Videos explicativos

Artículos explicativos originales extraídos de la videoteca de Cyber Crucible — ransomware, robo de datos, robo de identidad, seguridad autónoma y FortressAI — cada uno con el video correspondiente.

- ¿Están las empresas reaccionando de forma exagerada ante el riesgo de la IA, o se trata de un problema de visibilidad?
- ¿Por qué los modelos tradicionales de SOC tienen dificultades frente a los ciberataques a velocidad de máquina?
- ¿Cómo es en realidad la ciberseguridad verdaderamente autónoma en el día a día?
- ¿Pueden las herramientas de IA como ChatGPT reemplazar a un equipo humano de ciberseguridad?
- ¿Puede el ransomware seguir accediendo a los datos almacenados en servicios en la nube como OneDrive o Google Drive?
- Si el ransomware se elimina a sí mismo, ¿significa eso que el ataque ha terminado?
- ¿Debería la ciberseguridad centrarse en la resiliencia o en prevenir los ataques desde el principio?
- ¿Cómo ayuda Cyber Crucible a gestionar proveedores y resultados de ciberseguridad?
- ¿Cómo ayuda Cyber Crucible a controlar el gasto en ciberseguridad y los contratos con proveedores?
- ¿Funciona Cyber Crucible junto con otras herramientas de ciberseguridad y EDR?
- ¿Por qué la IA es un riesgo empresarial, y no solo una herramienta de productividad, para los directivos de la empresa?
- ¿Los empleados ya están usando herramientas de IA antes de que nuestra empresa tenga una política oficial de IA?
- ¿Cuáles son las señales de advertencia de que está ocurriendo un ataque de ransomware?
- ¿Qué sucede realmente en los momentos durante un ataque de ransomware?
- ¿Qué sucede realmente cuando el ransomware ataca un servidor de una empresa?
- ¿Por qué el ransomware ataca los archivos compartidos antes de llegar a mi escritorio?
- ¿Qué inspiró al fundador a crear Cyber Crucible?
- ¿De dónde provienen realmente los ataques de ransomware?

¿Están las empresas reaccionando de forma exagerada ante el riesgo de la IA, o se trata de un problema de visibilidad?

Respuesta breve: La mayoría de las organizaciones no está reaccionando de forma exagerada ante el riesgo de la IA; simplemente carecen de visibilidad real sobre cómo se están utilizando realmente las herramientas de IA en todo su entorno. Sin esa visibilidad, la suposición más segura es que el riesgo actual se está subestimando, no exagerando.

Por qué el "riesgo de la IA" a menudo se reduce a puntos ciegos

Cuando las empresas evalúan su exposición al riesgo relacionado con la IA, aparece un patrón común: algunas organizaciones admiten abiertamente que no tienen una idea clara de cómo se están utilizando las herramientas de IA internamente. Otras creen que sí tienen visibilidad, solo para descubrir lo contrario una vez que se implementa el monitoreo. En la práctica, una vez que se activa el seguimiento, el volumen y la variedad de uso de herramientas de IA que salen a la luz suelen ser sorprendentes, hasta el punto de que a veces las funciones de visibilidad deben ejecutarse en un modo controlado o simulado simplemente para poder mantener el ritmo de la cantidad de actividad que aparece casi de inmediato.

Esta brecha sugiere que las preocupaciones sobre el riesgo de la IA rara vez son exageradas. Con mayor frecuencia, la preocupación está subestimada porque los líderes trabajan sin los datos necesarios para juzgar la situación con precisión.

Por qué el riesgo desconocido debe tratarse como un riesgo alto

Una forma útil de pensar en esto es similar a las finanzas personales: si nunca revisas el saldo de tu cuenta bancaria, la suposición responsable es que no tienes fondos significativos disponibles, no lo contrario. La misma lógica se aplica al uso de la IA dentro de una empresa. Sin variables concretas, como qué herramientas se utilizan, con qué frecuencia y por quién, las organizaciones no tienen una base confiable para suponer que el riesgo es bajo. El valor predeterminado responsable es asumir la exposición en el peor de los casos hasta que los datos reales de uso demuestren lo contrario.

El patrón más amplio detrás de la adopción de la IA

En todos los usuarios, unidades de negocio y las propias herramientas de IA, siguen surgiendo casos de uso nuevos y, a menudo, no autorizados más rápido de lo que la gobernanza puede seguir el ritmo. Este patrón constante indica que la mayoría de las organizaciones, independientemente de su tamaño o sector, todavía están poniéndose al día con la forma en que la IA se está utilizando realmente en su entorno. Establecer una visibilidad clara es el primer paso necesario antes de que el riesgo de la IA pueda evaluarse o gestionarse con precisión.

https://player.vimeo.com/video/1176539821

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué los modelos tradicionales de SOC tienen dificultades frente a los ciberataques a velocidad de máquina?

Respuesta breve: Los centros de operaciones de seguridad tradicionales se diseñaron para una era del hacking más lenta y predecible, basándose en firmas y análisis humano para detectar amenazas después de que ocurrieran. Los atacantes actuales utilizan herramientas automatizadas que mutan constantemente, por lo que las defensas deben migrar hacia enfoques preventivos y sin firmas que operen más rápido que el propio ataque.

Cómo ha cambiado el panorama de amenazas

Hace años, las herramientas maliciosas se comportaban de manera bastante consistente e identificable. Los equipos de seguridad podían construir métodos de detección basados en patrones conocidos, ya que los atacantes aún no dependían en gran medida de la automatización para cambiar constantemente sus técnicas. Ese enfoque funcionaba lo suficientemente bien como para detectar algunas de las amenazas más sofisticadas de aquella época, incluidos ataques altamente dirigidos descubiertos hace más de una década.

Ese panorama ya no existe. Los atacantes modernos utilizan la automatización para generar variaciones rápidas de sus herramientas, lo que dificulta que la detección basada en firmas se mantenga al día. Para cuando se identifica, cataloga e implementa una nueva firma en una infraestructura de seguridad, el atacante a menudo ya ha pasado a una nueva variante.

Por qué los modelos de SOC heredados se quedan atrás

Los flujos de trabajo tradicionales de un SOC dependen de identificar indicadores conocidos y luego investigar y responder mediante procesos en gran medida manuales o semimanuales. Este modelo asume que los atacantes se mueven a un ritmo que da tiempo a los defensores para analizar y reaccionar. Cuando los ataques están automatizados y pueden mutar en tiempo real, esa suposición deja de ser válida, dejando una brecha persistente entre el momento en que surge una amenaza y el momento en que se aborda.

Qué deben hacer las defensas modernas en su lugar

Las herramientas de seguridad ahora deben operar sin depender únicamente de firmas previamente conocidas. En cambio, deben detectar y prevenir el comportamiento malicioso directamente, actuando a velocidad de máquina en lugar de esperar a los ciclos de análisis impulsados por humanos. La tecnología FortressAI de Cyber Crucible se basa en este principio, centrándose en detener el ransomware, el robo de datos y los intentos de robo de identidad mediante una acción automatizada y preventiva, en lugar de una coincidencia de firmas posterior a los hechos.

https://player.vimeo.com/video/1182235055

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Cómo es en realidad la ciberseguridad verdaderamente autónoma en el día a día?

Respuesta breve: La seguridad autónoma genuina debería sentirse rutinaria y de bajo esfuerzo, no como una fuente constante de alertas o ansiedad. Si una herramienta de seguridad requiere atención continua, ajustes o preocupación, no está funcionando de manera autónoma.

Por qué el objetivo es ser "aburrido"

Los equipos de seguridad y el personal de TI ya hacen malabares con más tareas de las que realmente pueden terminar. Añadir una herramienta que exige revisiones periódicas, análisis manual de alertas o solución de problemas a altas horas de la noche anula el propósito de la automatización. Una protección autónoma eficaz debería operar silenciosamente en segundo plano, de forma muy similar a un extintor de incendios montado en la pared. La mayoría de las personas no piensan en su extintor hasta que un inspector pasa una vez al año para confirmar que está cargado y listo. El resto del tiempo, simplemente permanece ahí, cumpliendo su función sin requerir atención.

Ese es el estándar que debería cumplir la seguridad autónoma. Debe manejar las amenazas por sí sola, sin distraer al personal de otras prioridades ni convertirse en un elemento más en una lista de tareas pendientes ya larga.

Qué significa esto en la práctica

Si un producto de seguridad le hace revisar paneles de control constantemente, dudar si detectó algo o perder el sueño preguntándose si realmente está funcionando, no es verdaderamente autónomo: es simplemente otra tarea manual con una etiqueta distinta. FortressAI de Cyber Crucible está diseñado en torno a esta idea: detectar y detener el ransomware, el robo de datos y la actividad de robo de identidad sin necesitar supervisión humana constante para funcionar correctamente.

La medida del éxito no es cuánta actividad genera una herramienta de seguridad ni con qué frecuencia necesita ajustes. Es cuán poco hay que pensar en ella. Cuando la seguridad autónoma funciona como se pretende, debería ser poco notable: presente, confiable y prácticamente invisible hasta el momento en que se la necesita.

https://player.vimeo.com/video/1190816235

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Pueden las herramientas de IA como ChatGPT reemplazar a un equipo humano de ciberseguridad?

Respuesta breve: No. Las herramientas de IA de propósito general pueden respaldar el trabajo de seguridad al resumir información o responder preguntas básicas, pero no son lo suficientemente confiables como para reemplazar a un equipo de seguridad capacitado cuando hay decisiones reales de riesgo en juego.

