con el tiempo, las herramientas se mejoran y automatizan para desafiar la evolución de las defensas.

Ciclos de vida de los ecosistemas

La mayoría de los tipos de ataque son introducidos y empleados por primera vez por individuos, pero con el tiempo aumenta la especialización. Los diferentes actores de la amenaza se especializan en áreas como:

- Creación y mejora de herramientas para su uso en ataques
- Proporcionar infraestructura para lanzar ataques
- Lanzamiento y gestión de los ataques a lo largo de su ciclo de vida (piense en la atención al cliente)-136
- Procesamiento de pagos por ataques de ransomware y extorsión

- Venta de números de tarjetas de crédito y de la seguridad social, credenciales de acceso y propiedad intelectual robados a ciberdelincuentes y otros compradores

Hoy en día, las herramientas, la infraestructura e incluso la gestión de los ataques pueden obtenerse “como servicio” a bajo coste para un periodo de tiempo o un proyecto determinado.

En general, cuanto más avanzado y especializado es el ecosistema comercial desarrollado para un tipo de ataque, más extendido está su uso.

Dirigirse a los ciclos de vida

Muchos ataques comienzan dirigiéndose a un tipo de organización, a la vulnerabilidad de un producto o a una región geográfica. Con el tiempo, se extienden a empresas más o menos grandes, a nuevas industrias y a más regiones geográficas y hablantes de idiomas. En ocasiones, los analistas pueden observar la expansión que se está produciendo y anticipar la siguiente serie de objetivos.

Las ventajas de seguir los ciclos de vida de los ataques

Es posible rastrear las herramientas maliciosas, las tendencias de los atacantes y los ciclos de vida de los objetivos en la Dark Web y en fuentes de foros clandestinos. Las herramientas maliciosas comercializadas se discuten, comparten y venden a menudo. Los actores de la amenaza intercambian información sobre técnicas y objetivos y reclutan socios. A medida que los ecosistemas de ataque evolucionan, los analistas pueden observar los productos, servicios e información que se ofrecen, sus precios y sus fuentes. A medida que los participantes en esos ecosistemas se anuncian o solicitan servicios, los analistas pueden seguir los intereses de los actores de la amenaza para conocer sus planes y actividades, a menudo mucho antes de que estos se hagan públicos por las víctimas o los medios de comunicación.

Esta inteligencia puede ayudar a las organizaciones a identificar los tipos de ataques emergentes con mucha antelación, para que puedan adelantarse a la tecnología defensiva, los procesos y la formación. Los que tienen más presupuesto pueden incluso simular los ataques para perfeccionar sus defensas.

Veamos algunos ejemplos de amenazas emergentes que son relevantes hoy en día.



El seguimiento de los ciclos de vida de los ataques es también una buena manera de evitar la ansiedad innecesaria en la sala de juntas. Los medios de comunicación están llenos de historias de amenazas que pueden ser “emergentes” durante años, o que nunca se materializan. Las organizaciones pueden utilizar la inteligencia para priorizar correctamente los riesgos y calmar a los directivos que reaccionan ante el último susto mediático.

Deepfakes: la próxima frontera del fraude

Los deepfakes son imágenes y grabaciones alteradas digitalmente con algoritmos de aprendizaje automático para presentar a una persona conocida haciendo o diciendo algo que no hizo o dijo.

Las tecnologías para crear deepfakes se están convirtiendo en una mercancía, y las herramientas están ampliamente disponibles para fines amateurs y “recreativos”. Hasta ahora, los principales usos han sido fijar los rostros de las personas (famosos, amigos y enemigos) a los cuerpos de otras personas (normalmente desnudos).

Sin embargo, la prensa ha prestado mucha atención al potencial de la tecnología deepfake para ser utilizada en campañas de desinformación política. De hecho, ha habido casos en Malasia y Gabón en los que esto parece haber ocurrido (los enlaces a los informes sobre estos incidentes y otros mencionados en esta sección se incluyen en el informe que aparece en la sección “En la web” más abajo).

¿Una futura amenaza para los consumidores y las empresas?

Pero, ¿se adoptará la tecnología deepfake por parte de los ciberdelincuentes que se dirigen a consumidores y empresas? ¿Puede la inteligencia decir a las organizaciones si está justificado que empiecen a prepararse ahora para contrarrestar los deepfakes?

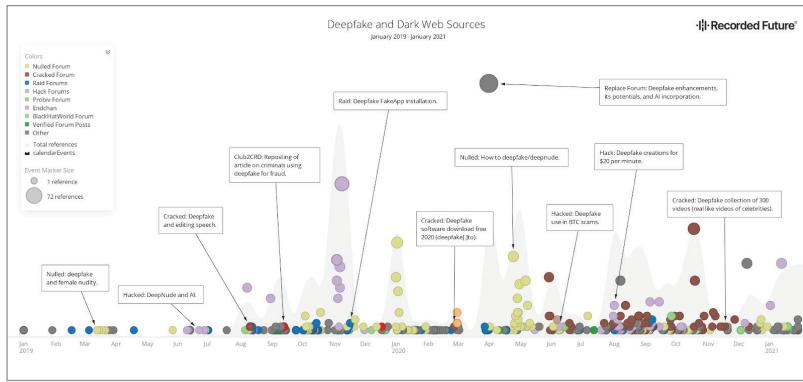


Figura 16-1: Referencias a las actividades de deepfake en fuentes de la Dark Web. (Fuente: Recorded Future)

La Figura 16-1 muestra que las referencias a las actividades de deepfake han aumentado significativamente en los últimos dos años, incluyendo las discusiones sobre el uso de la tecnología de deepfake para las campañas de fraude. Las principales ubicaciones de estas discusiones fueron los sitios web profundos en inglés y ruso, aunque los temas también se plantearon en foros en turco, español y chino.

Las actividades han empezado a superar la fase de debate. En los foros y mercados de la Dark Web se ofrece un número cada vez mayor de herramientas y servicios, entre los que se incluyen herramientas cada vez más potentes para crear rostros “intercambiados” y manipular fotos, vídeos y grabaciones de audio deepfake. Además, cada vez aparecen más foros en los que se comparten técnicas y experiencias para crear deepfakes avanzados y, en algunos casos, utilizarlos de forma poco ética.

Los actores de la amenaza han comenzado a ofrecer y solicitar servicios como:

- Sesiones de formación sobre cómo crear deepfakes
- Servicios de creación y edición de vídeos e imágenes Deepfake
- Servicios de creación de tarjetas y documentos bancarios fraudulentos con tecnología deepfake

Por último, han aparecido algunos ejemplos de fraudes perpetrados con tecnología deepfake. El director general de una empresa de energía con sede en el Reino Unido recibió una serie de tres llamadas telefónicas de lo que parecía el director general de la empresa matriz alemana de su empresa con órdenes de transferir 220 mil euros a la cuenta bancaria de un proveedor. Un director de banco en Hong Kong recibió una llamada telefónica aparentemente de un director de empresa con el que había hablado antes, pidiéndole que transfiriera 35 millones de dólares necesarios para una adquisición. De hecho, ambos eran deepfakes de audio cuidadosamente preparados.

Entonces, ¿qué nos dice la inteligencia sobre los deepfakes como amenaza emergente, y cómo deben responder las organizaciones?

- Las tecnologías de deepfake y los ecosistemas comerciales están madurando a un ritmo que hace que las actividades de deepfake relacionadas con el fraude sean una amenaza para las empresas que hay que tomar muy en serio.
- Las organizaciones deberían empezar a preparar estrategias de mitigación, como formar a los empleados clave para que reconozcan las deepfakes (al menos las menos sofisticadas), eliminar la autenticación solo por audio para las decisiones empresariales importantes y desplegar tecnologías de detección de deepfakes.
- Las organizaciones deben vigilar la deep web para detectar indicios de que las tecnologías y los ecosistemas de deepfake se están adaptando para realizar tareas como derrotar los métodos de autenticación basados en el reconocimiento facial y de voz, o crear contenidos sintéticos más convincentes para ataques de spearphishing e ingeniería social. Esto representaría graves amenazas para las prácticas de seguridad existentes y merecería un despliegue acelerado de contramedidas.



Para un análisis en profundidad de la aparición y el desarrollo de las actividades de deepfake en la Dark Web, lea el informe del Grupo Insikt de Recorded Future: [El negocio del fraude: Deepfakes, la próxima frontera del fraude](#).

Contratación de información privilegiada para el fraude

Los ataques internos han sido durante mucho tiempo un problema importante para las organizaciones de seguridad, pero la preocupación ha sido normalmente los empleados con un agravio

real o percibido contra su empleador, o bien los empleados que se marchan llevándose listas de clientes, diseños de productos y otra información de propiedad a sus nuevos empleadores.

