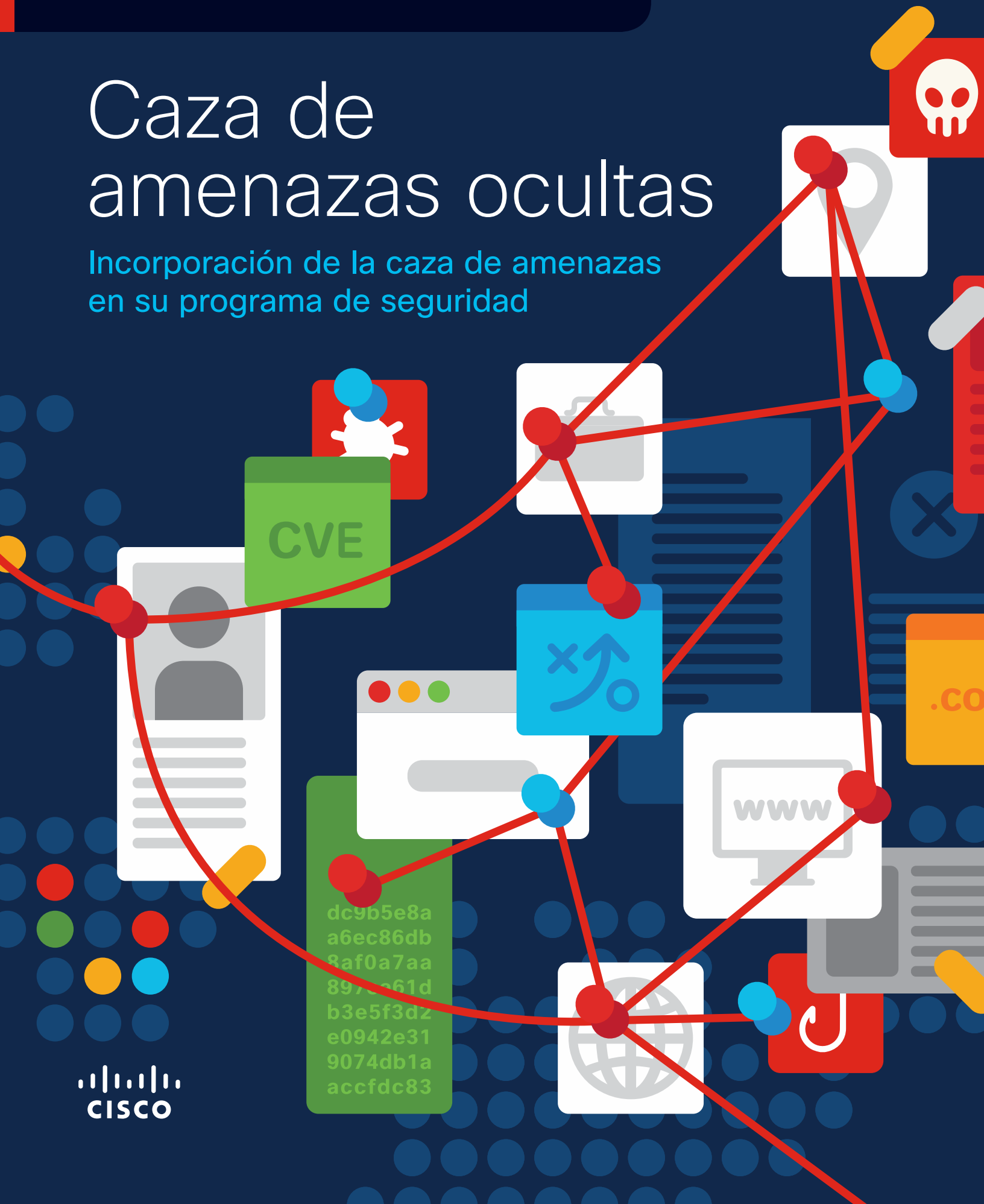
Caza de amenazas ocultas

Incorporación de la caza de amenazas en su programa de seguridad

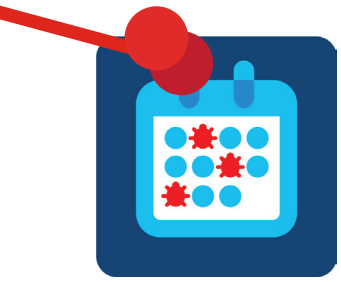


cisco

Contenido

Introducción

Es la 1:00 y todo está bien. Ha regresado de almorzar y como investigador sénior de amenazas de SOC de la empresa, acaba de revisar los paneles de SIEM en busca de alertas de seguridad. Nada fuera de lo común ha llamado su atención. Un proyecto de automatización reciente ha reducido drásticamente el tiempo que se tarda en realizar este barrido de seguridad, lo que libera un tiempo valioso que se hubiera invertido previamente en tareas manuales. Entonces, ¿cómo pasa este tiempo?



La caza de amenazas es una actividad que se planifica y realiza con regularidad para ayudar a fortalecer su postura frente a la seguridad.

Tal vez es momento de considerar la caza de amenazas. La caza de amenazas implica ir más allá de lo que ya conocemos o de lo que se nos ha alertado. El software de seguridad solo nos alerta sobre los riesgos y comportamientos que sabemos que son maliciosos. La caza de amenazas consiste en aventurarse a lo desconocido.