Por qué la confianza de la IA puede ser engañosa

Herramientas como ChatGPT a menudo presentan respuestas con un tono de certeza, incluso cuando la información subyacente es incompleta o incorrecta. Esto puede crear una falsa sensación de autoridad, similar a una persona persuasiva que afirma algo con tanta confianza que otros lo aceptan como un hecho sin verificarlo más a fondo. En una conversación cotidiana, ese tipo de confianza fuera de lugar es un problema menor. En ciberseguridad, donde las decisiones afectan la forma en que una organización identifica y responde a las amenazas, aceptar resultados inexactos sin cuestionarlos puede provocar daños reales. El análisis de seguridad depende del contexto, la verificación y el criterio que los modelos de IA de propósito general actuales no están equipados para replicar por completo.

Dónde la IA todavía puede ayudar

A pesar de estas limitaciones, las herramientas de IA no carecen de valor en un contexto de seguridad. Pueden servir como punto de partida para la investigación, ayudar a explicar conceptos o asistir en la redacción y organización de información. Utilizada de esta manera, la IA funciona como una herramienta de apoyo en lugar de una que toma decisiones. La clave está en reconocer la diferencia entre una IA que asiste a un analista con conocimientos y una IA que intenta evaluar y mitigar el riesgo de forma independiente, lo cual requiere una experiencia más profunda de la que estas herramientas ofrecen actualmente.

El argumento a favor de expectativas honestas

Los proveedores y profesionales de IA que establecen expectativas realistas, en lugar de exagerar lo que estas herramientas pueden hacer, tienen más probabilidades de generar confianza duradera. Sobrevender las capacidades de la IA en materia de seguridad corre el riesgo de erosionar la confianza una vez que las limitaciones se hacen evidentes. Una comunicación clara y mesurada sobre lo que la IA puede y no puede hacer ayuda a las organizaciones a tomar decisiones informadas sobre cómo incorporarla de manera responsable. El enfoque de Cyber Crucible refleja este mismo principio: en lugar de posicionar a la IA como un reemplazo de defensores capacitados, las tecnologías de protección autónoma como FortressAI están diseñadas para trabajar junto con la experiencia humana, fortaleciendo la capacidad de una organización para prevenir el ransomware, el robo de datos y el robo de identidad, sin pretender eliminar la necesidad de una supervisión informada.

https://player.vimeo.com/video/1134578207

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Puede el ransomware seguir accediendo a los datos almacenados en servicios en la nube como OneDrive o Google Drive?

Respuesta breve: Sí. Aunque el almacenamiento en la nube estuvo alguna vez fuera del alcance del ransomware, los atacantes han adaptado sus métodos y ahora pueden apuntar a los datos almacenados en la nube mediante técnicas como el mapeo de unidades y, más comúnmente hoy en día, el robo de claves de API y tokens de sesión.

Cómo ha cambiado el enfoque del ransomware hacia los datos en la nube

Cuando el trabajo remoto impulsó un rápido cambio hacia el almacenamiento en la nube, tanto las empresas como los ciberdelincuentes se estaban adaptando al nuevo entorno al mismo tiempo. En las primeras etapas de este cambio, el ransomware normalmente no podía tocar los archivos almacenados en plataformas en la nube: si los datos residían en la nube en lugar de en un servidor local, los atacantes generalmente los dejaban en paz porque carecían de una vía directa hacia ellos.

Eso cambió cuando los atacantes aprendieron a conectar manualmente el almacenamiento en la nube, como una cuenta de Amazon, OneDrive o Google Drive, a un sistema infectado. Lo hicieron montando el almacenamiento en la nube como una letra de unidad local, de forma similar a cómo un dispositivo USB aparece como su propia unidad en una computadora. Una vez montados de esta manera, los archivos basados en la nube quedaban tan expuestos al cifrado como los archivos de un disco duro local.

La mayor amenaza actual: claves y tokens robados

A medida que el uso de la nube maduró, las tácticas de los atacantes volvieron a cambiar. En lugar de montar unidades manualmente, muchos ahora van tras las claves de API y los tokens de sesión: credenciales que otorgan acceso directo, a nivel de programa, a las cuentas y datos en la nube. Obtener una de estas es comparable a robar una contraseña, salvo que a menudo proporciona un acceso más amplio y rápido a los recursos en la nube que una contraseña robada por sí sola.

Este cambio es importante porque la misma velocidad y escalabilidad que hacen valiosa la computación en la nube para los equipos de TI legítimos ahora también está disponible para los atacantes. Entre los clientes de Cyber Crucible el año pasado, más de la mitad experimentó un intento de robo de un token de sesión en la nube destinado a secuestrar la sesión activa de un usuario, mientras que menos del 9 % sufrió algún compromiso real de datos. Esto sugiere que los atacantes están priorizando el robo de credenciales y tokens como su principal punto de entrada, con el robo de datos como objetivo secundario.

¿Los datos en la nube están automáticamente seguros?

El almacenamiento en la nube no garantiza protección contra el ransomware ni el robo de datos. Simplemente cambia el método que los atacantes deben usar para acceder a esos datos, desplazando el riesgo principal hacia el compromiso de credenciales y tokens de sesión en lugar del cifrado directo de archivos.

https://player.vimeo.com/video/1047006345

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Si el ransomware se elimina a sí mismo, ¿significa eso que el ataque ha terminado?

Respuesta breve: No. El ransomware moderno suele estar diseñado para autoeliminarse una vez que termina de cifrar los archivos, pero esa autoeliminación no tiene nada que ver con si sus sistemas o datos están realmente a salvo; simplemente elimina la evidencia de la herramienta que causó el daño.

Por qué la "desaparición" del ransomware no significa recuperación

Los atacantes actuales rara vez dependen de una sola pieza de malware para toda una intrusión. En cambio, normalmente utilizan una secuencia de herramientas independientes: una para recolectar credenciales, otra para localizar y exfiltrar datos valiosos, y una final para cifrar los archivos y así maximizar su influencia. Una vez que esa última herramienta de cifrado completa su trabajo, comúnmente se borra a sí misma del sistema. Lo que queda son notas de rescate con instrucciones de contacto y, lo que es más importante, archivos que permanecen bloqueados. La ausencia del malware en sí no es señal de resolución; simplemente significa que, desde la perspectiva del atacante, su trabajo ha finalizado.

Qué sucede realmente con sus datos

Para cuando ocurre el cifrado, el robo de datos ya suele haberse producido, y esa información se pierde sin importar lo que ocurra después. Los archivos cifrados que quedan pueden, en algunos casos, abordarse mediante la negociación con el atacante o mediante herramientas de descifrado, pero no hay garantía de éxito. Las técnicas que antes permitían el descifrado automatizado sin pagar a los atacantes se han vuelto mucho menos efectivas a medida que los operadores de ransomware han adaptado sus métodos. No existe una acción de recuperación sencilla, como reiniciar un dispositivo, que revierta el cifrado.

La verdadera elección después de un ataque

Una vez que el ransomware ha completado su curso y se ha autoeliminado, las organizaciones generalmente se quedan con dos caminos: reconstruir los sistemas y datos afectados a partir de copias de seguridad limpias, o intentar el descifrado mediante el pago y la negociación con el atacante. Ninguna de las dos opciones es rápida ni está garantizada, razón por la cual la prevención —detener el ransomware antes de que ocurra el cifrado y el robo de datos— sigue siendo mucho más efectiva que intentar responder después de los hechos.

https://player.vimeo.com/video/1043482941

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Debería la ciberseguridad centrarse en la resiliencia o en prevenir los ataques desde el principio?

Respuesta breve: La resiliencia —recuperarse después de un ataque— es importante, pero el objetivo más importante es prevenir el ransomware, el robo de datos y el robo de identidad antes de que se produzca el daño, ya que los ataques automatizados son incesantes y cada vez están mejor informados sobre cuándo atacar.

Dos significados de "resiliencia"

El término "resiliencia" en ciberseguridad ha derivado hacia dos ideas distintas. Una es si las propias herramientas de seguridad pueden seguir funcionando bajo ataque —esencialmente, si el software destinado a protegerlo puede sobrevivir a ser atacado o manipulado directamente, de manera similar a preguntarse si una cámara de seguridad puede seguir grabando después de que alguien intente desactivarla. La otra, de significado más tradicional, es si su negocio puede recuperarse y salir adelante después de que ya se haya producido una brecha.

Ambas son importantes, pero ninguna debería ser la estrategia principal. Los ataques modernos son automatizados y constantes. La razón principal por la que las organizaciones no son atacadas sin cesar es que los atacantes se han vuelto expertos en leer señales sobre qué objetivos merecen su tiempo —por ejemplo, evitando a empresas que claramente no cuentan con los recursos financieros para hacer rentable un ataque. Ese nivel de selección automatizada de objetivos significa que la resiliencia por sí sola es una postura reactiva frente a un adversario que siempre está sondeando.

Por qué la prevención debe ser lo primero

Ser resiliente después de una brecha es comparable a tener un buen taller de reparación de confianza después de un accidente automovilístico. Es útil, pero es mucho mejor evitar el accidente por completo. Nadie quiere poner a prueba lo bien que funciona el proceso de reparación si, en

cambio, puede evitar la colisión desde el principio.

Aplicado a la seguridad empresarial, esto significa que la prioridad debe ser detener los ataques antes de que tengan éxito —el equivalente a tener frenos confiables en lugar de solo un buen plan de reparación para después de un choque. Cyber Crucible avanza hacia este resultado centrándose en la prevención autónoma, con el objetivo de detener los intentos de ransomware, robo de datos y robo de identidad antes de que puedan causar daño, en lugar de depender únicamente de la recuperación y la limpieza posteriores.

https://player.vimeo.com/video/1194994916

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Cómo ayuda Cyber Crucible a gestionar proveedores y resultados de ciberseguridad?