Desgraciadamente, se ha abierto un nuevo frente en la guerra entre los ciberdelincuentes y los grupos de seguridad: el reclutamiento en línea de personas internas dispuestas a traicionar a sus empleadores.

El ejemplo más destacado que ha salido a la luz hasta ahora ha sido la contratación de un empleado de Tesla a través de WhatsApp. Le ofrecieron un millón de dólares en bitcoins para colocar un malware en la red de la compañía, un malware diseñado para robar datos de la enorme “Gigafactoría” de Tesla en Nevada. El grupo que estaba detrás del ataque planeaba exigir un cuantioso rescate para no filtrar la información de propiedad del fabricante de automóviles.

El empleado fue detenido antes de que el plan pudiera llevarse a cabo, pero su reclutador indicó que el grupo delictivo ya había realizado supuestamente varios “proyectos especiales” contra otras empresas.

Otros ciberdelincuentes han solicitado información privilegiada. El grupo de ransomware LockBit tuvo la inspiración (y el valor) de colocar un anuncio en las pantallas de los sistemas que habían bloqueado con el ransomware, donde podía ser leído por los empleados de la víctima y los consultores de seguridad contratados para hacer frente al ataque (ver cuadro de texto).

Extractos del mensaje de LockBit en el que se recluta a los iniciados

¿Le gustaría ganar millones de dólares?

Nuestra empresa adquiere acceso a las redes de varias empresas, así como información privilegiada que puede ayudarle a robar los datos más valiosos de cualquier empresa.

Puede proporcionarnos datos

contables para el acceso a cualquier empresa, por ejemplo, el nombre de usuario y la contraseña para RDP, VPN, correo electrónico corporativo, etc.

Las empresas nos pagan la ejecución de la hipoteca por el descifrado de los archivos y la prevención de la fuga de datos.

Estas actividades llevan el tema de los ataques internos a un nivel completamente nuevo. Una cosa es detectar a unos cuantos empleados descontentos y que saltan de un puesto a otro, que dependen de sus propios conocimientos técnicos, normalmente

limitados, para vengarse de su empleador o ganarse el favor de una nueva empresa. Otra cosa es que una sofisticada banda de delincuentes coloque millones de dólares delante de toda la plantilla.

Afortunadamente, la inteligencia puede mejorar en gran medida las probabilidades de detectar y bloquear la solicitud de información privilegiada:

- Alertar a las organizaciones de que la captación de información privilegiada es una amenaza requiere atención y cierto grado de priorización
- Descubrimiento de “charlas” en la Dark Web sobre los planes de captación de información privilegiada en determinados sectores, e incluso en determinadas empresas, y sobre las TTP que se utilizarán en los ataques
- Supervisión de las redes sociales para detectar campañas publicitarias dirigidas a los empleados de determinadas empresas

Venta de bases de datos y acceso a la red

Los ciberdelincuentes llevan muchos años vendiendo bases de datos robadas y acceso a redes específicas, pero recientemente los mercados de estos productos se han vuelto más sofisticados. Por ejemplo:

- Las bases de datos violadas se venden por partes, por ejemplo, combinaciones específicas de direcciones de correo electrónico, contraseñas, información financiera y PII.
- Las bases de datos robadas se están compartiendo gratuitamente en varios foros de la Dark Web.
- Los grupos criminales están ofreciendo el contenido de las bases de datos recientemente comprometidas mediante una suscripción mensual en la Dark Web y en plataformas de intercambio de archivos.

- La capacidad de acceder a redes comprometidas a través de credenciales robadas, software de terceros comprometido, protocolo de escritorio remoto (RDP), routers de Internet, ataques PowerShell y otros métodos se venden ahora a través de subastas, con precios iniciales, pasos de puja, comentarios sobre los vendedores y servicios de custodia para retener los fondos hasta que se completen las transacciones.

Un ejemplo especialmente preocupante es que los grupos de ransomware y otros actores de amenazas suelen comprar el acceso a la red de las organizaciones a los “intermediarios de acceso inicial”. Esta división del trabajo permite a los grupos de ransomware y a otros grupos acceder a más redes y lanzar más ataques de los que podrían haber conseguido por sí solos.

En muchos sentidos, estas innovaciones son buenas para los delincuentes y malas para las víctimas. Sin embargo, las organizaciones que pueden navegar por los nuevos mercados pueden reunir información que les ayude a identificar y corregir los puntos débiles de sus defensas.



Las bases de datos expuestas suelen contener direcciones de correo electrónico y contraseñas que pueden proporcionar una vía de acceso incluso a las organizaciones mejor defendidas. Para ver cómo una sola contraseña comprometida pudo derribar el mayor oleoducto de combustible de Estados Unidos y provocar escasez de gasolina en toda la costa este, lea Hackers Breached Colonial Pipeline Using Compromised Password. Para conocer las nuevas formas en que los ciberdelincuentes están monetizando las bases de datos comprometidas y el acceso a la red, lea el informe del Grupo Insikt de Recorded Future: Las violaciones de las bases de datos siguen siendo la principal amenaza cibernética para las organizaciones.

Estar al día con la Dark Web es difícil

La inteligencia de la Dark Web es extremadamente valiosa para los equipos de seguridad, pero obtenerla puede ser muy difícil. A muchos foros y mercados solo se puede acceder por invitación, y las invitaciones solo se conceden a personas con

la formación y los conocimientos lingüísticos adecuados (a veces a nivel de conocimiento de un dialecto específico). A los buenos les puede llevar años hacerse pasar por un hacker malintencionado para conseguir la credibilidad necesaria.

Sección 3: Creación y ampliación de su programa de inteligencia

Capítulo 17

Marcos analíticos para la inteligencia

En este capítulo

- Conozca las ventajas de utilizar marcos de inteligencia
- Comprender los puntos fuertes y débiles de los tres marcos más conocidos
- Vea cómo se complementan los tres marcos

Los marcos de inteligencia analítica proporcionan estructuras para pensar en los ataques y en los adversarios. Promueven una amplia comprensión de cómo piensan los atacantes, las TTP que utilizan y en qué momento del ciclo de vida de un ataque se producen eventos específicos. Este conocimiento permite a los defensores tomar medidas decisivas más rápidamente y detener a los atacantes antes.

Los marcos también centran la atención en los detalles que requieren una mayor investigación. Esta atención al detalle garantiza que las amenazas se han eliminado por completo y que se han establecido medidas para evitar futuras intrusiones del mismo tipo.

Por último, los marcos son útiles para compartir información dentro y entre equipos y organizaciones. Proporcionan una gramática y una sintaxis comunes para explicar los detalles de los ataques y cómo se relacionan entre sí. Un marco compartido facilita la incorporación de información de proveedores, foros de código abierto, centros de análisis e intercambio de información (ISAC) y otras fuentes.



Los marcos que se describen a continuación son complementarios, no competitivos. Puede optar por utilizar uno, dos o los tres.

La Cyber Kill Chain® de Lockheed Martin

La Cyber Kill Chain®, desarrollada por primera vez por Lockheed Martin en 2011, es uno de los primeros y más conocidos marcos de inteligencia en ciberseguridad. Se basa en el concepto militar de la cadena de muerte, que divide la estructura de un ataque en etapas. Al segmentar un ataque, los defensores pueden determinar en qué fase se encuentra y desplegar las contramedidas adecuadas.

La Cyber Kill Chain describe siete etapas de un ataque:

1. Reconocimiento
2. Armonización
3. Entrega
4. Explotación
5. Instalación
6. Mando y control
7. Acciones sobre los objetivos (a veces denominadas exfiltración)

Estas etapas suelen presentarse en un diagrama similar al de la Figura 17-1.

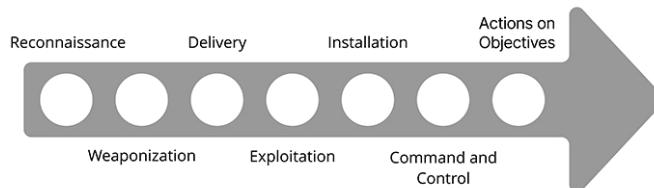


Figura 17-1: Diagrama del marco de la Cyber Kill Chain de Lockheed Martin. (Fuente: Lockheed Martin)

Los equipos de seguridad pueden optar por desarrollar respuestas estándar para cada etapa.

Por ejemplo, si se consigue detener un ataque en la fase de explotación, se puede tener una gran confianza en que no se ha instalado nada en los sistemas objetivo, y puede no ser necesaria una actividad completa de respuesta a incidentes.