La caza de amenazas es un ejercicio activo de seguridad, con la intención de encontrar y erradicar a los atacantes que han penetrado su entorno sin aumentar la alarma. Esto se diferencia de las investigaciones tradicionales y las respuestas que provienen de las alertas que aparecen después de que se detectó una actividad potencialmente maliciosa.

La realidad

Por supuesto, esta situación podría sonar algo idealizada. Quiero decir, ¿quién tiene realmente una tarde libre? Siempre hay algo más que hacer, ¿verdad?

La realidad es que, la mayoría de las veces, la caza de amenazas no es una actividad que se hace por capricho. Tampoco es algo que se hace en una investigación en curso como el paso siguiente en un procedimiento. En cambio, es una actividad que se planifica y realiza con regularidad para ayudar a fortalecer su postura frente a la seguridad. Fundamentalmente, es otra herramienta en su arsenal de seguridad.

Nada de esto suena fácil cuando su agenda está repleta y su lista de tareas es larguísima. Sin embargo, hacerse tiempo en el calendario para realizar actividades de caza de amenazas tiene algunos beneficios clave.

Más vale prevenir que curar

Para comenzar, la identificación y erradicación de amenazas desconocidas y no detectadas siempre es algo bueno. Incluso cuando no se detecta una amenaza particular, los ejercicios de caza de amenazas a menudo identifican las debilidades en su entorno que puede reforzar y definir nuevas políticas. En última instancia, lo que surge de la búsqueda regular de amenazas es que puede reducir significativamente la superficie de ataque de futuros actores maliciosos.

También existen oportunidades importantes para aprovechar lo aprendido durante una campaña de caza de amenazas. Estos ejercicios pueden identificar áreas donde se pueden implementar alertas de comportamientos maliciosos, así como dónde desarrollar la automatización para repetir en un ámbito de caza de amenazas en particular. A partir de ahí, puede realizar ejercicios adicionales de caza de amenazas, desarrollar y ampliar sus protecciones y capacidades.

Dónde comenzar

El objetivo de este documento es ofrecer una descripción general de la disciplina de caza de amenazas. Exploraremos los pormenores de la caza de amenazas, destacaremos por qué es un esfuerzo valioso, quién debe participar, qué y dónde debe mirar, y cuándo debe hacerlo.

También existen varias disciplinas de seguridad con tareas que se superponen con la caza de amenazas. Compararemos y contrastaremos las disciplinas; también demostraremos que, si bien la caza de amenazas es similar a otras tareas, merece un lugar en su arsenal de seguridad.

Por último, analizaremos cómo puede desarrollar campañas eficaces de caza de amenazas dentro de su organización. Una de las cosas más difíciles de determinar es por dónde comenzar. Para ayudarlo, comenzamos con las medidas simples que puede tomar para comenzar a desarrollar su postura frente a la caza de amenazas, a la vez que fortalece la seguridad de su organización.

Caza de amenazas comparado con _____

En lo que respecta a las disciplinas de seguridad, la caza de amenazas es una especialidad comparativamente reciente. Debido a esto, se dan superposiciones con otras prácticas relacionadas con la seguridad. De hecho, muchas personas actualmente involucradas en la caza de amenazas tienen experiencia con estos otros roles dentro de sus carreras. Las siguientes son algunas comparaciones rápidas con otras disciplinas.

La respuesta ante incidentes

Este papel quizás sea el más similar a la caza de amenazas. Ambas disciplinas se ocupan directamente de las amenazas en su entorno. La diferencia principal es que la respuesta ante los incidentes es reactiva: usted sabe que algo está en la red o, al menos, que ha intentado acceder a la red debido a las alertas de seguridad, el comportamiento de la red o los terminales, u otras pruebas. En cambio, en la caza de amenazas, no hay necesariamente pruebas de una amenaza. Está buscando activamente algo en lugar de tratar de contener y corregir lo que sabe que está allí.

Las pruebas de penetración

La caza de amenazas y las pruebas de penetración también comparten algunas similitudes. En esencia, ambas intentan buscar debilidades en una red. Sin embargo, las pruebas de penetración generalmente buscan problemas de configuración o vulnerabilidades conocidas para obtener acceso a una red o información confidencial. El objetivo de la caza de amenazas no es necesariamente obtener acceso a nada, sino identificar amenazas ocultas presentes en un entorno, erradicarlas y definir políticas para prevenirlas en el futuro.

La gestión de riesgos

La idea de la gestión de riesgos es determinar las debilidades dentro de la red o en los sistemas, determinar su gravedad, priorizar y luego, tomar las medidas apropiadas para corregirlas. Esto puede implicar la identificación de fuentes de amenazas y la caza de amenazas puede ayudar a informar una evaluación de riesgos. Sin embargo, estas evaluaciones generalmente abarcan mucho más que la caza de amenazas, al considerar todos los riesgos potenciales, tanto conocidos como desconocidos.