Respuesta breve: Cyber Crucible se encarga de la prevención automatizada en el endpoint, lo que le permite seleccionar y responsabilizar a su propio proveedor de monitoreo o respuesta, en lugar de quedar atado a un servicio empaquetado y difícil de evaluar, vinculado a un único proveedor de EDR o XDR.

El problema oculto de los servicios de seguridad empaquetados

Muchas organizaciones pagan sumas considerables por un centro de operaciones de seguridad alojado que viene junto con un producto particular de detección y respuesta en el endpoint o de detección y respuesta extendida. El problema es que este tipo de arreglo a menudo deja al cliente con poca visibilidad sobre qué tan atento o eficaz es realmente ese servicio de monitoreo. Es posible que no sepa con qué nivel de detalle se está vigilando su entorno, con qué rapidez se escalan los problemas, o si su cuenta es prioritaria para ese proveedor. Debido a que el monitoreo está vinculado a la tecnología subyacente, hay poco margen para negociar, medir o reemplazar el servicio si no cumple con las expectativas.

Separar la prevención del monitoreo restaura el control

Cyber Crucible se centra en la capa de prevención de la protección de endpoints, deteniendo automáticamente los intentos de ransomware, robo de datos y robo de identidad. Debido a que la prevención se gestiona de forma independiente, las organizaciones ya no están obligadas a aceptar un paquete único para detección y respuesta. En cambio, obtiene la libertad de elegir el socio de detección y respuesta gestionada (MDR) o de servicios de seguridad gestionados (MSSP) que mejor se adapte a sus necesidades, ya sea su propio personal interno, un MSSP especializado, u otro proveedor de MDR completamente distinto.

Por qué importa la elección

Esta separación le brinda la capacidad de definir sus propios acuerdos de nivel de servicio, medir la calidad y la capacidad de respuesta del equipo que monitorea su entorno, y responsabilizar a ese proveedor mediante una relación contractual real. En lugar de esperar que un proveedor empaquetado le esté prestando la atención adecuada, puede evaluar y hacer cumplir estándares de desempeño según sus propios términos. En definitiva, el enfoque de Cyber Crucible consiste en otorgar a las organizaciones un control genuino: control frente a los atacantes y, con igual importancia, control sobre las relaciones y contratos con los proveedores que respaldan su programa de seguridad.

https://player.vimeo.com/video/1046829518

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Cómo ayuda Cyber Crucible a controlar el gasto en ciberseguridad y los contratos con proveedores?

Respuesta breve: Cyber Crucible no necesariamente reduce su presupuesto total de seguridad, pero le brinda mayor control sobre cómo se gasta ese presupuesto, ya que le permite separar la prevención de ransomware y robo de datos de los servicios de monitoreo y respuesta, de modo que usted pueda elegir y responsabilizar al proveedor que se encarga de estos últimos.

El costo oculto de los servicios de SOC agrupados

Muchas organizaciones pagan sumas considerables a un centro de operaciones de seguridad (SOC) alojado que viene agrupado con una plataforma EDR o XDR. El desafío de este tipo de acuerdo es que el cliente normalmente tiene poca visibilidad sobre qué tan atento o eficaz es realmente ese equipo de monitoreo. No existe una manera sencilla de medir la calidad de la respuesta, el compromiso del personal o qué tan en serio se prioriza su cuenta. Básicamente, usted confía en que el servicio que opera detrás de escena funciona bien, sin contar con una forma práctica de verificarlo.

Separar la prevención del monitoreo

Cyber Crucible se centra específicamente en el aspecto de prevención de la protección de endpoints, deteniendo el ransomware, el robo de datos y el robo de identidad antes de que se produzca algún daño. Debido a que la prevención se gestiona de forma independiente, las organizaciones ya no están obligadas a depender de un único proveedor agrupado tanto para la prevención como para el monitoreo. Esto significa que usted puede seleccionar su propio proveedor de detección y respuesta gestionadas (MDR), un MSSP, o incluso confiar en su propio equipo interno para el monitoreo y la respuesta continuos.

Recuperar el control sobre la responsabilidad de los proveedores

Esta separación es importante porque restaura su capacidad de negociar y hacer cumplir acuerdos de nivel de servicio claros con los proveedores que usted elija. Puede evaluar la capacidad de respuesta, medir el desempeño y responsabilizar a los proveedores de maneras que no son posibles cuando la prevención y el monitoreo están vinculados bajo un mismo contrato. En resumen, el valor no reside únicamente en la defensa técnica contra los atacantes, sino en recuperar la supervisión y el control sobre sus propias relaciones con los proveedores, los contratos y la calidad del servicio por el que está pagando.

https://player.vimeo.com/video/1046667196

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Funciona Cyber Crucible junto con otras herramientas de ciberseguridad y EDR?

Respuesta breve: Sí. Cyber Crucible está construido sobre sus propios sensores patentados y su tecnología de monitoreo de comportamiento, por lo que funciona junto con prácticamente cualquier otro producto de seguridad sin interferir con las herramientas existentes.

Por qué la compatibilidad no es un problema

Cyber Crucible no depende de ganchos (hooks) de EDR compartidos ni de integraciones a nivel de sistema de las que también dependen otros proveedores de seguridad. Dado que su enfoque de detección y monitoreo, incluidos los métodos de recopilación de comportamiento que respaldan a FortressAI, está construido de manera personalizada desde cero, no compite por los mismos recursos del sistema ni interfiere con los ganchos que utilizan otras herramientas de protección de endpoints. Este diseño permite que Cyber Crucible funcione como una capa de protección adicional en lugar de un reemplazo o una superposición conflictiva. Se ha implementado junto con productos de una amplia variedad de proveedores de seguridad establecidos y, en la práctica, la mayoría de los entornos no muestran ningún problema de compatibilidad.

Cuándo se necesitan ajustes

La rara situación que requiere una configuración adicional involucra software personalizado, desarrollado internamente por una empresa. Ocasionalmente, estas herramientas propias exhiben patrones de comportamiento que se asemejan al tipo de actividad que Cyber Crucible está diseñado para detectar, como cambios rápidos de archivos o interacciones inusuales con el sistema. Cuando esto ocurre, la solución es sencilla: se puede agregar una regla de exclusión simple para que Cyber Crucible reconozca la herramienta interna como legítima. Esta exclusión permanece confiable siempre que el software interno se mantenga correctamente firmado y sin modificaciones, es decir, que continúe coincidiendo con su estado esperado y verificado. Si se cumplen esas condiciones, la herramienta funciona con normalidad junto con Cyber Crucible sin fricciones continuas.

Qué significa esto para los equipos de seguridad

Las organizaciones no necesitan eliminar ni reconfigurar su conjunto de herramientas de seguridad actual para adoptar Cyber Crucible. Está diseñado para complementar las defensas existentes, añadiendo una capa dedicada centrada en la prevención de ransomware, robo de datos y robo de identidad, sin interrumpir las herramientas que ya protegen el entorno.

https://player.vimeo.com/video/1043463490

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué la IA es un riesgo empresarial, y no solo una herramienta de productividad, para los directivos de la empresa?

Respuesta breve: Los equipos directivos suelen considerar la IA únicamente como un impulsor de la productividad, pero el uso no gestionado de la IA puede exponer secretos empresariales fundamentales —planes de producto, datos de ingresos y estrategia de ventas— directamente a partes externas. Se trata de un riesgo estratégico y financiero que debe estar sobre la mesa del CEO, el CFO, el COO y la dirección de ventas, y no solo del departamento de TI.

Un tipo de exposición diferente

Los incidentes tradicionales de ciberseguridad, como una filtración de datos que termina con registros de clientes en la dark web, siguen un patrón conocido: la dirección responde, los reguladores pueden intervenir, en ocasiones se pagan multas y la junta directiva recibe un informe. Las empresas ya han lidiado antes con este tipo de escenarios, y existen procesos para gestionarlos.

La IA introduce una nueva categoría de exposición, menos comprendida. Cuando los empleados utilizan herramientas de IA sin las salvaguardas adecuadas, es posible que estén introduciendo información empresarial confidencial —planes de producto futuros, previsiones de beneficios, canalizaciones de ventas— en sistemas que nunca fueron diseñados para contener esa información. A diferencia de un incidente de hackeo, esto no es necesariamente el resultado de un ataque. Puede ocurrir simplemente por el uso normal y bien intencionado de la IA por parte del personal.

El problema de las consultas internas

Un riesgo que suele pasarse por alto es lo que ocurre dentro de una empresa una vez que una herramienta de IA tiene un acceso amplio a documentos y datos internos. Si los controles de

acceso no se diseñan cuidadosamente, un empleado podría hacerle una simple pregunta a un asistente de IA y recibir una respuesta detallada que contenga planes confidenciales que nunca deberían circular libremente, ni siquiera internamente. Eso es un fallo de gobernanza, no un error técnico, y puede ser tan perjudicial como una filtración externa.

Por qué esto corresponde al nivel directivo

No invertir en un entorno de IA interno debidamente controlado no elimina esta categoría de riesgo; simplemente la desplaza fuera de la supervisión directa de la organización. Los líderes empresariales jamás considerarían publicar estados de pérdidas y ganancias o canalizaciones de ventas en un sitio web público. El uso no gestionado de la IA puede generar un resultado similar sin que nadie lo pretenda. Tratar esto como un riesgo empresarial central, y no como un asunto puramente técnico, es esencial para proteger las ventajas competitivas que la dirección se ha esforzado en construir.

https://player.vimeo.com/video/1211538534

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Los empleados ya están usando herramientas de IA antes de que nuestra empresa tenga una política oficial de IA?