La Cyber Kill Chain también permite a las organizaciones construir un modelo de defensa en profundidad que se dirige a partes específicas de la cadena de muerte. Por ejemplo, puede adquirir inteligencia específicamente para supervisar:

- Referencias a su organización en la web que indiquen actividades de reconocimiento
- Información sobre el armamento contra las nuevas vulnerabilidades reportadas en las aplicaciones de su red

Limitaciones de la Cyber Kill Chain

La Cyber Kill Chain es una buena manera de empezar a pensar en cómo defenderse de los ataques, pero tiene algunas limitaciones. Una de las principales críticas a este modelo es que no tiene en cuenta el funcionamiento de muchos ataques modernos. Por ejemplo, los adversarios pueden omitir por completo el reconocimiento si no tienen interés en dirigir los ataques contra determinados segmentos.

Sin embargo, incluso con sus limitaciones, la Cyber Kill Chain crea una base sólida para discutir los ataques y dónde detenerlos. También facilita el intercambio de información sobre los ataques dentro y fuera de la organización utilizando puntos de ataque estándar y bien definidos.

Para saber más sobre la Cyber Kill Chain, lea el [libro blanco seminal](#) y visite el sitio web de [Cyber Kill Chain](#).



El modelo del diamante

El Modelo Diamante fue creado en 2013 por investigadores del ya desaparecido Centro de Análisis de Inteligencia Cibernética e Investigación de Amenazas (CCIATR). Se utiliza para hacer un seguimiento de los grupos de ataques a lo largo del tiempo, más que del progreso de los ataques individuales.

En su forma más sencilla, el Modelo Diamante tiene un aspecto similar al de la Figura 17-2. Se utiliza para clasificar los diferentes elementos de un ataque. El diamante de un atacante o grupo de ataque no es estático, sino que evoluciona a medida que el atacante ajusta las TTP y cambia la infraestructura y los objetivos.

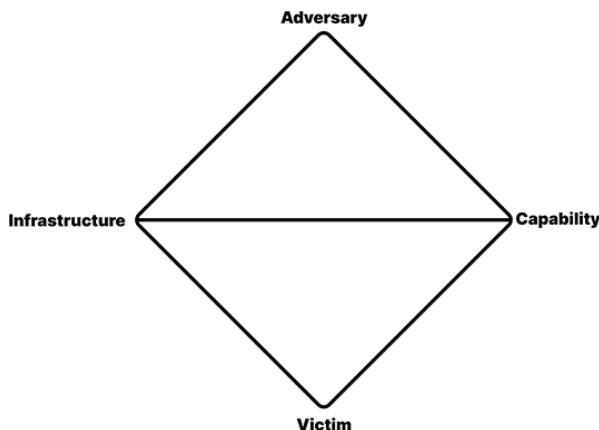


Figura 17-2: Un diseño sencillo del Modelo Diamante.
(Fuente: CCIATR)

El Modelo Diamante permite a los defensores rastrear a un atacante, las víctimas, las capacidades del atacante y la infraestructura que éste utiliza. Cada uno de los puntos del diamante es un punto de giro que los defensores utilizan durante una investigación para conectar un aspecto de un ataque con los demás.

Pivotante

Digamos que descubre el tráfico de comando y control hacia una dirección IP sospechosa. El Modelo Diamante le permitiría “pivotar” desde este indicador inicial para encontrar información sobre el atacante asociado a esa dirección IP, y luego investigar las capacidades conocidas de ese atacante. Conocer esas capacidades le permitirá mapear las herramientas y técnicas del adversario con mayor rapidez

y eficacia. O bien, imagine que su solución de inteligencia utiliza el Modelo Diamante. Si la junta directiva pregunta quién está lanzando ataques similares contra otras organizaciones de su sector (atribución), podrá encontrar rápidamente una lista de víctimas, el probable atacante y una descripción de las TTP de ese atacante. Esto le permitirá decidir qué defensas hay que poner en marcha.

Flexibilidad

Una de las mayores ventajas del Modelo Diamante es su flexibilidad y extensibilidad. Puede añadir diferentes aspectos de un ataque bajo el punto apropiado del diamante para crear perfiles complejos de diferentes grupos de ataque. Otras características de un ataque que puede ser rastreado incluyen:

1. Fase
2. Resultado
3. Dirección
4. Metodología
5. Recursos

Inconvenientes del modelo del diamante

El inconveniente es que los modelos Diamond requieren mucho mantenimiento. Algunos aspectos del modelo, especialmente las infraestructuras, cambian rápidamente. Si no se actualiza constantemente el diamante de un atacante, se corre el riesgo de trabajar con información obsoleta. Sin embargo, incluso con estos retos, el Modelo Diamante puede facilitar el trabajo de muchos responsables de seguridad al ilustrar respuestas rápidas sobre la evolución de las amenazas.



Marca la hora de cada actualización de un diamante para que todo el mundo que lo utilice tenga visibilidad sobre la antigüedad de la información.

Si no tiene tiempo ni recursos para gestionar este tipo de modelo usted mismo, puede obtener información actualizada de un proveedor de inteligencia externo.

Para obtener más información sobre el modelo del diamante, lea la entrada del blog de Recorded Future “[Aplicación de la inteligencia de seguridad al modelo del diamante del análisis de intrusiones](#)”, o descargue el libro blanco original “[El modelo del diamante del análisis de intrusiones](#).”

El marco MITRE ATT&CK™

MITRE es una organización única en Estados Unidos: Una empresa encargada de gestionar la financiación federal de proyectos de investigación en múltiples agencias federales. Ha tenido un gran impacto en la industria de la seguridad, incluyendo el desarrollo y mantenimiento de las bases de datos Common Vulnerabilities and Exposures (CVE) y Common Weakness Enumeration (CWE).

MITRE ha desarrollado otros marcos muy importantes para la inteligencia, entre ellos:

- El Intercambio Automatizado de Información de Inteligencia de Confianza (TAXII™): un protocolo de transporte que permite a las organizaciones compartir inteligencia a través de HTTPS y utilizar comandos comunes de la API para extraer esa inteligencia.
- Structured Threat Information eXpression (STIX™): un formato estandarizado para presentar la información
- El marco Cyber Observable eXpression (CybOX™): un método para rastrear los observables de los incidentes de ciberseguridad

Categorías de comportamiento de los atacantes

El marco de MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) fue creado como un medio para rastrear el comportamiento adversario en el tiempo. ATT&CK se basa en la Cyber Kill Chain, pero en lugar de describir un solo ataque, se centra en los indicadores y las tácticas asociadas a adversarios específicos.

ATT&CK utiliza 14 categorías de tácticas diferentes para describir el comportamiento del adversario:

1. Reconocimiento
2. Desarrollo de recursos
3. Acceso inicial
4. Ejecución
5. Persistencia
6. Escalada de privilegios

7. Evasión de la defensa
8. Acceso a las credenciales
9. Descubrimiento
10. Movimiento lateral
11. Colección
12. Mando y control
13. Exfiltración
14. Impacto

Cada una de estas categorías tácticas incluye técnicas individuales que describen el comportamiento del adversario. Por ejemplo, bajo la categoría de Acceso Inicial, los comportamientos incluyen “Adjunto de Spearphishing”, “Enlace de Spearphishing”, “Relación de confianza” y “Cuentas válidas”.



Véase el marco ATT&CK de MITRE Enterprise en https://attack.mitre.org/wiki/Main_Page.

Esta clasificación de los comportamientos permite a los equipos de seguridad ser muy detallados en la descripción y el seguimiento de los comportamientos adversos, y facilita el intercambio de información entre los equipos.

ATT&CK™ es útil en una amplia gama de funciones de seguridad, desde las operaciones de seguridad y el análisis de amenazas hasta la respuesta a incidentes. El seguimiento del comportamiento del adversario de forma estructurada y repetible permite a los equipos

- Priorizar la respuesta a los incidentes
- Mapa de indicadores a los atacantes
- Identificar agujeros en la postura de seguridad de la organización



Los marcos de inteligencia pueden utilizarse para estandarizar la forma en que sus equipos de seguridad examinan las amenazas, los indicadores, las vulnerabilidades y los actores. Si no está preparado para crear su propio marco de análisis, considere la posibilidad de asociarse con empresas de seguridad que ofrezcan soluciones basadas en marcos existentes. Este enfoque le permite disfrutar de las ventajas del marco y mejorar rápidamente la eficacia de sus actividades de seguridad.