La evaluación de riesgos

De manera similar a la caza de amenazas, la evaluación de riesgos consiste en averiguar si su red ha sido vulnerada por delincuentes desconocidos. Sin embargo, es un ejercicio mucho más amplio que la caza de amenazas. Durante las evaluaciones de riesgo, se instalan varias herramientas en toda la red, buscando en forma generalizada cualquier cosa fuera de lo común. En cambio, la caza de amenazas comienza con una idea o situación muy particular y mantiene el enfoque en ese ámbito.

Las 5 " W"

Determinar por dónde comenzar puede ser un desafío a la hora de definir ejercicios de caza de amenazas dentro de su organización. La utilización de las cinco " W", a menudo utilizadas en periodismo, puede ser una buena manera de comenzar a planificar el proceso.

Su equipo de caza de amenazas probablemente se superponga con su equipo de respuesta ante incidentes y la caza de amenazas agudiza sus habilidades y los tiempos de respuesta cuando se enfrentan a un incidente real.

¿Por qué? (why)

La inversión inicial en la detección proactiva de amenazas puede fortalecer significativamente la postura de una organización frente a la seguridad. El hecho es que existen atacantes organizados, capacitados y bien financiados. Si usted se convierte en el objetivo de uno de estos grupos, ellos pueden trabajar con esmero en la búsqueda de una debilidad para ingresar. Lamentablemente, no es posible descubrirlo todo, incluso con las mejores herramientas de seguridad. Aquí es donde entra en juego la caza de amenazas: su mandato principal es encontrar a estos tipos de atacantes.

Una ventaja adicional para la caza de amenazas es que llevar a cabo estos ejercicios genera familiaridad con herramientas y técnicas que son muy importantes cuando se produce un ataque o una intrusión. Su equipo de caza de amenazas probablemente se superponga con su equipo de respuesta ante incidentes y la caza de amenazas agudiza sus habilidades y los tiempos de respuesta cuando se enfrentan a un incidente real. Se puede ver como práctica para cuando algo sale mal.

Identificar quién (who)

Crear ese equipo de caza de amenazas puede parecer tan abrumador como reunir a un equipo de superhéroes para que trabajen en pos de la derrota de un enemigo común. Parte de formar ese equipo consiste en reunir personas con diferentes conjuntos de habilidades y contextos.

Si usted es una organización grande, el primer paso puede ser tan simple como apartar una parte del tiempo al mes para que un grupo, o equipo especializado, planifique, se desempeñe e informe sobre una campaña de caza de amenazas. Sin embargo, si es una organización pequeña con tan solo algunas personas de TI especializadas (tal vez solo una), es probable que no sea tan sencillo. En este caso, es posible que desee incorporar la experiencia externa de un tercero para que lo ayude. Esto conlleva ventajas y desventajas. Del lado positivo, es probable que obtenga acceso a personas que cumplen con los requisitos de habilidades de la caza de amenazas. Sin embargo, un equipo externo de caza de amenazas no estará tan familiarizado con los pormenores de su red específica como lo estará el personal interno.

Independientemente de esto, hay una combinación de habilidades básicas necesarias en un equipo para llevar a cabo una campaña de caza de amenazas:

- **Familiaridad con la seguridad de redes y terminales**

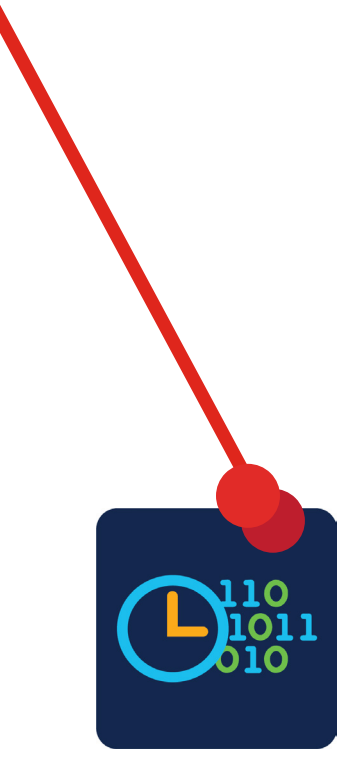
  Esto casi no hace falta decirlo. Necesitará miembros experimentados de su equipo de SOC o TI que tengan un vasto y profundo conocimiento de los problemas de seguridad y los procedimientos recomendados.

- **Comprensión de análisis de datos**

  A menudo, la caza de amenazas requiere provocar patrones a partir de datos sin procesar. Comprender el análisis estadístico lo ayudará a identificar patrones en los datos. La visualización de datos es igualmente importante para detectar y compartir las anomalías que se encuentran.

- **Una curiosidad innata**

  La caza de amenazas no es un ejercicio preestablecido. A veces puede asemejarse a una actividad artística. Requiere una cierta cantidad de pensamiento creativo, conectar artículos aparentemente no relacionados o preguntar: " me pregunto qué sucedería si..."



Antes de poder hacer algo relacionado con la caza de amenazas, deberá asegurarse de tener el registro adecuado activado para llevar a cabo la caza.

Desde el punto de vista de un profesional de la seguridad, una ventaja de la caza de amenazas es que es divertida. La caza de amenazas les da un descanso a los empleados de su departamento de SOC o TI de la naturaleza reactiva diaria de sus funciones y la oportunidad de ir al ataque. Estas tareas activas y satisfactorias para los empleados a menudo pueden generar tasas de conservación de empleados de SOC más altas y retenerlos en un campo en el que puede ser difícil encontrar personas altamente calificadas y, a menudo, mantenerse activo.