Respuesta breve: Sí. La mayoría de las organizaciones descubren que empleados, contratistas, consultores y proveedores ya están utilizando herramientas de IA de maneras creativas e inesperadas mucho antes de que se finalice cualquier política formal de IA o proyecto de gobernanza. Esperar a tener una política "perfecta" antes de abordar el uso de la IA deja a la empresa ciega ante lo que ya está sucediendo.

La suposición común

Muchos líderes suponen que la adopción de IA dentro de su organización está en pausa hasta que se redacte, apruebe e implemente una política oficial. La idea es que los empleados esperarán pacientemente a tener reglas claras antes de experimentar con nuevas herramientas. En la práctica, esta suposición rara vez se sostiene. Las personas tienden a buscar formas de trabajar de manera más eficiente, exista o no una directriz formal todavía.

Lo que realmente encuentran las organizaciones

Cuando las empresas implementan herramientas de monitoreo o cumplimiento, como FortressAI de Cyber Crucible, a menudo descubren que el uso de IA está mucho más extendido y es más variado de lo esperado. El personal es ingenioso por naturaleza; esa misma creatividad y capacidad de resolución de problemas que los convierte en empleados valiosos también los lleva a encontrar nuevas formas no autorizadas de usar herramientas de IA para ahorrar tiempo o mejorar su rendimiento. Esto no es tanto una señal de mala intención como de naturaleza humana: las personas utilizarán las herramientas disponibles para facilitar su trabajo, sin importar si una política lo permite oficialmente o no.

Por qué la visibilidad importa más que una política perfecta

El verdadero riesgo no es que aún no se haya finalizado una política. Es que las organizaciones a menudo carecen de visibilidad sobre cómo ya se está utilizando la IA en su entorno. Sin esa visibilidad, los equipos de seguridad y cumplimiento no pueden evaluar la exposición a la fuga de datos, el uso no autorizado de herramientas u otros riesgos vinculados a la adopción de la IA. En lugar de esperar a que se complete un marco integral de gobernanza de IA, las organizaciones se benefician al obtener primero información sobre los patrones de uso actuales. Comprender lo que realmente está sucediendo sobre el terreno permite que las políticas se basen en la realidad y no en suposiciones sobre el comportamiento de los empleados.

https://player.vimeo.com/video/1176537677

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Cuáles son las señales de advertencia de que está ocurriendo un ataque de ransomware?

Respuesta breve: Una vez que se activa el ransomware, puede paralizar un negocio en tan solo 60 a 90 segundos, por lo que las señales de advertencia visibles tienden a aparecer solo cuando el ataque ya está desarrollándose, no con la suficiente antelación como para detenerlo manualmente. La verdadera defensa consiste en detectar el trabajo de preparación que realizan los atacantes de antemano, antes de que lleguen a activar el detonante final.

Por qué el ransomware parece repentino

Los ataques de ransomware suelen describirse como instantáneos, pero eso es engañoso. Los atacantes normalmente pasan tiempo dentro de una red de antemano, mapeando silenciosamente los sistemas, obteniendo acceso y posicionándose para causar el máximo daño. Este trabajo preparatorio es similar al de un equipo militar que prepara un campo de batalla antes de que comience una operación. Una vez que todo está listo, el evento real de cifrado o bloqueo puede completarse en menos de dos minutos. Para cuando los empleados notan que algo anda mal, el daño ya está, en gran medida, en marcha.

Cómo se ve el momento del ataque

Cuando se ejecuta un ataque, las empresas suelen notar un cambio repentino e inquietante: ciertas aplicaciones o servicios dejan de responder, las conexiones de red se vuelven inestables, los sistemas telefónicos pueden caerse y las operaciones normales se sienten interrumpidas casi al mismo tiempo. Igual de inquietante es que algunos sistemas siguen funcionando con normalidad durante esta ventana. Esa aparente normalidad no es una buena señal. A menudo significa que los atacantes están utilizando esos sistemas no afectados como cobertura mientras el resto del entorno está siendo comprometido.

Por qué la detección temprana importa más que la reacción

Dado que las señales visibles del ransomware aparecen únicamente en los segundos finales y de rápido desarrollo de un ataque, esperar para reaccionar ante esas señales no es una estrategia confiable. Una protección significativa depende de identificar y detener la actividad maliciosa durante la etapa de preparación, antes de que los atacantes estén listos para actuar. Esta es la capa en la que están diseñadas para operar herramientas de detección autónoma como FortressAI de Cyber Crucible, con el objetivo de interrumpir el comportamiento del atacante antes de que llegue al punto de no retorno, en lugar de esperar los síntomas externos que aparecen cuando el ataque ya está en curso.

https://player.vimeo.com/video/1043488930

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Qué sucede realmente en los momentos durante un ataque de ransomware?

Respuesta breve: La fase de cifrado real de un ataque de ransomware es sorprendentemente rápida, y a menudo se completa en aproximadamente 60 a 90 segundos una vez activada, aunque los atacantes dedican un tiempo considerable y no visible previamente a posicionarse dentro de una red. Para el momento en que aparecen síntomas visibles, el daño ya está ocurriendo en tiempo real, razón por la cual la detección debe producirse antes del desencadenante final, no después.

La calma antes del ataque

Antes de que el ransomware se active, los atacantes suelen pasar tiempo moviéndose silenciosamente por los sistemas de una empresa, identificando datos valiosos, desactivando copias de seguridad y estableciendo las condiciones necesarias para un ataque exitoso. Este trabajo preparatorio puede pasar inadvertido porque las operaciones normales del negocio continúan como de costumbre. La red puede parecer estable y saludable justo hasta el momento en que el atacante decide lanzar la etapa final. De manera similar a un inquietante silencio justo antes de que ocurra algo catastrófico, este período de calma puede ser engañoso, ya que no refleja la interrupción que está por ocurrir.

La rápida aparición del daño

Una vez lanzado, un evento de ransomware puede desarrollarse en menos de dos minutos. En esa breve ventana de tiempo, los empleados pueden notar interrupciones súbitas: el correo electrónico deja de funcionar, los sistemas telefónicos quedan en silencio, las aplicaciones se comportan de manera errática o las conexiones de red se vuelven inestables. Estos son síntomas del cifrado y del compromiso del sistema ocurriendo simultáneamente en todo el entorno. Debido a que el proceso avanza con tanta rapidez, normalmente no hay suficiente tiempo para que una persona intervenga manualmente una vez que comienza.

Por qué algunos sistemas siguen funcionando

Un detalle inquietante de muchos incidentes de ransomware es que no todo falla al mismo tiempo. Algunos servicios pueden seguir funcionando con normalidad incluso mientras otros colapsan. Esto suele ocurrir porque esos sistemas no afectados son precisamente donde el atacante todavía está operando, utilizándolos como punto de apoyo o área de preparación. Reconocer este patrón es importante, ya que asumir que un problema es "solo parcial" puede crear una falsa sensación de seguridad mientras el compromiso está activamente en curso. La prevención eficaz depende de identificar y detener la actividad maliciosa antes de que comience la etapa destructiva final, ya que, una vez activada, la ventana de acción es extremadamente breve.

https://player.vimeo.com/video/1046658956

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Qué sucede realmente cuando el ransomware ataca un servidor de una empresa?

Respuesta breve: Cuando el ransomware ataca un servidor, los atacantes normalmente deshabilitan primero sus servicios y luego cifran sus datos mientras impiden que los equipos de TI y seguridad puedan intervenir, a veces utilizando docenas o incluso cientos de estaciones de trabajo comprometidas para llevar a cabo el cifrado de forma remota.

Las primeras señales de un ataque

Uno de los primeros indicadores de que un servidor ha sido comprometido es una pérdida repentina de servicio. Dado que los atacantes saben que el ransomware puede corromper archivos accidentalmente durante el cifrado, muchos deciden deliberadamente detener las aplicaciones que se ejecutan en un servidor antes de que comience el proceso de cifrado. Esto significa que los empleados o clientes que dependen de ese sistema —ya sea una plataforma de nómina, una aplicación web u otro servicio crítico para el negocio— pueden notar una interrupción antes de que nadie se dé cuenta de que se está produciendo un incidente de seguridad.

Bloqueando a los defensores mientras el cifrado se propaga

Una vez que el ataque está en marcha, el ransomware comienza a cifrar los datos almacenados en el servidor. Para evitar que los equipos de seguridad o los administradores intervengan, los atacantes suelen bloquear el acceso de red al servidor, aislándolo de las personas que normalmente responderían ante la amenaza. Esta táctica le da al atacante tiempo para terminar de cifrar los archivos antes de que los defensores puedan actuar.

Las estaciones de trabajo pueden ser el verdadero punto débil

Curiosamente, el servidor en sí no siempre es el origen del peligro. En muchos casos, los atacantes comprometen una gran cantidad de estaciones de trabajo de empleados —a veces 50, 70 o más— que ya cuentan con acceso legítimo al servidor. Estas estaciones de trabajo se utilizan luego simultáneamente para cifrar los datos del servidor de forma remota. Debido a que el ataque se lanza desde múltiples puntos finales a la vez, las estaciones de trabajo conectadas al servidor a menudo representan una vulnerabilidad mayor que la propia infraestructura del servidor.