Capítulo 18

Fuentes y tipos de datos de inteligencia: Un marco de trabajo

En este capítulo

- Conozca un marco para organizar las fuentes y tipos de datos de inteligencia
- Vea ejemplos de fuentes y tipos de datos para ataques de ransomware
- Revise cómo los datos de inteligencia pueden guiar las respuestas a cada fase de un ataque

Un marco para los datos de inteligencia

En el capítulo anterior hemos hablado de cómo los marcos de inteligencia analítica pueden ayudar a los equipos de seguridad a pensar sistemáticamente en los ataques y los adversarios, y hemos examinado tres de ellos. En este capítulo presentamos un marco desarrollado por Recorded Future que se centra en las fuentes de datos de inteligencia y los tipos de datos que pueden utilizarse para anticipar, detectar y responder a una amenaza específica.

La amenaza que utilizamos en este ejemplo es un “ataque de ransomware de doble extorsión”. Se trata de un ataque en el que los adversarios exfiltran copias de los archivos de datos antes de cifrar los originales para poder amenazar a las víctimas con la divulgación de datos sensibles, así como con la interrupción de su negocio. La Figura 18-1 muestra las cuatro etapas de un ataque de ransomware de doble extorsión con las fuentes de datos relevantes y los correspondientes tipos de datos de Recorded Future.

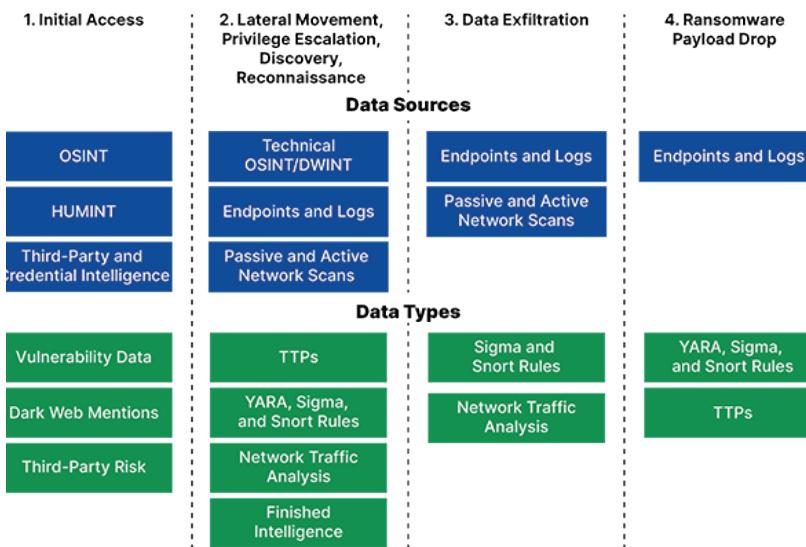


Figura 18-1: Fuentes de datos de inteligencia y tipos de datos para un ataque de ransomware de doble extorsión. (Fuente: Recorded Future)

Acceso inicial

Durante la fase de acceso inicial de un ataque de ransomware de doble extorsión (o cualquier otro tipo de ataque de ransomware), los adversarios intentan hacerse un hueco en la red de la organización víctima. Por lo general, acceden de una de estas maneras:

- Lanzar un ataque de phishing
- Explotación de una vulnerabilidad en el punto final o en una aplicación orientada a Internet
- Uso de credenciales robadas

OSINT

Para evitar el acceso inicial, las organizaciones pueden aprovechar la inteligencia de fuente abierta (OSINT), es decir, la información que se puede obtener en la web abierta y de otras fuentes públicas. Probablemente, los ejemplos más importantes son las bases de datos de vulnerabilidades, las pruebas de concepto publicadas sobre vulnerabilidades existentes y los informes de los medios de comunicación sobre ataques de día cero.

HUMINT

La inteligencia humana (HUMINT) relacionada con el acceso inicial incluye:

- Debates en foros de ciberseguridad, comunidades y centros de análisis e intercambio de información específicos del sector (ISAC)
- Charla en foros de la Dark Web
- Kits de exploits y herramientas de ransomware promocionados en mercados de la Dark Web

Esta información permite conocer las organizaciones y los sectores a los que se dirigen los ciberdelincuentes y las técnicas y herramientas que utilizan para atacar a las víctimas.

Inteligencia de terceros y credenciales

Hoy en día, los ciberdelincuentes a veces ponen en peligro a proveedores, contratistas y otros socios de la cadena de suministro débilmente defendidos, y luego emplean las credenciales robadas de ellos para acceder a su objetivo principal. También encuentran o compran credenciales en sitios de pasta y mercados de la Dark Web. La inteligencia de terceros y la inteligencia de identidad pueden ayudar a bloquear el acceso inicial desde estas vías, tal y como comentamos en los capítulos 9 y 13.

Respuestas

Las organizaciones pueden aprovechar estas fuentes y tipos de datos para frustrar el acceso inicial:

- Supervisión del correo electrónico en busca de palabras clave y otros indicadores de campañas de phishing utilizadas para los ataques de ransomware
- Parchear las vulnerabilidades que presentan las mayores amenazas para la organización
- Endurecimiento de las políticas y aumento de los requisitos de autenticación para los usuarios de alto riesgo
- Exploración de ataques dirigidos a organizaciones y productos de su cadena de suministro
- Supervisión de la Dark Web en busca de actores de amenazas que vendan acceso a su organización y a otras como la suya

Movimiento lateral, escalada y reconocimiento

Durante la segunda fase de un ataque de ransomware de doble extorsión, los adversarios exploran la red y los sistemas de la organización, buscando ampliar el alcance de su ataque a través de la red corporativa. Si los defensores detectan esta actividad, pueden trabajar para contener el ataque antes de que se produzcan más daños, por ejemplo, aislando las máquinas infectadas y evitando que el ransomware se propague por la red.

Técnica OSINT y DWINT

Como mencionamos en el capítulo 2, la inteligencia técnica (u operativa) incluye información como los vectores y las vulnerabilidades que se utilizan en los ataques, los indicadores de red asociados a los dominios de mando y control de los atacantes y otras TTP de los ciberdelincuentes. Este tipo de datos está disponible tanto en la OSINT como en la inteligencia de la Dark Web (DWINT) y puede mejorarse mediante el análisis técnico de datos de mando y control, muestras de malware y otros artefactos.

Puntos finales y registros

El movimiento lateral, la escalada de privilegios, el descubrimiento y el reconocimiento implican el uso de herramientas de código abierto, malware personalizado y herramientas nativas de los sistemas operativos que pueden dejar artefactos observables en la red, los puntos finales, los servidores y los dispositivos de red y seguridad. El conocimiento de las TTP de los atacantes y otros datos de inteligencia pueden orientar a los defensores sobre dónde buscar estos indicadores.

Además, se pueden encontrar pruebas sobre los ataques en curso desplegando reglas de YARA, Sigma y Snort para supervisar los sistemas de puntos finales, los registros y la red en busca de este tipo de comportamientos maliciosos. Estas reglas son firmas de malware y actividades maliciosas a nivel de archivo, registro y red, respectivamente, y pueden obtenerse de proveedores de inteligencia y organizaciones de ciberseguridad.



¿Qué son las reglas YARA, Sigma y Snort? Las reglas YARA describen cadenas y patrones de bytes únicos en archivos que los productos de seguridad pueden utilizar para identificar, clasificar y bloquear muestras de malware. Las reglas Sigma son firmas de amenazas para los SIEM. Permiten a los SIEM identificar los eventos de registro asociados a los ataques, como las conexiones a servidores de comando y control externos, los intentos de inicio de sesión en cuentas y el uso de herramientas de acceso remoto. Las reglas de Snort ayudan a los sistemas de detección y prevención de intrusiones a identificar escaneos, sondeos y otras actividades maliciosas basadas en la red. (Por cierto, YARA significa “Otro acrónimo recursivo/ridículo”).

El escaneos de red

Los registros pueden revelar mucha información sobre las etapas intermedias del ransomware y otros ataques, pero no todo. El escaneo de la red proporciona información adicional sobre las vulnerabilidades y la actividad de los atacantes.

Los escáneres de red pasivos “escuchan” el tráfico de red existente para identificar las aplicaciones activas, los puertos abiertos y las sesiones de red que indican actividades maliciosas, como la comunicación con sitios web externos y los intentos inusuales de acceder a datos sensibles. Los escáneres activos “hablan” en las redes y buscan vulnerabilidades, configuraciones incorrectas y otras debilidades de seguridad.

Los tarros de miel son otro tipo de técnica de escucha pasiva. Atrapan a los atacantes intentando navegar por una réplica falsa de la red de la organización. Los tarros de miel ofrecen un asiento de primera fila para conocer las TTP de los atacantes.