Cuándo cazar (when)

Finalmente, las cazas más exitosas son las planificadas. Debe definir un ámbito para la caza, identificar objetivos claros y reservar parte del tiempo para realizar la caza. Cuando haya terminado, debe evaluar los pasos para mejorar su postura frente a la seguridad, estableciendo estrategias de seguridad para abordar los resultados hacia adelante.

En otras ocasiones, también es posible que desee llevar a cabo un ejercicio de caza de amenazas cuando sospeche que puede haber ocurrido un comportamiento riesgoso.

- **¿Un usuario en particular descarga muchos más datos de lo normal en un día determinado?**
- **¿Un usuario intenta iniciar sesión en un sistema al que no tiene acceso?**
- **¿Parece que un administrador borró sus registros de bash?**

Muchos de estos comportamientos podrían indicar acciones de un actor malicioso que ha comprometido un dispositivo y es un lugar bastante sencillo para comenzar una caza de amenazas.

Por último, hay momentos en los que una caza de amenazas puede surgir de manera inesperada. ¿Alguna noticia sobre ciberseguridad que llamó la atención de su director general de Información alguna vez dio lugar a un correo electrónico o una llamada telefónica preguntando si la empresa es vulnerable? Esta es una pregunta perfectamente válida e implementar un proceso de consultas de campo como esta puede ahorrar una gran cantidad de tiempo y recursos.

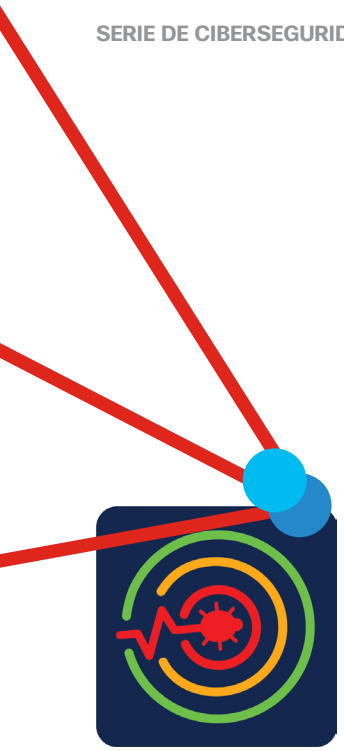
Qué (what) y dónde (where)

En última instancia, los datos son clave para cualquier caza de amenazas. Antes de poder hacer algo relacionado con la caza de amenazas, deberá asegurarse de tener el registro adecuado activado para llevar a cabo la búsqueda. El hecho es que, si no puede ver lo que sucede en sus sistemas, no puede responder en consecuencia.

Escoger a partir de qué sistemas arrancar a menudo dependerá del alcance de la caza en una caza podría ser terminales en el departamento de Finanzas, en otra podría centrarse en los servidores web. En algunos casos, incluso es posible que desee instalar herramientas en el entorno para monitorear determinados tipos de tráfico. Los registros extraídos por estos sistemas temporales luego se utilizarán en la caza.

Por supuesto, permitir el registro puede llenar rápidamente los recursos de almacenamiento y recopilar registros puede consumir fácilmente el tiempo de su equipo. Esto puede requerir separar los recursos físicos para almacenar registros y configurar la automatización básica para enviarlos allí. En el corto plazo, es posible que deba ser selectivo acerca de la amplitud de configuración de los sistemas de registro. La utilización de herramientas como la información de seguridad y el software de administración de eventos (SIEM) puede recorrer un largo camino para hacer que el análisis de los registros sea más rápido y sencillo.

En los primeros ejercicios de caza de amenazas, el resultado puede incluir una lista de preguntas que no se pudieron responder, en función de los registros disponibles. Con el tiempo, será más claro qué sistemas deben tener activado el inicio de sesión, y a qué nivel, para obtener los resultados deseados.



El objetivo de su ejercicio de caza de amenazas debe ser descubrir los TTP de un atacante; es lo más valioso porque es difícil que el atacante lo reemplace.