Este patrón resalta por qué la defensa contra el ransomware no puede centrarse únicamente en los servidores. La seguridad de los puntos finales en todos los dispositivos con acceso al servidor desempeña un papel fundamental para detener los ataques antes de que el cifrado se propague. FortressAI de Cyber Crucible está diseñado para identificar e interrumpir estos comportamientos en las etapas más tempranas, ya sea que la amenaza se origine en un servidor o se propague desde estaciones de trabajo conectadas.

https://player.vimeo.com/video/1041172405

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué el ransomware ataca los archivos compartidos antes de llegar a mi escritorio?

Respuesta breve: Cuando el ransomware infecta una estación de trabajo individual, esa máquina rara vez es el objetivo real. Los atacantes utilizan la infección inicial como punto de partida para alcanzar recursos de red compartidos, y solo cifran o dañan el escritorio local después de haber atacado ya datos de mayor valor en otros lugares.

Por qué el escritorio es la última parada, no la primera

Un error común es pensar que, si el ransomware se instala en el equipo de un empleado en particular, los archivos de ese empleado son lo que persiguen los atacantes. En realidad, el malware está programado para ir más allá de la máquina local casi de inmediato. Una vez que obtiene acceso, comienza a escanear la red en busca de recursos accesibles de mayor valor, como servidores de archivos, wikis internas o bases de datos que contienen información de clientes. Cifrar o exfiltrar estos datos centralizados es el verdadero objetivo, ya que afecta a una parte mucho mayor de la organización que la carpeta de un solo usuario.

La nota de rescate llega al final, no al principio

Debido a que los atacantes priorizan los datos de toda la red antes de tocar el dispositivo de origen, el empleado infectado suele ser la última persona en notar que algo anda mal. Para cuando aparece una nota de rescate en la pantalla de esa persona, los atacantes ya suelen haber terminado de cifrar o robar datos en gran parte de la infraestructura de la empresa. Esta secuencia es intencional. Permite a los atacantes infligir el máximo daño operativo antes de que alguien en la organización tenga la oportunidad de detectar la intrusión o responder a ella. La nota de rescate visible es, en esencia, una señal de que el daño más grave ya ha ocurrido entre bastidores.

Qué significa esto para la defensa

Las fotos o documentos personales almacenados localmente en un escritorio suelen ser el objetivo menos importante en un ataque de ransomware, aunque puedan ser la señal más visible de uno. Una defensa eficaz debe tener en cuenta este patrón centrándose en detectar y detener la actividad maliciosa lo antes posible, antes de que pueda alcanzar los sistemas compartidos. FortressAI de Cyber Crucible está diseñado teniendo en cuenta esta secuencia de ataque, con el objetivo de intervenir en las primeras etapas de una intrusión en lugar de reaccionar únicamente cuando el cifrado se hace visible en máquinas individuales.

https://player.vimeo.com/video/1043466243

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Qué inspiró al fundador a crear Cyber Crucible?

Respuesta breve: Cyber Crucible surgió de una carrera dedicada a desarrollar soluciones únicas para misiones gubernamentales clasificadas, y del deseo de aplicar ese mismo impulso de resolución de problemas para ayudar a muchas más personas a combatir el ransomware y el cibercrimen en todo el mundo.

De misiones clasificadas a un problema global

Mucho antes de que Cyber Crucible existiera como empresa, su fundador ya resolvía problemas de seguridad complejos, incluyendo la identificación de una forma de tomar el control de una botnet para proteger a las personas de ella. Ese patrón de descomponer desafíos técnicos difíciles y diseñar soluciones prácticas se trasladó a una carrera en la Agencia de Seguridad Nacional (NSA) y en otras organizaciones gubernamentales. Una y otra vez, se construía una nueva herramienta o técnica para resolver una necesidad específica de una misión, solo para usarse una vez, entregarse a un equipo aliado o dejarse de lado después de cumplir su propósito limitado. Cada invención era importante, pero su impacto se detenía en el límite de una única misión clasificada.

Convertir soluciones individuales en algo que todos puedan usar

Ese ciclo de resolver un problema y luego ver cómo su utilidad permanecía contenida en un solo equipo u operación se volvió frustrante con el tiempo, aunque el trabajo en sí fuera significativo. Cuando el ransomware surgió como una amenaza generalizada, presentó un tipo diferente de oportunidad: la posibilidad de aplicar ese mismo enfoque inventivo, pero dirigido a un problema que afecta a organizaciones e individuos en todas partes, no solo a una unidad especializada. La conclusión fue que ayudar a una población más amplia de personas requería más que otra herramienta personalizada para un caso de uso limitado. Requería un producto comercial que pudiera implementarse de manera fácil y confiable a gran escala.

Por qué esto define a Cyber Crucible hoy

Ese cambio de mentalidad es la base del enfoque de Cyber Crucible. En lugar de construir una solución para un solo equipo o una sola misión, el objetivo es crear tecnología, impulsada por FortressAI, que funcione de manera automática y constante para organizaciones de todo el mundo, de modo que menos personas tengan que experimentar el daño y la interrupción causados por el ransomware, el robo de datos y el robo de identidad. El trabajo enfocado en misiones del pasado sigue siendo importante, pero el propósito que impulsa a Cyber Crucible es alcanzar y proteger al mayor número de personas posible.

https://player.vimeo.com/video/1046673820

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿De dónde provienen realmente los ataques de ransomware?

Respuesta breve: Los operadores de ransomware no se limitan a un puñado de países conocidos; la automatización y las herramientas delictivas económicas permiten ahora que los atacantes operen desde casi cualquier parte del mundo.

La historia simplificada de los medios no coincide con la evidencia

La cobertura noticiosa suele señalar a un solo país o región como origen de los ataques de ransomware porque eso permite un titular rápido y fácil de digerir. En la práctica, la experiencia directa respondiendo a incidentes en curso cuenta una historia mucho más compleja. Cuando Cyber Crucible comenzó a gestionar casos activos de ransomware, nuestro equipo recibió una amplia variedad de llamadas telefónicas relacionadas con los ataques, muchas de ellas provenientes de teléfonos prepago o desechables ("de usar y tirar") sin historial de propiedad rastreable. Estas llamadas provenían de muchas regiones diferentes, incluyendo el sur de Asia, Oriente Medio, partes de Europa, Sudamérica e incluso Norteamérica. Algunos de los interlocutores eran operadores de bajo nivel, mientras que otros parecían ser los verdaderos desarrolladores del malware, quienes en ocasiones mantenían conversaciones sorprendentemente profesionales, de igual a igual, sobre los detalles técnicos de sus ataques.

La automatización ha reducido la barrera de entrada

Si bien ciertas regiones del mundo pueden seguir produciendo una proporción desmedida de desarrolladores de ransomware con gran habilidad técnica, el auge de los kits de ransomware como servicio, las herramientas de automatización y el uso básico de asistencia de IA para las comunicaciones ha facilitado enormemente la participación de actores menos sofisticados. Alguien con habilidades técnicas limitadas puede ahora alquilar infraestructura de ataque, comprar acceso robado a redes a través de intermediarios de acceso inicial ("initial access brokers") y ejecutar una campaña de extorsión con una inversión inicial mínima. Esto ha abierto efectivamente la puerta a que delincuentes oportunistas ubicados en cualquier lugar participen, en lugar de restringir la actividad del ransomware a un pequeño conjunto de grupos vinculados a estados-nación.

Por qué esto importa para la defensa

La jerga regional, los patrones de lenguaje y el comportamiento de las llamadas observados durante estos incidentes refuerzan la idea de que los atacantes están geográficamente dispersos, y no limitados a una sola nación "actor malicioso". Entender el ransomware como una empresa criminal distribuida globalmente e impulsada por la automatización, en lugar de una narrativa geopolítica simplista, conduce a estrategias de defensa mejor fundamentadas y a una visión más clara del riesgo real que enfrentan las organizaciones.

https://player.vimeo.com/video/1047715735

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿A quién atacan realmente hoy los ciberdelincuentes de ransomware?

Respuesta breve: los operadores de ransomware ya no se centran únicamente en organizaciones grandes y de alto perfil. La automatización y las herramientas basadas en IA han hecho rentable atacar a empresas de casi cualquier tamaño, lo que significa que la mayoría de las organizaciones deben asumir que son un objetivo potencial.

Cómo ha cambiado la selección de objetivos desde 2020

En los primeros días del ransomware moderno, llevar a cabo un ataque desde el acceso inicial hasta la extorsión requería hackers expertos y experimentados que trabajaban en gran medida de forma manual. Eso limitaba el número de atacantes capaces y mantenía el foco en objetivos grandes y de alto valor, donde el beneficio justificaba el esfuerzo.

A medida que creció la demanda, los grupos de hackers ya establecidos comenzaron a operar más como negocios en expansión. En lugar de depender únicamente de un pequeño número de operadores expertos, empezaron a crear programas de ransomware como servicio que empaquetan métodos de ataque probados en manuales de estrategias repetibles y automatizados. Esto permitió que operadores con menos experiencia llevaran a cabo campañas efectivas, de manera similar a como un vendedor junior puede tener éxito utilizando un guion elaborado a partir de los métodos de un vendedor destacado.

Por qué las organizaciones más pequeñas ahora están en riesgo

La automatización, el aprendizaje automático y la automatización robótica de procesos permiten a estos operadores ejecutar muchos ataques a la vez, gestionar las negociaciones de rescate y administrar el soporte de pago o recuperación a gran escala. Una vez que estas funciones se automatizaron en gran medida, atacar a empresas más pequeñas también se volvió rentable, ya que son las máquinas —y no las personas— quienes gestionan la mayor parte del contacto y el seguimiento.