Inteligencia terminada

Las fuentes y tipos de inteligencia descritos anteriormente pueden producir miles de datos en poco tiempo. Pero juntar esas piezas y detectar patrones requiere mucho contexto y conocimiento de fondo. Por eso es importante dotar a los equipos de seguridad y de caza de amenazas de una inteligencia acabada que describa en profundidad los ataques y los métodos de ataque y destaque las novedades y las tendencias. La inteligencia terminada está disponible en organizaciones industriales, agencias gubernamentales y proveedores de servicios de inteligencia.

Resuestas

Las organizaciones pueden utilizar la inteligencia sobre el movimiento lateral, la escalada de privilegios, el descubrimiento y el reconocimiento para:

- Bloquear el tráfico de red hacia IP y URL maliciosas, como los servidores de comando y control y los sitios web que alojan herramientas maliciosas y cargas útiles de segunda etapa.
- Ajuste las reglas y políticas de los SIEM, los productos de seguridad para puntos finales y los sistemas de detección y prevención de intrusiones
- Cierre los puertos innecesarios en los sistemas orientados a Internet y restrinja el acceso a las aplicaciones y fuentes de datos con información sensible
- Crear líneas de base de los comportamientos de los sistemas de red y de los puntos finales y supervisar las desviaciones

Exfiltración de datos

Obviamente, es mucho mejor detener un ataque de ransomware de doble extorsión antes de que se exfiltren los datos. Sin embargo, detectar a los atacantes en el acto de exfiltración de datos permite a las organizaciones:

- Cortar el flujo de datos y limitar el alcance (“radio de explosión”) del ataque
- Bloquear o eliminar la carga útil del ransomware para evitar la parte de cifrado del ataque y prevenir la interrupción de la empresa

Puntos finales y registros

La exfiltración de datos puede detectarse a menudo mediante el análisis de registros y eventos en los puntos finales. El despliegue de reglas Sigma y Snort basadas en la inteligencia sobre el ransomware y otras amenazas puede ayudar a los SIEM y a los productos de detección y prevención de intrusiones a realizar estas tareas con mayor rapidez y precisión.

El escaneos de red

El análisis del tráfico de red basado en escaneos de red pasivos y activos también puede ayudar a identificar casos de exfiltración de datos, así como el tráfico de red hacia servidores externos y redes de bots utilizados en anteriores ataques de ransomware. Los analistas también pueden buscar actividades inusuales, como la exfiltración de grandes cantidades de datos a dominios y direcciones IP sospechosos o maliciosos.

Respuestas

Cuando se detecta una exfiltración de datos, es el momento de poner en marcha su plan de contención sin demora. Este proceso debe incluir:

- Bloquear todo el tráfico de red hacia y desde las máquinas infectadas y los sitios web externos asociados al ataque
- Analizar los datos de los puntos finales y de los registros para determinar el punto de acceso inicial y qué sistemas se han visto comprometidos
- Poner en cuarentena los sistemas comprometidos y eliminar el malware y las herramientas maliciosas, incluido el código utilizado para exfiltrar datos y la carga útil del ransomware
- Determinar qué datos han sido exfiltrados y tomar las medidas adecuadas para cambiar las credenciales y notificar a las partes interesadas

Caída de la carga útil del ransomware

La fase final de un ataque de ransomware de doble extorsión consiste en soltar la carga útil del ransomware en puntos finales y servidores de la red, cifrar los archivos y enviar las peticiones de rescate.

En algunos ataques de ransomware todo esto ocurre en un periodo muy corto, y la organización víctima no tiene tiempo para contener la propagación. Sin embargo, en otros casos las actividades se extienden, y la detección temprana puede permitir a los equipos de seguridad contener la propagación.

Puntos finales y registros

La mayoría de las actividades maliciosas en esta fase del ataque se producen en los puntos finales y en los servidores, por lo que la mejor forma de obtener una alerta temprana es analizar los cambios que se producen en ellos. Las actividades asociadas al malware incluyen:

- Acceso y modificación de archivos en un volumen inusual
- Desactivación de las herramientas de seguridad
- Eliminar o modificar las copias de seguridad
- Interferir con los procesos y servicios que facilitan la recuperación

Al igual que en las fases anteriores, la inteligencia incrustada en las reglas de YARA, Sigma y Snort puede desempeñar un papel importante al permitir que los productos antimalware, los SIEM y los sistemas de detección y prevención de intrusiones identifiquen comportamientos maliciosos y proporcionen inteligencia que pueda utilizarse después de la infracción.

Esta es también un área en la que la inteligencia sobre las TTP de los atacantes puede desempeñar un papel vital al proporcionar a los equipos de seguridad información oportuna sobre lo que los atacantes harán a continuación.

Un marco flexible

Esta discusión ha cubierto solo un ejemplo de un marco para las fuentes y tipos de datos de inteligencia. El marco variará para otros tipos de ataques, con menos o más fases y diferentes formas de inteligencia. Pero en cualquier escenario de ataque, el proceso de creación de dicho marco ayudará a su equipo:

- Identificar y las mejores fuentes de inteligencia para cada fase del ataque, y obtener acceso a ellas
- Identificar los tipos de datos más útiles y establecer herramientas y procesos para capturar, analizar, presentar y difundir la información clave
- Conseguir un consenso sobre las prioridades para adquirir y utilizar la información

Capítulo 19

Su viaje de inteligencia

En este capítulo

- Examine las formas de aclarar sus necesidades y objetivos de inteligencia
 - Explore los factores clave de éxito que contribuyen a la eficacia de los programas
 - Aprenda a empezar de forma sencilla y a ampliar la escala
-

En este capítulo, sugerimos algunas de las mejores prácticas para trazar su viaje de inteligencia y construir un programa de inteligencia integral.

No comience con las alimentaciones de las amenazas

Muchas organizaciones comienzan sus programas de inteligencia suscribiendo feeds de datos de amenazas y conectándolos con una solución SIEM. Esto puede parecer una forma lógica de empezar porque muchas fuentes de datos sobre amenazas son de código abierto (es decir, gratuitas), y los indicadores técnicos que ofrecen parecen útiles y fáciles de interpretar. Dado que todo el malware es malo, y que cada URL sospechosa podría ser utilizada por un atacante, cuantas más pistas tenga sobre ellas, mejor, ¿verdad?

En realidad, la gran mayoría de los resultados de los honeypots, las muestras de malware y las URL sospechosas no son relevantes para las amenazas actuales de su organización. Por eso, alimentar su SIEM con grandes volúmenes de datos de amenazas sin filtrar creará casi con toda seguridad más alertas que respuestas y, en última instancia, el tipo de fatiga por alertas que examinamos en el capítulo 4.

Aclare sus necesidades y objetivos de inteligencia

Dado que la inteligencia proporciona valor a muchos equipos de su organización, es importante desarrollar prioridades que reflejen con precisión las necesidades y objetivos generales de la organización.

Responde a estas preguntas

Desarrolle un conjunto claro de objetivos determinando las necesidades de cada grupo de seguridad en su organización y las ventajas que la inteligencia les proporcionará.

Comience por considerar estas preguntas:

- ¿Cuáles son sus mayores riesgos?
- ¿De qué manera necesita la inteligencia para hacer frente a cada uno de esos riesgos?
- ¿Cuál es el impacto potencial de abordar cada riesgo?
- ¿Qué lagunas hay que cubrir con información, tecnología o personas para que la inteligencia sea eficaz en esos ámbitos?



Para una visión completa del poder de la inteligencia, descargue “[El kit de inteligencia de seguridad definitivo](#).” Esta colección curada de libros blancos, informes, videos, podcasts y más describe en detalle cómo funciona la inteligencia y todas las formas en que beneficia a su organización.

Identifique cuáles de sus equipos se beneficiarán de la inteligencia

Los equipos de toda la organización se beneficiarán de la inteligencia que impulsa la toma de decisiones informadas y proporciona perspectivas perspicaces. La inteligencia que es completa, relevante y fácil de consumir tiene el potencial de revolucionar la forma en que los diferentes roles de su organización operan día a día. A la hora de determinar cómo avanzar en su estrategia de inteligencia, es importante identificar a todos los usuarios potenciales de su organización y alinear la inteligencia con sus casos de uso únicos. Asegúrese de pensar también fuera de su organización de seguridad, porque grupos como el jurídico, el de recursos humanos, el de informática y el

de operaciones comerciales también se benefician de la inteligencia.



Desglose los resultados de la inteligencia que utilizará cada grupo y cómo se beneficiarán exactamente en términos de tiempos de respuesta, ahorro de costes, eficiencia del personal, decisiones de inversión, etc. Las necesidades y los beneficios no siempre son evidentes. Documentar estos detalles le permitirá establecer prioridades, justificar inversiones y encontrar nuevos usos para la inteligencia.