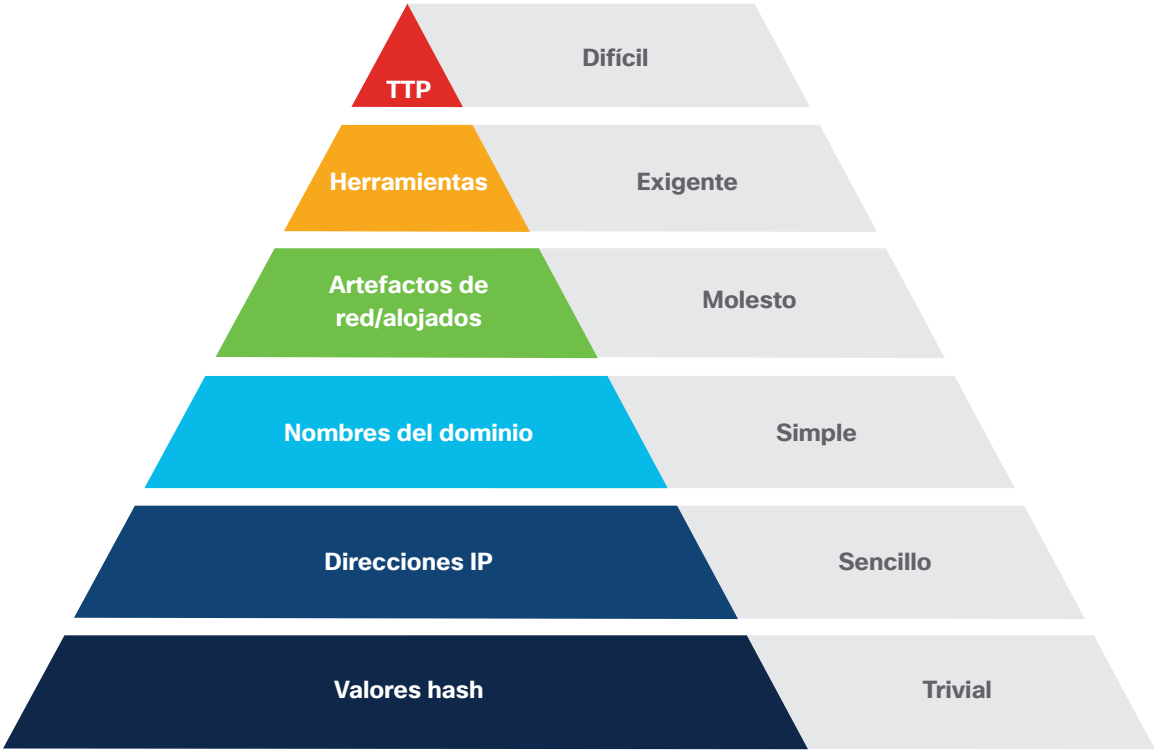
La pirámide del dolor

David Blanco, investigador de seguridad, presentó un enfoque titulado la Pirámide del dolor que describe cómo causar a los adversarios la mayor dificultad al atacar su red. Cada una de las seis capas representa diferentes enfoques que puede adoptar, comenzando con el simple y avanzando hasta el más difícil.

Por ejemplo, en la base de la pirámide se encuentran los hashes. Los archivos que llevan hashes maliciosos conocidos son fáciles de detectar y también son simples de reemplazar para el atacante. Lo mismo sucede con las direcciones IP, aunque esto requiere un poco más de trabajo, tanto para encontrar como para que un atacante reemplace, por lo tanto, es una parte más pequeña de la pirámide. Los dominios son un poco más difíciles, los artefactos de red son aún más difíciles, etc.

El objetivo de su ejercicio de caza de amenazas debe ser descubrir las tácticas, las técnicas y los procedimientos (TTP) de un atacante. Estos son los más valiosos porque son difíciles de reemplazar por el atacante. A menudo es lo más difícil de identificar o lo que más tiempo conlleva, principalmente porque requiere comparar puntos de datos de diferentes conjuntos de datos y realizar conexiones donde la relación no es evidente al principio.

El truco es que, a medida que avanzan en la pirámide, obliga a los adversarios a invertir más recursos en atacar su red, lo que dificulta y aumenta las probabilidades de que sean capturados. El objetivo final de la Pirámide del dolor es que, siguiendo sus principios, su red se vuelve tan difícil de hackear que los atacantes se trasladan a otros objetivos más simples.



Fuente: David J. Bianca, blog personal

Cómo buscar

En cuanto a cómo, hay varias maneras de abordar un ejercicio de caza de amenazas. Los recursos y las habilidades disponibles entrarán en juego en el nivel de detalle en el que se lleva a cabo una campaña de caza de amenazas.

En la siguiente sección, empezaremos con formas sencillas y básicas de comenzar a cazar amenazas y, luego, iremos en ascenso en el nivel de complejidad. La idea aquí es que, después de cada ejercicio de caza de amenazas, pueda aprovechar lo aprendido. Establecer estrategias, automatización y cambios de políticas donde sea necesario sienta las bases para pasar a las técnicas más avanzadas.

Análisis de los registros

A veces, las actividades más simples de caza de amenazas provienen de investigaciones o informes sobre amenazas descubiertas recientemente. En estos días, es común incluir indicadores de riesgo (IoC) junto con la investigación para que otros los utilicen. Estos puntos de datos generalmente constan de direcciones IP, URL, dominios, hashes de archivo u otros IoC que comprendan una amenaza.

Una de las maneras más sencillas de iniciar un ejercicio de caza de amenazas es cotejar los registros de los sistemas con los IoC. Las herramientas de línea de comando o las secuencias de comandos simples pueden ser suficiente para comenzar. El uso de un SIEM es otro método para comparar rápidamente los IoC con los registros. También hay productos de seguridad más avanzados que pueden ayudar a facilitar la caza de amenazas, ya que le permite copiar y pegar los IoC en un panel para ver si se los ha visto en su entorno.