Este cambio significa que los atacantes son menos selectivos. Los objetivos "de gran envergadura" siguen atrayendo atención debido al tamaño de un posible pago, pero la actividad cotidiana de estas operaciones criminales se asemeja cada vez más a la prospección de ventas rutinaria: sistemas automatizados que buscan continuamente cualquier organización que pueda pagar. Los sistemas que realizan la selección de objetivos generalmente no tienen conocimiento alguno de quién o qué es realmente el objetivo, ya sea una gran empresa o una pequeña organización sin fines de lucro.

Qué significa esto para las organizaciones

Dado que la selección de objetivos es en gran medida automatizada e indiscriminada, la pregunta más relevante para la mayoría de las organizaciones no es si podrían ser elegidas específicamente, sino qué tan preparadas están ante un eventual intento. Soluciones como Cyber Crucible, construidas sobre FortressAI, están diseñadas para ayudar a las organizaciones a detectar y detener el ransomware y las amenazas relacionadas, sin importar el tamaño o el perfil del objetivo.

https://player.vimeo.com/video/1047715793

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Quién corre mayor riesgo de sufrir un ataque de ransomware y por qué son elegidos como objetivo?

Respuesta breve: el riesgo de ransomware a menudo depende de a quién los "corredores de acceso" criminales encuentran más fácil de vulnerar o a quién se les paga específicamente por vulnerar, lo que significa que las escuelas, los hospitales y los proveedores de infraestructura con defensas más débiles o datos valiosos suelen encabezar la lista.

Cómo se eligen los objetivos en primer lugar

Detrás de la mayoría de los incidentes de ransomware existe un mercado que la mayoría de las personas nunca ve. Un grupo, a menudo denominado corredores de acceso inicial, dedica su tiempo a irrumpir en las redes sin ningún plan específico sobre lo que sucederá a continuación. Una vez que han obtenido un punto de apoyo, anuncian ese acceso para su venta, describiendo exactamente qué controlan, como derechos administrativos sobre herramientas de seguridad, la capacidad de desactivar protecciones antivirus o el acceso a una gran parte de los dispositivos de una organización. Podrían describir, por ejemplo, haber comprometido la flota de dispositivos de un distrito escolar o las herramientas de acceso remoto de un proveedor de TI. Los compradores, que van desde grupos de robo de datos hasta operadores de ransomware y actores patrocinados por estados, luego pujan por ese acceso según lo valioso y completo que parezca.

Cuando los ataques son encargados, no solo oportunistas

También existe un segundo patrón, más dirigido. Aquí, un comprador, como un grupo de ransomware o un actor estatal, presenta una solicitud específica: encontrar y comprometer un número determinado de organizaciones que cumplan ciertos criterios, como hospitales de un tamaño particular en una región específica, o proveedores de servicios públicos como plantas de

tratamiento de agua. Los corredores de acceso entonces tratan esto como una tarea de ventas, buscando activamente organizaciones que se ajusten al perfil. Una vez que tienen éxito, venden ese acceso al solicitante original, aunque ambas partes por lo general nunca interactúan directamente ni conocen la identidad de la otra. Por eso, los grupos repentinos de ataques contra organizaciones similares, como varios hospitales en una misma región, a menudo reflejan una orden de compra coordinada en lugar de una coincidencia.

Por qué esto importa para la defensa

Debido a que la selección de objetivos puede ser tanto oportunista como específicamente encargada, cualquier organización con controles de seguridad débiles, datos sensibles o servicios críticos puede convertirse en un objetivo, independientemente de su tamaño o sector. Comprender esta dinámica entre compradores y vendedores subraya por qué las defensas proactivas y siempre activas importan más que reaccionar después de que una vulneración ya haya sido vendida al mejor postor.

https://player.vimeo.com/video/1047715835

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Quién dirige realmente los ataques de ransomware y cómo operan?

Respuesta breve: Los ataques de ransomware son llevados a cabo por una red poco organizada de desarrolladores, revendedores y operadores que funcionan de forma muy similar a una cadena de suministro empresarial, y los más eficaces tratan la extorsión como un oficio profesional en lugar de un rencor personal.

El ransomware como cadena de suministro organizada

El ransomware rara vez es obra de un solo hacker que actúa en solitario. En cambio, funciona más como una industria distribuida integrada por desarrolladores de malware que crean las herramientas, revendedores o afiliados que distribuyen el acceso a ese malware, y operadores que llevan a cabo los ataques reales contra las víctimas. Cada grupo desempeña una función distinta, de forma similar a como un proveedor de software legítimo podría depender de fabricantes, distribuidores y equipos de ventas. Esta estructura por capas es parte de lo que hace resiliente al ransomware: interrumpir un eslabón de la cadena no necesariamente detiene la operación en su conjunto.

Los profesionales frente a los atacantes emocionales

No todos los atacantes se comportan de la misma manera una vez que sus intentos son bloqueados. Cyber Crucible ha experimentado directamente este contraste. En un caso, un atacante vinculado a Europa del Este llamó después de ser detenido, tratando el encuentro como un rompecabezas técnico por resolver en lugar de un insulto personal. Ese individuo incluso hizo referencia a detalles internos del software para demostrar que había realizado ingeniería inversa del producto, y luego continuó contactando periódicamente después, hablando de sus operaciones casi como lo haría un colega.

En contraste, otro atacante vinculado a Bangladesh reaccionó con ira y hostilidad después de ser frustrado, recurriendo a insultos en lugar de buscar soluciones. Ese contacto no continuó interactuando con el tiempo.

Por qué esto importa para la defensa

Estas experiencias sugieren que los actores de amenazas más "exitosos" y persistentes tienden a ser aquellos que abordan el ransomware como un desafío empresarial: metódicos, pacientes y enfocados en encontrar soluciones alternativas. Entender a los atacantes como adversarios de tipo empresarial, en lugar de simplemente criminales caóticos, ayuda a orientar el diseño de tecnologías defensivas como FortressAI de Cyber Crucible: anticipar intentos calculados de eludir las protecciones, no solo ataques aislados o impulsados por la emoción.

https://player.vimeo.com/video/1047715866

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Quién es el cliente ideal para la protección contra ransomware de Cyber Crucible?

Respuesta breve: Cyber Crucible es la opción más adecuada para las personas que piensan en términos de impacto empresarial, no solo de características técnicas. Esto incluye a líderes de TI con recursos limitados y a ejecutivos que comprenden lo que incluso una breve interrupción podría costarle a la empresa.

Por qué el pensamiento empresarial importa más que el cargo

No existe un único cargo que defina al cliente ideal de Cyber Crucible. Lo que importa es si la persona comprende las consecuencias reales de un incidente de ransomware o de robo de datos: pérdida de ingresos, interrupción de operaciones y el tipo de daño financiero que puede perdurar durante meses o años después. Alguien con esta mentalidad no necesita que lo convenzan de que la prevención automatizada vale la pena; ya entiende que evitar el tiempo de inactividad está directamente relacionado con proteger las ganancias y mantener el negocio en funcionamiento.

Esto es diferente de una conversación de ventas puramente técnica, en la que el valor de un producto queda enterrado bajo jerga que solo los especialistas pueden seguir. El enfoque de Cyber Crucible, impulsado por FortressAI, se diseñó en torno a un resultado sencillo y práctico para los clientes en primer lugar, con la tecnología subyacente construida para respaldar ese resultado. Debido a esto, las conversaciones más claras suelen darse con personas que se preocupan por lo que significa una falla de seguridad para el negocio, no solo por cómo funciona el software internamente.

Ejemplos de los interlocutores adecuados

Un director de TI que gestiona personal y presupuesto limitados, y que es personalmente responsable del tiempo de actividad y la fiabilidad del sistema, suele comprender el valor rápidamente, ya que el tiempo de inactividad afecta su carga de trabajo diaria y su desempeño.

Por otro lado, un CEO o un CFO puede impulsar la protección automatizada incluso cuando un equipo de seguridad se siente satisfecho con las medidas existentes, simplemente porque reconoce que una breve interrupción, a veces de tan solo una hora, puede generar un daño financiero que tarda más de un año en recuperarse.

El punto en común

Ya sea que la conversación comience con un líder de TI centrado en las operaciones o con un ejecutivo con mentalidad financiera, el ajuste más fuerte para Cyber Crucible es cualquier persona que evalúe la ciberseguridad a través del prisma de la continuidad del negocio y el riesgo financiero, en lugar de únicamente el detalle técnico.

https://player.vimeo.com/video/1046877762

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué los ataques de ransomware son cada vez más comunes cada año?

Respuesta breve: Los ataques de ransomware están aumentando porque los grupos de ciberdelincuentes han evolucionado de actores desorganizados y oportunistas a operaciones disciplinadas que utilizan la automatización para atacar a muchas víctimas de manera eficiente y extraer el pago rápidamente.

De startups caóticas a operaciones organizadas

Cuando el ransomware se convirtió por primera vez en una amenaza generalizada, muchos atacantes eran inexpertos. Una ola de personas recientemente desempleadas durante la era de la pandemia intentó incursionar en el cibercrimen, a menudo con resultados inconsistentes. Como ocurre con cualquier industria emergente, solo los operadores más organizados y capaces sobrevivieron a ese período inicial de depuración. Con el tiempo, estos grupos comenzaron a funcionar menos como oportunistas dispersos y más como negocios estructurados enfocados en generar ingresos consistentes.