Factores clave del éxito

Hay varios factores que suelen contribuir a la eficacia de los programas de inteligencia. Cuanto antes las ponga en práctica, más rápido se dará cuenta de todo el valor de la inteligencia.

Generar ganancias rápidas con la supervisión

La supervisión de la información de seguridad suele proporcionar beneficios rápidos con inversiones relativamente modestas. La clave es buscar unos pocos tipos de datos que sean especialmente significativos para su negocio y su estrategia de seguridad de la información para anticiparse a las amenazas emergentes y proporcionar alertas tempranas de ataques reales. Estas actividades podrían incluir:

- Comprobación de nuevas vulnerabilidades que afectan a sus paquetes de software, servidores y puntos finales más importantes
- Seguimiento de las tendencias de las amenazas que suponen riesgos potenciales para las operaciones de su empresa
- Vigilancia de cualquier credencial, dato o código corporativo filtrado que aparezca en sitios web públicos u oscuros
- Buscar en la web y en las redes sociales los nombres de su organización y sus marcas, unidades de negocio y productos

Es probable que haya algunos tipos de datos de vital importancia para su empresa que sean posibles de supervisar sin invertir en nueva infraestructura o personal. De este modo, es probable que se generen ganancias rápidas, se demuestren las ventajas de la inteligencia y se genere entusiasmo por el programa.

Garantizar la utilidad de los informes

Muchas organizaciones caen en la rutina de elaborar informes diarios que son poco o nada útiles. A menudo se trata de listas con viñetas de amenazas detectadas con una simple calificación de impacto bajo/medio/alto. Aunque estos informes demuestran que los analistas se mantienen ocupados y aumentan la concienciación sobre las ciberamenazas en toda la organización, normalmente no tienen ningún impacto en los resultados operativos.

No se preocupe por la elaboración de informes según un calendario. En su lugar, asegúrese de que todos los informes y comunicaciones que elabore contengan información y conocimientos que capaciten a las partes afectadas para tomar decisiones y emprender las acciones adecuadas. Lo ideal es que incluyan al menos información básica sobre:

- Los probables actores de la amenaza
- Técnicas y herramientas utilizadas por el o los actores de la amenaza
- Objetivos probables en la organización
- Si la amenaza representa un peligro real para la organización
- La probabilidad de que los controles de seguridad existentes sean capaces de mitigar la amenaza
- Acciones recomendadas para responder

Automatizar todo lo posible

Los programas de inteligencia eficaces suelen centrarse en la automatización desde el principio. Empiezan por automatizar tareas fundamentales como la agregación de datos, la comparación, el etiquetado y la contextualización. Cuando estas tareas las realizan las máquinas, los humanos se liberan para centrarse en tomar decisiones eficaces e informadas.

A medida que su programa de inteligencia se vuelve más sofisticado, puede encontrar aún más oportunidades de automatización. Podrá automatizar el intercambio de información entre un grupo más amplio de soluciones de seguridad y automatizar más flujos de trabajo que proporcionen inteligencia a los equipos de operaciones de seguridad y

respuesta a incidentes, a los analistas de amenazas, a los equipos de prevención de fraudes, a los especialistas en gestión de vulnerabilidades, a los gestores de riesgos de terceros y a los defensores de la marca. Podrá descargar más trabajo de gran volumen a sus soluciones de inteligencia haciendo que el software correlacione automáticamente los datos de las amenazas, produzca puntuaciones de riesgo, identifique los falsos positivos y mucho más.

PRECAUCIÓN

Cuando evalúe las soluciones de inteligencia, examine el nivel en que emplean la automatización. ¿La automatización se limita a agregar y cruzar datos, o la solución añade un contexto que equipa a sus equipos para tomar decisiones basadas en el riesgo con confianza? Tenga en cuenta que la introducción de más datos en bruto en su software de inteligencia solo añade valor si se analizan, organizan y entregan automáticamente en un formato fácil de consumir con contexto.

Integrar la inteligencia con los procesos y la infraestructura

Integrar una solución de inteligencia en los sistemas existentes es una forma eficaz de hacer que la inteligencia sea accesible y utilizable sin abrumar a los equipos con nuevas tecnologías.

Una parte fundamental de la integración consiste en garantizar que su solución de inteligencia tenga visibilidad sobre los eventos y actividades de seguridad capturados por sus herramientas de seguridad y de red existentes. La combinación y correlación de puntos de datos internos y externos produce una auténtica inteligencia que es relevante para su negocio y se sitúa en el contexto de un panorama de amenazas más amplio.

El otro aspecto crítico de la integración es ofrecer la información más importante, específica, relevante y contextualizada al grupo adecuado en el momento adecuado. Para lograrlo, integre su solución de inteligencia con su SIEM y otras herramientas de seguridad, ya sea a través de API o mediante interfaces desarrolladas en colaboración con los proveedores de herramientas de seguridad.

SUGERENCIA

Cuando se evalúan las soluciones de inteligencia, es importante entender cuáles se integran fácilmente con el software existente y son compatibles con los casos de uso de los equipos de seguridad.

Conseguir que los expertos nutran a los expertos internos

El valor que se obtiene de la inteligencia está directamente relacionado con su capacidad para hacerla relevante para su organización y aplicarla a los procesos de seguridad existentes y nuevos.

Alcanzará estos objetivos más rápidamente si trabaja con un proveedor o consultor que proporcione capacidades técnicas y experiencia que permitan a su organización sacar el máximo provecho de la inteligencia. Con el tiempo, trabajar con un socio de este tipo permitirá a los miembros de su equipo convertirse en expertos en inteligencia por derecho propio.



Busque socios que tengan un amplio y profundo banco de expertos en inteligencia. Estos especialistas deben tener los conocimientos y la experiencia necesarios para comprender sus necesidades a fin de ayudarle a obtener el máximo valor de su inversión. Asegúrese de que estarán disponibles cuando recurra a su experiencia, y de que trabajarán con usted para identificar nuevas ventajas de aprovechar la inteligencia en su organización. Los socios que elija deben estar comprometidos con su éxito actual y seguir apoyando a sus equipos de seguridad a medida que avanza.



Encuentre más información sobre la selección de la solución de inteligencia adecuada descargando “[La Guía del Comprador de Inteligencia](#),” de Recorded Future. Incluye una práctica plantilla de solicitud de propuestas que se puede utilizar para evaluar las capacidades de los distintos proveedores.

Empezar de forma sencilla y aumentar la escala

La inteligencia no es un monolito que deba caer en la organización de seguridad de una sola vez. En cambio, tiene opciones en cuanto a la forma de recopilar, procesar, analizar y difundir la información a las distintas partes interesadas y grupos.

Puede optar por empezar de forma sencilla con su personal actual (en lugar de crear un equipo de inteligencia dedicado), unas pocas fuentes de datos y la integración con las herramientas de seguridad existentes, como su SIEM y su sistema de gestión de vulnerabilidades. Pronto podrá beneficiarse de la ampliación

con personal dedicado, más fuentes de datos, más integraciones de herramientas y más flujos de trabajo automatizados, como se muestra en la Figura 19-1.

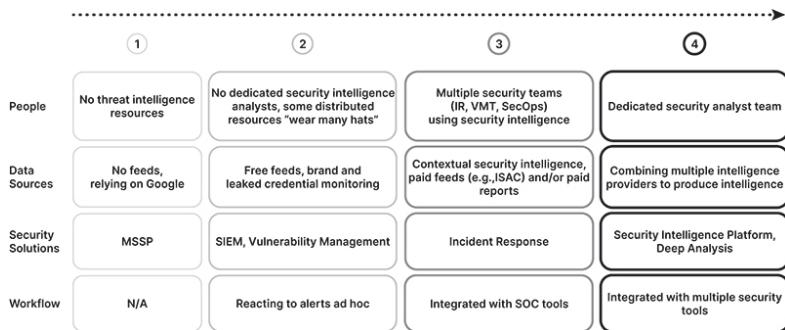


Figura 19-1: Cuatro etapas de madurez del programa de inteligencia: desde la ausencia de recursos internos hasta un programa totalmente dotado de personal y altamente automatizado.

(Fuente: Recorded Future)

Comience su viaje investigando las necesidades de cada grupo en su organización de seguridad y determinando cómo la inteligencia les permitirá alcanzar sus objetivos.