Una vez que se sienta cómodo con estas actividades, es momento de profundizar en los registros y comenzar a detectar nuevos IoC que pueden existir. Aquí es donde entran en juego las habilidades de análisis de datos. Aplicar modelos estadísticos a los registros, como la agrupación en clústeres o la distribución de frecuencias, puede ayudar a esclarecer las anomalías. Finalmente, usted espera alcanzar la cima de la Pirámide del dolor e identificar los TTP de un atacante.

Poner a prueba una teoría

Algunos pueden sostener que la comparación de los registros con los IoC conocidos no es una verdadera caza de amenazas. El razonamiento es que simplemente está

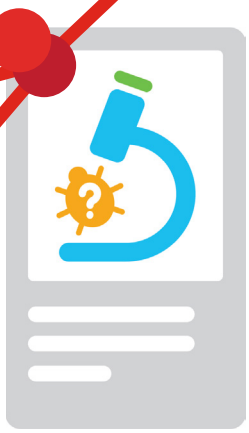
Caza de amenazas en acción

Jeff Bollinger administra las investigaciones de seguridad de CSIRT aquí en Cisco. A continuación, puede verse un relato en primera persona de un ejercicio de caza de amenazas que llevó a cabo su equipo.

" Al analizar los datos históricos de los terminales de Cisco AMP en busca de indicadores de riesgo, vimos un instalador de malware binario sospechoso que el usuario eliminó.

Recuperamos el binario restaurando el archivo único a partir del archivo de respaldo (corporativo) del usuario y pudimos revertirlo y extraer indicadores adicionales (nombres de hosts C2) que luego aplicamos a toda nuestra telemetría de red.

Esto benefició a los hosts adicionales afectados que no se activaron en el hash del instalador de malware original".



Si usted es el experimentado del equipo, no crea que lo ha visto todo antes. En su lugar, intente demostrar que no es una amenaza. Si no puede hacerlo de manera automática, investigue más a fondo.

haciendo una comparación uno a uno. En estos casos, para calificar como caza de amenazas, hay que profundizar más.

Aquí es donde entra en juego la creatividad. Hay que elaborar una teoría sobre dónde puede residir una amenaza, los vectores que podría haber utilizado para llegar allí o las técnicas que aprovechó. A continuación, se encuentran algunas ideas del tipo de investigaciones que puede realizar.

- **Leer noticias de seguridad**

  Las últimas noticias sobre el panorama de amenazas pueden estar repletas de material para una caza de amenazas. Por ejemplo, si hubo una vulnerabilidad crítica en un proceso de Windows recientemente divulgado, investigue si se produjo alguna actividad extraña en torno a ese proceso. Por supuesto, preste especial atención al material que se aplica a su sector. Por ejemplo, si trabaja en aviación, un ladrón de tarjetas de crédito no tendría una prioridad alta. Por el contrario, si trabaja en el sector bancario, no aplicará una amenaza que se encuentra atacando un ICS.

- **Consultar los informes de comportamiento extraño**

  Investigue informes inusuales de la actividad del personal. ¿Los sistemas suspendidos se activan repentinamente durante la noche? Investigue qué es lo que los activa. ¿Una oficina informó que encontraron datos internos en una fuente externa? Busque indicaciones de exfiltración de datos.

- **Filtrar lo normal para encontrar lo anormal**

  La actividad inusual es un buen punto de partida, pero no siempre es fácil de detectar. A veces, hay que cavar hondo para encontrarla. Observe una actividad en particular con un objetivo malicioso en mente. Por ejemplo:

  - Busque largas conexiones de red, lo que podría ser un signo de exfiltración de datos. Filtre las esperadas y vea si alguna de las restantes es sospechosa.
  - Observe los picos de actividad de la CPU y los procesos que los crean, lo que podría indicar criptominería o una actividad de registro de ladrones de información. Filtre aquellos que son conocidos y analice los que no lo son.
  - ¿Qué tipo de archivos está descargando la herramienta BITSAdmin? Podría utilizarse para desplegar herramientas maliciosas, ya que muchas amenazas utilizan herramientas locales para enmascarar sus acciones. Retire las descargas periódicas que espera y céntrese en el resto.
  - Observe las tareas programadas Los atacantes pueden agregar sus propias tareas para iniciar ciertas actividades maliciosas. ¿Hay alguna que no esté administrada por los administradores del sistema? Investigue las que parezcan sospechosas.

Todos los casos en los que el comportamiento parece fuera de lo común son áreas principales para profundizar y encontrar la causa raíz. Sin embargo, es importante abordar cualquier cosa que se encuentre con algo de precaución. Solo porque algo parezca extraño, no significa necesariamente que sea un delincuente. Asegúrese de comparar sus hallazgos con otras fuentes de datos antes de sacar conclusiones. Al mismo tiempo, si usted es el experimentado del equipo, no crea que ya lo ha visto todo. En su lugar, intente demostrar que no es una amenaza. Si no puede hacerlo de manera automática, investigue más a fondo.

Ir tras la fuente

Ha logrado identificar una amenaza dentro de su red, determinar qué le permitió ingresar y tomar medidas para evitar que vuelva a

suceder. Sin embargo, la próxima vez que realice un ejercicio de caza de amenazas, encontrará que los atacantes han regresado de otra manera.

Si descubre constantemente que su organización es víctima de ataques, podría valer la pena investigar quién está atacando, la infraestructura que utiliza para atacar e intentar detener al grupo.