Para 2024, esta madurez se ha traducido en una fuerte dependencia de la automatización. Las operaciones de ransomware establecidas ahora utilizan herramientas automatizadas para incorporar a participantes menos experimentados en sus ataques, manteniendo al mismo tiempo procesos eficientes y repetibles. Esto les ha permitido escalar su actividad mucho más allá de lo que un pequeño equipo de hackers expertos podría lograr manualmente.

Calibrar el ataque para obtener el máximo pago

Una parte clave de esta evolución es aprender a dimensionar correctamente un ataque. Si una intrusión es demasiado leve, un equipo de TI bien preparado simplemente puede restaurar los sistemas y evitar pagar nada. Si un ataque es demasiado extenso y elimina toda la infraestructura de la empresa, es posible que no quede ningún negocio viable para emitir un pago de rescate. Los

grupos de ransomware modernos apuntan a un punto intermedio: suficiente disrupción para presionar a una empresa a pagar rápidamente, sin causar tanto daño que la recuperación o la negociación se vuelvan irrelevantes.

Por qué la automatización impulsa el aumento

Una vez que un proceso de ataque puede automatizarse, los ciberdelincuentes ya no se conforman con perseguir a una sola víctima a la vez. Utilizando herramientas que se asemejan a la inteligencia artificial, el aprendizaje automático y la automatización robótica de procesos, pueden atacar a docenas o cientos de organizaciones en paralelo. Muchas víctimas optan por no divulgar públicamente los incidentes, lo que permite a los atacantes completar un ciclo de extorsión y pasar a nuevos objetivos. Este modelo de negocio escalado y repetible—más que cualquier nueva tecnología en particular—es la razón principal por la que los ataques de ransomware continúan en aumento.

https://player.vimeo.com/video/1043463561

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué Cyber Crucible utiliza IA en lugar de un equipo humano de SOC para detener el ransomware?

Respuesta breve: Cyber Crucible se diseñó como un sistema completamente automatizado desde el primer día, porque los ataques de ransomware se desarrollan mucho más rápido de lo que cualquier equipo humano de seguridad puede reaccionar, y la inteligencia artificial es la única forma práctica de modelar y actuar sobre el comportamiento del ataque en tiempo real.

El problema de depender de los tiempos de respuesta humanos

Cuando Cyber Crucible se desarrolló por primera vez, alrededor de 2019, el ransomware ya superaba la capacidad de respuesta de los equipos de operaciones de seguridad. Incluso las primeras cepas de ransomware podían bloquear todos los sistemas de una organización en cuestión de minutos. Eso no dejaba una ventana realista para que una persona notara las señales de advertencia, evaluara lo que estaba ocurriendo e interviniera antes de que se produjeran daños graves. Desde entonces, los ataques solo se han acelerado; algunos informes sugieren que la red de una empresa mediana puede quedar totalmente comprometida en tan solo 90 segundos. A esa velocidad, esperar que un analista humano detecte y detenga un ataque en curso simplemente no es viable, sin importar lo capacitado o bien dotado que esté el equipo.

Por qué el modelado de comportamiento requiere IA

Detener un ataque tan rápido requiere más que alertas veloces: requiere un software capaz de reconocer patrones de comportamiento malicioso y tomar una decisión de contención de forma instantánea, sin esperar a que una persona interprete los datos. Construir manualmente ese tipo de modelado de comportamiento detallado, que cubra las numerosas formas en que un ataque podría desarrollarse, llevaría mucho más tiempo del que tiene disponible cualquier defensor. La

inteligencia artificial se convirtió en la herramienta necesaria para construir estos modelos de comportamiento con la eficiencia suficiente como para integrarlos directamente en el software de seguridad, permitiendo que las decisiones se tomen en el momento en que comienza un ataque, en lugar de después de que este haya ocurrido.

La IA como una necesidad práctica, no una tendencia

El avance hacia una defensa impulsada por IA no obedeció a seguir una tendencia de la industria: fue una respuesta práctica a un problema de tiempos que la supervisión basada en humanos no podía resolver. El enfoque de Cyber Crucible refleja la idea de utilizar la herramienta adecuada para la tarea adecuada: cuando los ataques se comprimen en cuestión de segundos, la defensa debe operar en la misma escala temporal, lo que implica una toma de decisiones automatizada y basada en IA, en lugar de una revisión manual.

https://player.vimeo.com/video/1046871333

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué los equipos de seguridad reciben miles de alertas al día y cómo pueden gestionarlas?

Respuesta breve: La sobrecarga de alertas no apareció de la noche a la mañana; se acumuló gradualmente a medida que los atacantes se volvieron más automatizados y evasivos, convirtiendo señales de advertencia antes claras en indicios débiles y ambiguos que requieren un profundo conocimiento experto para interpretarse. Cyber Crucible fue diseñado para romper este ciclo al gestionar la detección y la respuesta de forma automática, en lugar de pedir a los equipos humanos que examinen interminables señales de baja confianza.

Cómo la fatiga por alertas se convirtió en la norma

El sistema de alertas de seguridad no se degradó porque los proveedores decidieran trasladar la carga a los clientes. Ocurrió lentamente, a medida que los atacantes perfeccionaron sus técnicas para mutar y automatizarse más rápido de lo que las herramientas defensivas podían etiquetar de forma concluyente un evento como malicioso. Lo que antes era un indicador claro de compromiso se convirtió en una pista débil enterrada entre otras innumerables pistas débiles. Clasificarlas correctamente requiere un tiempo considerable por parte de analistas de nivel sénior, y a menudo lo que parece sospechoso resulta no ser más que un controlador de impresora que funciona mal. Mientras tanto, una sola alerta de baja confianza pasada por alto puede ser el único rastro visible de una intrusión grave y activa.

Por qué más alertas no significó mejor seguridad

A medida que las herramientas de detección intentaban mantener el ritmo de las amenazas en evolución, compensaron marcando cualquier cosa mínimamente inusual. Esto generó una avalancha de alertas que técnicamente cumplía con el requisito de advertir a los clientes, pero

dejaba a los equipos de seguridad sin posibilidad real de investigar cada una. El resultado natural es uno de dos escenarios: los equipos comienzan a ignorar las alertas de baja confianza —precisamente donde suelen esconderse los atacantes sofisticados— o se ven abrumados, y el trabajo crítico simplemente no se realiza, sin importar el esfuerzo o la intención.

Un punto de partida diferente

Al reconocer que las soluciones incrementales no resolverían un problema arraigado en años de complejidad acumulada, Cyber Crucible abordó el tema desde un ángulo completamente distinto. En lugar de generar más alertas para que los humanos las clasifiquen, nuestra tecnología FortressAI está diseñada para detectar y responder de forma autónoma a las amenazas de ransomware, robo de datos y robo de identidad en tiempo real. Utilizando enfoques modernos como la IA generativa, Cyber Crucible busca reducir la dependencia de la revisión manual de alertas y corregir el desequilibrio subyacente entre la automatización de los atacantes y la capacidad de los defensores.

https://player.vimeo.com/video/1186492629

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué el robo de credenciales e identidad es más peligroso que el cifrado de ransomware?

Respuesta breve: El cifrado de ransomware es el paso visible y final de un ataque, pero el daño real suele ocurrir antes, de forma inadvertida, cuando los atacantes recopilan automáticamente contraseñas, tokens de sesión, claves y monederos de criptomonedas. Cyber Crucible se enfoca en detectar y detener esa etapa temprana y oculta, en lugar de esperar al momento en que los datos quedan bloqueados.

Por qué las herramientas de seguridad suelen pasar por alto la amenaza mayor

Muchos productos de seguridad están diseñados para reaccionar ante el cifrado porque esa es la parte del ataque que una empresa realmente percibe: los sistemas dejan de funcionar, los archivos se vuelven ilegibles y las operaciones se detienen. Esta interrupción visible naturalmente atrae la mayor atención e inversión. Sin embargo, el cifrado suele ser la última acción que realiza un atacante, no la primera. Para cuando una empresa nota los efectos del ransomware, el atacante generalmente ya ha completado la parte más consecuente de la intrusión: recopilar silenciosamente datos relacionados con la identidad, como credenciales, tokens de autenticación, claves de cifrado y acceso a monederos digitales. Esta fase temprana no causa una interrupción visible, por lo que tiende a subestimarse, aunque otorga a los atacantes un acceso duradero y repetible a la red.

La silenciosa primera etapa de un ataque

Los ataques modernos son en gran medida automatizados, y la fase de robo de identidad puede completarse en solo unos segundos en toda una organización. Debido a que no hay una interrupción inmediata del negocio, esta etapa carece de la urgencia y la visibilidad que genera el cifrado del ransomware, lo que facilita que pase desapercibida. Sin embargo, es esta etapa la que otorga a los atacantes la capacidad de regresar cuando lo deseen y provocar daños adicionales, incluida la implementación de ransomware más adelante.

Cómo aborda Cyber Crucible esta brecha

Cyber Crucible está diseñado para detectar el acceso no autorizado a datos de identidad en el momento en que ocurre, en lugar de esperar a que comience el cifrado. Debido a que esta actividad ocurre de forma tan rápida y silenciosa, se ha invertido un esfuerzo de ingeniería considerable para lograr que la detección sea tanto rápida como precisa, identificando quién accede a datos de identidad sensibles sin ralentizar las operaciones cotidianas del negocio ni la actividad de los usuarios.

https://player.vimeo.com/video/1141670023

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué el ransomware se ha vuelto tan difícil de detener y de recuperar?