Con el tiempo, podrá construir un programa de inteligencia integral que:

- Busca la mayor variedad posible de fuentes técnicas, abiertas y de la Dark Web
- Utiliza la automatización para ofrecer inteligencia fácilmente consumible
- Proporciona alertas totalmente contextualizadas en tiempo real con un número limitado de falsos positivos
- Se integra con sus otras tecnologías y procesos de seguridad y los mejora
- Mejora sistemáticamente la eficiencia y la eficacia de toda su organización de seguridad

Capítulo 20

Desarrollar su equipo central de inteligencia

En este capítulo

- Comprenda los procesos, las personas y la tecnología que conforman una capacidad de inteligencia dedicada
- Conozca cómo estos equipos utilizan la inteligencia para juzgar el riesgo e impulsar la continuidad del negocio
- Revise las formas de colaboración con las comunidades de inteligencia

Hemos visto cómo la inteligencia beneficia a sus equipos de seguridad. A continuación, algunas sugerencias sobre cómo organizar su equipo principal dedicado a la inteligencia.

Dedicados, pero no necesariamente separados

Como ya comentamos en el capítulo anterior, es posible que quiera comenzar su viaje de inteligencia con personas que sigan desempeñando otras funciones en diferentes equipos de seguridad de la organización.

Al final, es probable que surjan dos preguntas:

1. ¿Debe haber un equipo de inteligencia dedicado?
2. ¿Debe ser independiente o vivir dentro de un grupo de seguridad existente?

Las respuestas son: Sí, y depende.

Lo mejor es un equipo dedicado

A medida que desarrolle un programa integral de inteligencia, necesitará crear un equipo que se dedique a recopilar y analizar datos sobre amenazas y convertirlos en inteligencia. El único objetivo de este equipo será proporcionar información relevante y procesable a los principales interesados, incluidos los altos ejecutivos y los miembros del consejo de administración.

Se requiere dedicación y una perspectiva amplia para garantizar que los miembros de su equipo dediquen suficiente tiempo a la recopilación, el procesamiento, el análisis y la difusión de la inteligencia que proporciona el mayor valor a la organización en su conjunto. Es fundamental evitar la tentación de centrarse en las necesidades de inteligencia de un solo grupo por encima de cualquier otro.

El lugar que ocupa el equipo depende de su organización

Contar con un equipo de inteligencia con independencia organizativa (que en la Figura 20-1 se muestra como el director y el equipo de SI) tiene sus ventajas, como una mayor autonomía y prestigio.

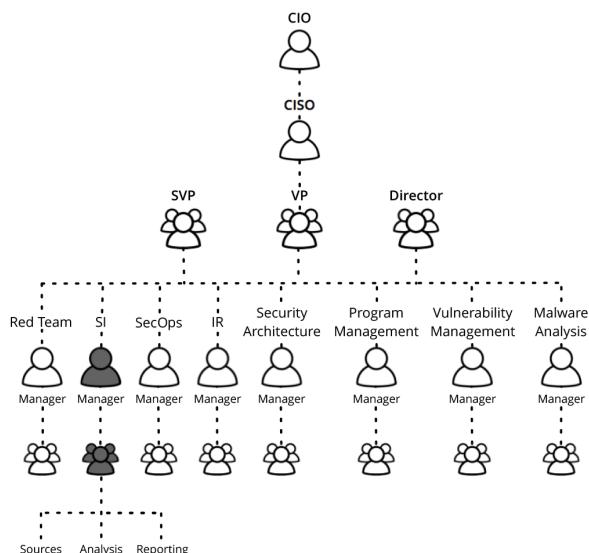


Figura 20-1: Inteligencia como un grupo independiente en la estructura organizativa de la seguridad (se muestra como el director y el equipo de SI).

Sin embargo, estas ventajas pueden verse completamente contrarrestadas por los problemas políticos asociados a la creación de un equipo con un nuevo gestor de alto nivel y su propio presupuesto que saca a los analistas cualificados de sus grupos existentes.

Un equipo de inteligencia dedicado no tiene que ser necesariamente una función separada que dependa directamente de un vicepresidente o del CISO, especialmente cuando se está empezando. En cambio, puede pertenecer a un grupo que ya trabaja con inteligencia. En muchos casos será el equipo de operaciones de seguridad o de respuesta a incidentes. Adoptar este enfoque suele ser una opción viable para evitar conflictos con los equipos de seguridad atrincherados.

Elegir a las personas

Si adopta un enfoque gradual para crear su equipo principal de inteligencia, comience con personas que ya forman parte de la organización de seguridad y que actualmente están aplicando la inteligencia a sus áreas particulares de experiencia. Puede que no tengan el título de “analista de inteligencia” o que no se vean a sí mismos de esa manera al principio,

pero es probable que sean las personas más capaces disponibles para formar la columna vertebral de su grupo de inteligencia emergente. Aunque puede contratar a recién licenciados con títulos de ciberseguridad, no recomendamos este enfoque, porque la experiencia en redes y seguridad es muy valiosa para un nuevo equipo, sobre todo al principio de un programa.

Competencias básicas

La función de inteligencia existe para fortalecer a todos los demás equipos de seguridad, capacitando a todos para proteger mejor a toda la organización. Es fundamental que el equipo de inteligencia incluya a personas que comprendan la actividad principal, los flujos de trabajo operativos, la infraestructura de red, los perfiles de riesgo y la cadena de suministro, así como la infraestructura técnica y las aplicaciones de software de la organización.

A medida que el equipo de inteligencia vaya madurando, es posible que quiera añadir miembros que sean expertos en:



Correlación de los datos externos con la telemetría interna

- Ingeniería inversa del malware y reconstrucción de los ataques (análisis forense)
- Proporcionar conocimiento de la situación de las amenazas y recomendaciones para los controles de seguridad
- Cazar proactivamente las amenazas internas, incluidas las amenazas internas
- Ingeniería de datos y generación de firmas para Yara, SIGMA u otros conjuntos de reglas
- Educar a los empleados y clientes sobre las ciberamenazas
- Compromiso con la comunidad de inteligencia en general
- Identificar y gestionar las fuentes de información

También es posible que desee añadir personal con diversos antecedentes, incluida la experiencia fuera de la tecnología de la información. En particular:

- Los analistas con formación militar y de inteligencia** suelen saber cómo estructurar los procesos de recopilación, análisis e información de datos, cómo ajustar los sesgos de las fuentes y cómo presentar la información y las conclusiones de forma clara, concisa y adaptada a su público.
- Los miembros del personal con experiencia** en la aplicación de la ley tienen conocimientos sobre las tácticas y métodos criminales, y son eficaces a la hora de distinguir los hechos de las opiniones.

Recogida y enriquecimiento de datos sobre amenazas

En el capítulo 2 hablamos de las fuentes de datos. Aquí exploramos cómo trabajar con una serie de fuentes para garantizar la precisión y la relevancia.

La ventaja humana

Los proveedores de inteligencia suelen proporcionar algunos tipos de inteligencia estratégica, pero también puede desarrollar

capacidades internas para recopilar información sobre los temas y eventos más relevantes para su organización.

Por ejemplo, puede decidir desarrollar un rastreador web interno que analice el código de las páginas web de los 5000 destinos web más visitados por sus empleados. Este análisis podría proporcionar información sobre el potencial de los ataques drive-by download. Podría compartir los conocimientos con el equipo de arquitectura de seguridad para ayudarles a proponer controles que defiendan contra esos ataques. Este tipo de inteligencia genera datos concretos, que son mucho más útiles que las anécdotas, las conjeturas y las estadísticas genéricas sobre los ataques.

Fuentes adicionales

Entre las fuentes propias que pueden reforzar sus recursos de inteligencia se encuentran:

- Alimentación del proveedor o del ISAC
- Permitir listas
- Listas de denegación
- Investigación del equipo de inteligencia

Combinación de fuentes

Una solución de inteligencia automatizada permite a los equipos de seguridad centralizar, combinar y enriquecer los datos procedentes de múltiples fuentes, antes de que los datos sean introducidos por otros sistemas de seguridad o vistos por los analistas humanos de los equipos de operaciones de seguridad.

La Figura 20-2 muestra los elementos de una solución automatizada contra las amenazas de este tipo. En este proceso, la información de un proveedor de inteligencia se filtra para encontrar los datos que son importantes para la organización y los equipos de seguridad específicos. A continuación, se enriquece con datos procedentes de fuentes de inteligencia internas y se emite en formatos adecuados para herramientas como el SIEM, el sistema de tickets, etc. Esta traducción automatizada de los datos brutos en conocimientos relevantes es la esencia de la inteligencia.