Sin embargo, esta no es una sugerencia para practicar la piratería ofensiva. Por más tentador que sea, hay una serie de problemas a la hora de ir por ese camino.

Para empezar, si ataca una infraestructura maliciosa, hay grandes probabilidades de que los atacantes lo noten y lo ataquen el doble. Sin embargo, esta vez es posible que su motivación no sea robar información, sino más bien una venganza: desactivar o destruir sistemas a su paso.

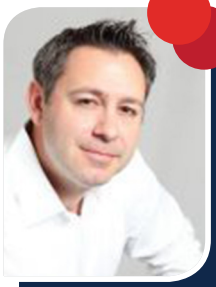
Otra razón para no hackearlos es que, en la mayoría de las ubicaciones de todo el mundo, hacerlo es ilegal. A pesar de que los sistemas en cuestión están realizando actividades ilegales, la piratería ofensiva sigue siendo piratería.

La buena noticia es que aún hay mucho que se puede hacer. Los IoC de un ataque pueden revelar mucho sobre los atacantes sin siquiera tener que tocar sus redes.

El mejor enfoque para lograr que los actores maliciosos se detengan es reunir todos los IoC que pueda descubrir, desde hashes hasta TTP, crear un perfil del atacante y, luego, entregar estos detalles a los organismos del orden público correspondientes. Estas autoridades son el mejor método para perseguir y detener a un atacante por medios legales.

Por supuesto, para todos, excepto para las organizaciones más grandes y atacadas, esto no siempre es algo que puede hacerse fácilmente de manera interna. Como resultado, la mayor parte de las organizaciones puede y debe depender de equipos de investigación de seguridad externos que han hecho su mandato de la investigación de dichos ataques. Las organizaciones de inteligencia de amenazas, como Talos Intelligence o Incident Response Services de Cisco, están para ayudar en estos casos.

El mejor enfoque para lograr que los actores maliciosos se detengan: reunir todos los IoC que pueda descubrir, crear un perfil del atacante y entregar estos detalles a los organismos del orden público correspondientes.



Aprovechar la caza de amenazas

Sean Mason, director de Gestión de amenazas de los servicios de asesoramiento de seguridad de Cisco, reflexiona sobre cómo sus equipos han aprovechado la caza de amenazas en Cisco.

"Realmente comencé a comprender y valorar la caza de amenazas en 2011 inmediatamente después del hack de RSA. Me encontré de reunión en reunión analizando cómo podíamos detectar este tipo de amenazas. Realmente nos hizo pensar de manera diferente. También nos dimos cuenta de qué tipo de brechas de visibilidad teníamos. Durante todos estos años, los diversos equipos en los que he estado han aprovechado la búsqueda de muchas maneras diferentes: ya sea de manera proactiva siguiendo una corazonada, respondiendo a un incidente o siendo diligente después de leer las últimas noticias de seguridad. Puedo afirmar sinceramente que, después de más de ocho años de aprovechar la caza de amenazas en diversas capacidades, es obvio que considero que es un componente fundamental para cada programa de seguridad exitoso".

Las secuelas

Por más importante que sea identificar y erradicar las amenazas ocultas en su red, descubrir cómo ingresaron y tomar medidas para evitar futuros ataques es quizás el aspecto más importante de la caza de amenazas. Programe una reunión posterior para analizar la búsqueda. En ella, muestre lo que se ha encontrado y analice lo que debe hacerse para solucionarlo. Luego, implemente cambios en la política de red para fijarlo.

A veces, las mejores campañas de caza de amenazas no cubren nada. El beneficio aquí es que ahora sabe concretamente que la ruta investigada no es actualmente un riesgo para su organización.

En ocasiones, no se trata tanto de encontrar una amenaza, sino de descubrir debilidades dentro de la organización. Una campaña de caza de amenazas exitosa puede descubrir un servidor mal configurado o una infracción de la política que necesita corrección. Y, por muy ilógico que parezca, a veces, las mejores campañas de caza de amenazas no descubren nada. El beneficio aquí es que ahora sabe concretamente que la ruta investigada no es actualmente un riesgo para su organización.

Agregar la automatización es otro paso esencial tras la caza de amenazas. Después de que se complete una caza de amenazas, es importante revisarla periódicamente para ver si regresa la actividad descubierta. Convierta lo que se ha encontrado en un proceso que pueda ejecutarse nuevamente. Configure una trampa con alertas al activarse. Con el tiempo, esto se convertirá en su cuaderno de estrategias de seguridad.

Conclusión

No hay manera de saber si su red está completamente libre de amenazas. Eso no significa que la búsqueda sea en vano. El beneficio de la caza de amenazas, además de eliminar las amenazas que lograron sobrevivir a sus defensas, es que puede aumentar aún más su postura frente a la seguridad.

Piense en la caza de amenazas como lo haría un albañil. Cuando construya una casa, comience con ese primer anillo de ladrillos, agregue mezcla para mantenerlos en su lugar y, luego, agregue otra capa de ladrillos. Repita el proceso capa por capa y construya las paredes.