Respuesta breve: El ransomware ha evolucionado de un simple truco de hackeo a una operación criminal madura y con estructura empresarial que utiliza cifrado en capas y claves que desaparecen para hacer que la recuperación sea casi imposible sin pagar. Comprender cómo funcionan realmente el cifrado y el manejo de claves explica por qué las copias de seguridad, las incautaciones de las fuerzas del orden y las soluciones rápidas suelen quedarse cortas.

En qué se diferencia el ransomware de una filtración de datos

Una filtración de datos consiste en robar información en silencio y venderla más tarde, mientras que los operadores de ransomware tienen un objetivo diferente: permanecer dentro de una red el tiempo justo para causar la máxima disrupción y luego revelarse. Una vez causado el daño, ocultarse ya no les importa. Esta operación está cada vez más automatizada y se gestiona como un negocio, con procesamiento de pagos y "atención al cliente" para el descifrado incluidos, porque los atacantes necesitan una forma fiable de cobrar dinero a gran escala.

El truco de cifrado detrás del ataque

El ransomware suele basarse en dos tipos de cifrado que funcionan juntos. El cifrado simétrico rápido (como AES) bloquea los archivos reales, mientras que el cifrado asimétrico, más lento —el mismo método utilizado para proteger el tráfico web—, protege la propia clave simétrica. Esta es una técnica criptográfica bien establecida tomada de sistemas de seguridad legítimos, pero en el ransomware significa que, incluso si de alguna manera se recuperara la clave de un solo archivo, los atacantes han añadido complejidad adicional para que descifrar un archivo dependa a menudo de generar una nueva clave para el siguiente, lo que hace que los atajos sean mucho más difíciles de lo que parecen.

Por qué las opciones de recuperación siguen debilitándose

El ransomware temprano reutilizaba una única clave en muchas víctimas, lo que permitía a los defensores extraer y compartir ocasionalmente una herramienta de descifrado. Los atacantes respondieron generando claves únicas y de un solo uso que nunca se almacenan en ningún lugar recuperable. Esto elimina la opción de qu

https://player.vimeo.com/video/1065143398

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Por qué el antivirus tradicional no puede detener los ataques de ransomware de día cero y sin archivos?

Respuesta breve: Las herramientas de seguridad basadas en firmas dependen del reconocimiento de patrones de ataque conocidos, pero los atacantes modernos prueban deliberadamente sus herramientas contra esas mismas defensas antes de implementarlas, y cada vez más evitan dejar archivos detectables por completo. Esta combinación de amenazas mutadas y no reconocidas junto con técnicas que operan únicamente en memoria ha hecho que los métodos de detección tradicionales sean mucho menos confiables.

El Problema de Depender de Firmas Conocidas

Los ataques de día cero son, por definición, lo suficientemente nuevos o alterados como para quedar fuera de lo que las herramientas de seguridad existentes ya reconocen. Los proveedores han prometido durante mucho tiempo mejoras para detectar estas amenazas, pero los atacantes tienen una ventaja inherente: pueden acceder a los mismos productos comerciales de seguridad que utilizan los defensores. Antes de lanzar una campaña, los atacantes suelen probar su malware contra herramientas de detección populares, refinándolo hasta que logra evadirlas. Esto convierte la detección en un objetivo en constante movimiento en lugar de una defensa fija.

Las Técnicas Sin Archivos Socavan las Listas Blancas

Los atacantes también han dejado de depender de colocar ejecutables maliciosos evidentes en un sistema. En cambio, secuestran aplicaciones legítimas y confiables ya aprobadas por las herramientas de listas blancas de aplicaciones, ejecutando actividad maliciosa a través de procesos que el software de seguridad asume que son seguros. Cuando este enfoque sin archivos se combina con código que muta rápidamente, los ataques pueden completarse en una ventana de

tiempo muy corta —a veces en apenas media hora— mucho antes de que un equipo humano de respuesta a incidentes pueda investigar de manera realista.

Los Atacantes Borran Sus Propias Huellas

En muchos casos, dado que el ataque reside en la memoria en lugar de en el disco, los atacantes eliminan registros, evidencia e incluso sensores de seguridad antes de finalizar su operación. Esto es similar a un ladrón que desactiva las cámaras de seguridad y las alarmas antes de cometer un delito: para cuando alguien busca evidencia, la visibilidad más útil ya ha sido destruida. Esta combinación de métodos de ataque impredecibles y evidencia autoeliminada es la razón por la que Cyber Crucible ha invertido un esfuerzo significativo en construir un enfoque automatizado y escalable, diseñado para capturar los datos críticos necesarios para tomar decisiones precisas antes de que los atacantes puedan borrar el rastro, en lugar de depender del reconocimiento de amenazas después de los hechos.

https://player.vimeo.com/video/1164197533

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿Utilizarán los hackers más IA en los ataques de ransomware en 2025?

Respuesta breve: Sí. Se espera que los atacantes sigan ampliando su uso de la inteligencia artificial, especialmente los modelos de lenguaje de gran tamaño, para hacerse pasar por personas de confianza y manipular a las víctimas para que otorguen acceso o confianza.

Por qué la IA se ha convertido en la favorita de los hackers

Los resultados de búsqueda, los feeds de noticias y las conversaciones cotidianas están ahora saturados de referencias a la IA, y ese mismo entusiasmo se ha apoderado de los ciberdelincuentes. Cuando la mayoría de las personas mencionan la IA, normalmente se refieren a modelos de lenguaje de gran tamaño como los que están detrás de ChatGPT y herramientas similares que pueden imitar de manera convincente la comunicación humana. Los atacantes han reconocido que esta capacidad es extremadamente útil para la ingeniería social. En lugar de depender de correos de phishing genéricos, pueden generar mensajes, voces o conversaciones que se asemejan estrechamente a un colega, proveedor o figura de autoridad real, lo que facilita mucho ganarse la confianza de un objetivo antes de atacar.

Espere tácticas de suplantación más refinadas

La tendencia de cara a 2025 no es que los ataques impulsados por IA sean completamente nuevos, sino que se están volviendo más pulidos y con un enfoque más empresarial. De la misma manera que las empresas legítimas están implementando agentes de ventas impulsados por IA y herramientas de alcance automatizado, los atacantes están perfeccionando sus propias técnicas de suplantación basadas en IA. Esto significa mensajes más convincentes que imitan a jefes, compañeros de trabajo o socios de confianza, todos diseñados para explotar las relaciones laborales de las que la gente depende cada día. El peligro es que una conversación que se siente personal y legítima en realidad puede provenir de un sistema de IA altamente capaz creado para manipular, no para ayudar.

Qué significa esto para la defensa

A medida que estas tácticas de suplantación maduran, las organizaciones deben asumir que los ataques basados en la confianza serán cada vez más difíciles de detectar únicamente por instinto. Verificar las solicitudes a través de canales independientes, en lugar de confiar en un mensaje o llamada tal cual, se vuelve cada vez más importante. Dado que estos ataques están diseñados para eludir el juicio humano, contar con capacidades automatizadas de detección y respuesta, como las integradas en FortressAI de Cyber Crucible, proporciona una capa adicional de protección cuando la ingeniería social logra sortear las defensas de una persona.

https://player.vimeo.com/video/1046827321

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

¿El uso de Cyber Crucible reduce el presupuesto general de seguridad de una empresa?

Respuesta breve: Cyber Crucible no está diseñado para reducir directamente su presupuesto de seguridad; en cambio, libera el tiempo y los recursos de personal que antes se dedicaban a la supervisión manual y a la persecución de falsos positivos, para que pueda redirigir esa capacidad hacia brechas de seguridad que antes no podía permitirse abordar.

Por qué la automatización no significa automáticamente ahorros

Es tentador suponer que reemplazar los procesos de seguridad manuales por una herramienta automatizada como Cyber Crucible reduciría de inmediato los costos. En la práctica, no suele ser así. Muchos programas de seguridad dependen de un conjunto de herramientas dispares que requieren ajustes constantes, supervisión y revisión manual de alertas. Cuando se introduce una automatización que reduce esta carga de trabajo manual, el valor no radica principalmente en una factura más baja, sino en el tiempo y la atención recuperados que gana su equipo. Esa capacidad recuperada tiende a reinvertirse en otras prioridades de seguridad, en lugar de contabilizarse como un ahorro puro.

Dónde se manifiesta el verdadero valor

La mayoría de los líderes de TI y seguridad ya saben que su lista de tareas pendientes supera al personal y las herramientas disponibles. La limitación de personal y las restricciones técnicas hacen que muchos riesgos conocidos simplemente queden sin atender. Al reducir el esfuerzo manual dedicado a filtrar falsos positivos y a vigilar constantemente los sistemas de detección, Cyber Crucible brinda a los equipos el margen necesario para finalmente abordar esos problemas descuidados. En este sentido, el beneficio tiene que ver con la flexibilidad y el control del presupuesto, no necesariamente con un presupuesto más reducido. Los líderes pueden elegir si reducir el gasto, reasignarlo o ampliar la cobertura hacia áreas que antes estaban fuera de alcance debido a las limitaciones de recursos.

Lo que Cyber Crucible puede y no puede prometer

Cyber Crucible no puede resolver todas las restricciones presupuestarias que enfrenta una organización. Lo que sí puede hacer es dar a los líderes de seguridad un mayor control sobre cómo su gasto se traduce en protección real. Al reemplazar la supervisión manual e intensiva en mano de obra por una defensa automatizada, los equipos obtienen la capacidad de dirigir su presupuesto existente hacia el fortalecimiento de la eficacia general del programa de seguridad que han trabajado en construir, en lugar de gastarlo en mantener herramientas que exigen atención constante.

https://player.vimeo.com/video/1043470826

Ver en Vimeo · Subtítulos: English, Français, Español, العربية