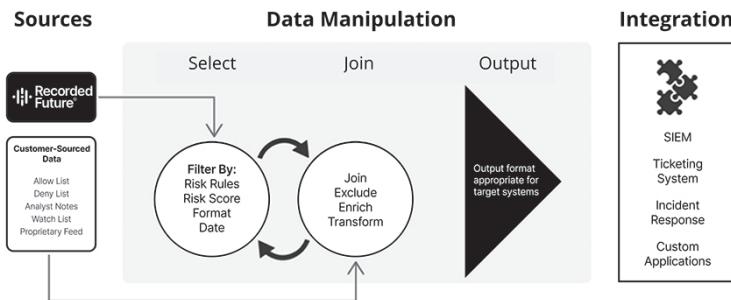


Figura 20-2: Una plataforma de inteligencia centraliza, combina y enriquece los datos, y luego los formatea para múltiples sistemas de destino. (Fuente: Recorded Future)

El papel de las máquinas inteligentes

Hemos llegado a un punto en el que los componentes automatizados han aprendido con éxito el lenguaje de las amenazas y son capaces de identificar con precisión los términos maliciosos.

Los avances en la analítica y el procesamiento del lenguaje natural (PLN) aportan ventajas adicionales al equipo de inteligencia. Con la tecnología adecuada, las referencias a las amenazas de todas las fuentes pueden convertirse en lenguaje neutro. Esto permite a los humanos y a las máquinas analizarlas, independientemente de la lengua original en la que aparecieron las referencias.

La combinación de análisis y PLN ofrece enormes oportunidades para que las organizaciones aprovechen la inteligencia. Estas tecnologías no solo eliminan las barreras lingüísticas, sino que también tienen el potencial de reducir la carga de trabajo de los analistas al asumir muchas tareas relacionadas con la recopilación y correlación de datos. Cuando se combinan con el poder de considerar múltiples datos y fuentes de información simultáneamente para producir verdadera inteligencia, estas capacidades hacen mucho más fácil construir un mapa comprensible del panorama de las amenazas.

Compromiso con las comunidades de inteligencia

La inteligencia no puede florecer en el vacío. Las relaciones externas son esenciales para el éxito de los equipos de inteligencia. Por muy avanzado que sea su equipo, ningún grupo es tan inteligente como el mundo de la inteligencia en su conjunto.

Muchas comunidades de inteligencia permiten a las organizaciones individuales compartir datos relevantes y oportunos sobre ataques, lo que permite a otros miembros proteger sus organizaciones antes de que sean víctimas. Colaborar con comunidades de confianza, como los ISAC, es crucial para disminuir el riesgo, no solo para su organización individual, sino también para toda la industria y el mundo cibernético en general. La participación requiere tiempo y recursos, como la comunicación con los compañeros por correo electrónico y la asistencia a conferencias sobre seguridad. Sin embargo, la construcción de relaciones debe ser una prioridad para que la inteligencia tenga éxito.

Conclusión

Utilizar la inteligencia para desbaratar a los adversarios

Ideas fundamentales del libro

Este libro parte de la idea de que la inteligencia es valiosa para todos en todas las funciones de seguridad, y más allá. La inteligencia permite a los equipos anticiparse a las amenazas, responder más rápidamente a los ataques y tomar mejores decisiones para reducir el riesgo. A lo largo de este libro, examinamos cómo adoptar un enfoque proactivo e integral de la seguridad aplicando la inteligencia a varias facetas de la estrategia de seguridad de su organización.

Eso es la inteligencia: un enfoque que amplía la eficacia de los equipos y las herramientas de seguridad exponiendo las amenazas desconocidas, informando de mejores decisiones e impulsando un entendimiento compartido para acelerar la reducción de riesgos en toda la organización. Los nueve pilares de la inteligencia de SecOps, la inteligencia de vulnerabilidades, la inteligencia de amenazas, la inteligencia de terceros, la inteligencia de marca y la inteligencia geopolítica, junto con la inteligencia de fraude, la inteligencia de identidad y la inteligencia de superficie de ataque recientemente introducidas, proporcionan a las organizaciones una poderosa visión de los riesgos a los que se enfrentan, al tiempo que agilizan la forma de trabajar de sus equipos.

¿Qué resultados obtendrá cuando adopte estos principios?

1. Desbaratará a los adversarios que tengan como objetivo su organización.

Si identifica a los adversarios más peligrosos para su organización y comprende cómo funcionan, pondrá las defensas adecuadas y hará la vida de los atacantes tan difícil que desistirán de sus esfuerzos por atacarle.

2. Obtendrá el contexto necesario para tomar decisiones informadas y actuar.

Al generar y consumir inteligencia contextual que es oportuna, clara y procesable, usted enriquecerá su conocimiento, simplificará los procesos de toma de decisiones y amplificará el impacto de todas sus soluciones de seguridad.

3. Su personal y sus máquinas trabajarán juntos para aumentar la eficacia general.

Las máquinas procesan y clasifican los datos brutos a una velocidad y escala extraordinarias, lo que permite a los humanos disponer del tiempo y el contexto necesarios para realizar un análisis intuitivo y de gran alcance. Al mejorar los flujos de trabajo humanos y automatizados, la inteligencia ahorrará tiempo y dinero, reducirá el desgaste humano y mejorará la seguridad en general.

4. Sus equipos de seguridad – y muchos otros en su organización – trabajarán de forma más inteligente.

Todos los equipos de seguridad, así como los ejecutivos y colegas de toda su organización -desde la gestión de riesgos y la prevención del fraude hasta la gestión de marcas y el riesgo de terceros, y más allá- recibirán más inteligencia relevante y menos datos brutos irrelevantes. Podrán interactuar con la inteligencia adecuada en el momento oportuno, en formatos fáciles de entender, a través de las herramientas de seguridad y colaboración existentes. Estarán capacitados para tomar mejores decisiones, más rápidamente.

Una de las grandes ventajas de la inteligencia es que permite ampliar el programa por etapas. Empiece por mejorar la eficacia de las actividades principales en las operaciones de seguridad, la respuesta a incidentes, la gestión de vulnerabilidades y la inteligencia sobre amenazas, o simplemente construya nuevas bases para los programas cada vez más importantes relacionados con el riesgo de terceros, la protección de la marca y la seguridad geopolítica. En cualquier caso, conseguirá ganancias cuantificables para su organización en cada paso. Esperamos que este manual le haya proporcionado una visión del vasto potencial de la inteligencia, iy de cómo lograrlo!

La inteligencia representa un elemento esencial para todo programa de seguridad, necesaria para poder mitigar los riesgos de manera constante y proactiva. Independientemente de la función de seguridad que desempeñe, la inteligencia permite tomar decisiones más inteligentes y rápidas. No es un dominio separado de la seguridad. Es el contexto que le permite trabajar de forma más inteligente, ya sea para dotar de personal a un SOC, gestionar las vulnerabilidades o tomar decisiones empresariales de alto nivel.

Descubra las distintas formas en que la inteligencia aporta valor a toda la empresa:

- **Inteligencia sobre SecOps:** acelere el triaje y permita que se dé respuesta a los incidentes de forma proactiva.
- **Inteligencia sobre vulnerabilidades:** priorice la aplicación de parches en función de la importancia real y la posibilidad de explotar las vulnerabilidades.
- **Inteligencia sobre amenazas:** aproveche el conocimiento de las tácticas, técnicas y procedimientos de los atacantes para reforzar las defensas de seguridad.
- **Inteligencia para responsables de seguridad:** visualice el amplio panorama de amenazas para evaluar el riesgo y tomar decisiones que mejoren los resultados.
- **Fuentes y tipos de datos de inteligencia, inteligencia de terceros, inteligencia de marca, inteligencia geopolítica,** marcos analíticos para inteligencia, y mucho más.

Novedades de la cuarta edición:

- **Inteligencia sobre fraudes:** impida el fraude con tarjetas de pago y otros tipos de fraude relacionados con las transacciones en línea.
- **Inteligencia sobre identidad:** proteja las identidades de los usuarios, detecte el fraude de identidad de los clientes y evite la apropiación de cuentas.
- **Inteligencia sobre la superficie de ataque:** descubra los activos ocultos en Internet y los riesgos de TI en la sombra.

Acerca de Recorded Future®

Recorded Future es la mayor empresa de inteligencia del mundo. La plataforma de inteligencia de Recorded Future ofrece la cobertura más completa de adversarios, infraestructuras y objetivos. Al combinar la recopilación y el análisis de datos automatizados persistentes y generalizados con el análisis humano, Recorded Future proporciona visibilidad en tiempo real del amplio panorama digital y permite a los clientes tomar medidas proactivas para disuadir a los adversarios y mantener la seguridad de sus empleados, sistemas e infraestructuras.