Con la caza de amenazas, esa primera capa de ladrillos podría ser activar registros suficientes y almacenarlo. La mezcla es la automatización que hace que esos registros ingresen regularmente. La siguiente capa de ladrillos es comparar los registros con los IoC. Automatice esos procesos para mantener los ladrillos en su lugar. Siga aprendiendo con capas de análisis de datos, comprobando teorías, etc.

Muy pronto, habrá creado un proceso de caza de amenazas sólido y estable que le dará la tranquilidad de que su organización está tan libre de amenazas como el entorno lo permite.

Herramientas para la caza de amenazas

Las siguientes son algunas herramientas recomendadas que pueden utilizarse para la caza de amenazas. Si bien la lista dista mucho de ser exhaustiva, será útil para comenzar.

Cisco Threat Response

Cisco Threat Response automatiza las integraciones en determinados productos de seguridad de Cisco, aplica inteligencia de amenazas de Cisco Talos y fuentes de terceros frente a eventos de seguridad para investigar automáticamente los indicadores de riesgo (IoC) y confirmar rápidamente las amenazas. También brinda la capacidad de recopilar y almacenar información clave de la investigación, administrar y documentar su progreso y hallazgos, y corregir las amenazas directamente desde el panel.

Red de amenazas de Cisco

Threat Grid combina el sandboxing avanzado con la inteligencia de amenazas en una solución unificada para proteger a las organizaciones contra el malware. Gracias a una sólida base de conocimientos sobre malware que cuenta con información contextual, comprenderá la actividad del malware o su potencial, la dimensión de la amenaza y el modo de defenderse de ella.

Cisco Stealthwatch

Cisco Stealthwatch es una solución completa de visibilidad y tráfico de red y análisis de seguridad en la nube. Incluso puede detectar malware en tráfico cifrado sin descifrarlo. Proporciona detección avanzada de amenazas, respuesta acelerada frente a amenazas y segmentación de la red simplificada mediante el aprendizaje automático multicapa y el modelado de entidades. Con el análisis avanzado de comportamiento, puede descubrir quién está en su red o en su infraestructura de nube pública y qué está haciendo.

Cisco Advanced Malware Protection (AMP) para terminales

AMP protege no solo los terminales, sino que puede ayudar en el análisis de malware y la búsqueda proactiva de amenazas. Las sólidas capacidades de búsqueda de AMP le permiten encontrar información diversa, como archivos, hash, URL, direcciones IP, claves de registro, usuarios, procesos, aplicaciones y mucho más. También puede mostrar el ciclo de vida de un archivo en su entorno, desde la primera vez que se vio, lo que hizo en el terminal y otra información.

Umbrella Investigate

Investigate ofrece la vista más completa de las relaciones y la evolución de dominios, IP, sistemas autónomos (ASN) y hash de archivo. Accesible a través de la consola web y la API, la inteligencia de amenazas enriquecidas de Investigate agrega el contexto de seguridad necesario para descubrir y predecir las amenazas.

Herramientas de administración de información y eventos de seguridad (SIEM)

Tener una SIEM es un paso clave para llevar a cabo actividades de caza de amenazas, especialmente al comenzar. Una SIEM bien configurada puede reducir considerablemente la cantidad de tiempo que se dedica a recopilar archivos de registro y realizar análisis básicos. Entre los ejemplos de SIEM conocidos, se incluyen Splunk, IBM QRadar y Exabeam.

Herramientas de monitoreo de terminales

Existen una gran variedad de herramientas disponibles para recopilar registros detallados de los terminales. El registro de eventos integrado de Windows es un buen lugar para comenzar y herramientas más complejas, como Sysmon y Process Monitor, pueden ampliar sus capacidades de registro. (Incluso existen configuraciones prediseñadas que lo ayudarán a comenzar). En Mac de Apple, consulte la consola para ver los registros.

Analizadores de paquetes

Son herramientas que pueden utilizarse para monitorear su tráfico de red. Las aplicaciones como Wireshark y tcpdump, y las API como pcap son herramientas populares para recopilar información sobre los datos que se transfieren a través de su red.

Acerca de la serie de ciberseguridad de Cisco

Durante la última década, Cisco ha publicado una gran cantidad de información crucial de seguridad e inteligencia de amenazas para profesionales de seguridad interesados en el estado de la ciberseguridad global. Estos informes exhaustivos proporcionaron explicaciones detalladas de los panoramas de amenazas y las consecuencias para las organizaciones, así como los procedimientos recomendados para defenderse frente a los efectos adversos de vulneraciones de datos.

En nuestro nuevo enfoque de liderazgo intelectual, el departamento de seguridad de Cisco está realizando una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner: Serie de ciberseguridad de Cisco. Hemos ampliado el número de títulos para incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas innovadores en el sector de seguridad, la recopilación previa de informes de la serie 2019 incluye el Reporte de referencia de privacidad de datos, el Reporte de amenazas, el Reporte de referencia de CISO, y el Reporte de seguridad del correo electrónico, pero vendrán otros más a lo largo del año.

Para más información y para acceder a todos los informes y las copias archivadas, visite www.cisco.com/mx/securityreports.

Sede central en América
Cisco Systems Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (USA), Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Ámsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco en www.cisco.com/go/offices

Publicado en agosto de 2019 THRT_05_0819_r1