¿Es Esta una Herramienta de Monitoreo Como Mis Otros Paneles de Seguridad?

La respuesta es que depende de cómo usted y su organización deseen utilizar la herramienta, pero probablemente "no".

Es importante señalar las estrategias de diseño de producto con Cyber Crucible:

1. La protección debe ser hiperautomatizada, y no debe requerir atención constante ni cuidado (atención a alertas), ni ajustes manuales (configuración) por parte de los usuarios.
2. Para los equipos de seguridad con más recursos, la telemetría valiosa debe estar disponible para ellos, para actividades avanzadas de búsqueda de amenazas, o para respaldar actividades de análisis forense y respuesta a incidentes.
3. La acción n.º 2 anterior no debe degradar de ninguna manera la protección implementada en la acción n.º 1.

El comentario más común que recibimos de la dirección de TI es que sus empleados no sabían que Cyber Crucible ya los había estado protegiendo durante semanas.

Tenemos muchos usuarios que aprovechan la herramienta en tres capacidades:

Configurar y Olvidar (Como sus Detectores de Humo)

Muchas organizaciones carecen de los recursos para tener cazadores de amenazas revisando la telemetría de Cyber Crucible (u otra herramienta), pero quieren que el riesgo de extorsión de datos "salga de su lista de preocupaciones". Eso está perfectamente bien, y la Prevención de Extorsión de Datos de Cyber Crucible está diseñada precisamente para eso.

Estos usuarios carecen de los recursos para dedicar tiempo a revisar los flujos de datos de Inyección de Procesos, Protección de Credenciales y Creación de Procesos.

Por lo tanto, encontramos que, a menos que estén respondiendo a una respuesta automatizada poco común por parte de Cyber Crucible, o estén realizando gestión de inventario, como cuando una nueva máquina necesita que se le despliegue Cyber Crucible...

...simplemente no inician sesión en el portal web de Cyber Crucible, y dejan que la automatización simplemente haga su trabajo.

¡Eso está perfectamente bien!

Búsqueda Avanzada de Amenazas + Protección Automatizada

Las capacidades de inyección de procesos, monitoreo de uso de credenciales y creación de procesos proporcionan un rico conjunto de datos, capturados mediante análisis de comportamiento a nivel de kernel, para realizar la búsqueda de amenazas.

La protección automatizada se activa una vez que comienza el robo de datos, el robo de credenciales (token, contraseña) o el cifrado de ransomware. Para todo lo demás, este es un excelente recurso.

El hallazgo más común hasta ahora son herramientas de gestión remota no gestionadas (al menos por los administradores de TI actuales) instaladas por los usuarios. Sí, a veces resultan en una protección automatizada contra la extorsión (es decir, la RMM no gestionada es utilizada por un actor malicioso), pero siempre es mejor conocer más sobre su entorno de antemano, ¡independientemente de eso!

Aquí hay un video rápido de un tipo de ataque que vimos en uso por atacantes, en múltiples entornos de clientes, que se utilizó para evadir con éxito las soluciones EDR de los clientes (no nos gusta mencionar nombres... había 3 productos en cuatro empresas).

rr-com-dll.mp4

Análisis Forense Posterior al Incidente y Remediación

Existen un par de tipos de casos de uso para los datos de Cyber Crucible.

El primero es para que una persona de seguridad en una empresa, o una persona de TI, pueda investigar la causa raíz de la suspensión de un programa. Para algunos clientes, que típicamente

instalan nuestro software y luego solo vuelven a iniciar sesión cuando hay nuevos empleados que incorporar, nunca han utilizado ninguna funcionalidad de Cyber Crucible excepto la página de Gestión de Agentes. Nos complace ayudarles a aprender sobre el análisis de causa raíz, que es sencillo e indoloro para usuarios técnicos y semitécnicos.

El segundo tipo de cliente para el análisis forense posterior al incidente son las firmas de DFIR que son convocadas para investigar un problema en un cliente, a veces a solicitud de la compañía de seguros cibernéticos, y Cyber Crucible se instala después de un incidente. (Oigan, no siempre podemos estar ahí antes que el atacante, por mucho que queramos... ¡de lo contrario, todas las empresas del mundo nos tendrían, y la extorsión sería cosa del pasado!)

La mejor manera de describir una implementación después de un ataque de extorsión es "desordenada". No porque seamos difíciles de instalar o de comenzar a proteger. ¡Todo lo contrario! En ese caso, los atacantes normalmente se han movido por el sistema, y están incrustados en los sistemas operativos, el equipo de red, Active Directory, y están operando en memoria. Múltiples máquinas terminan teniendo procesos suspendidos, y a veces los atacantes incluso intentan recuperar el control. Es un poco como tomar una medicina que al principio te hace sentir mal, pero que necesitas para llegar a mejorar.

Los clientes que ya están estresados a veces reaccionan emocionalmente ante "más" ruido, a medida que los atacantes finalmente son erradicados y derrotados. Hay mucha educación en cuanto a por qué o cómo sus pilas de seguridad existentes no encontraron a los atacantes. Al final, sin embargo, la empresa recupera el control sobre su infraestructura de TI. No se convertirán en una de las 80-90% de las empresas que son re-extorsionadas un año o dos después, en lo que llamamos "la economía de suscripción a la extorsión".

El tercer tipo de cliente que tenemos es un MSSP que, a menudo es socio de Cyber Crucible, y que está respondiendo a una protección automatizada de Cyber Crucible. Necesitan descubrir la manera en que el atacante logró un punto de apoyo temporal, y cerrar cualquier brecha en la seguridad. La buena noticia es que HIPAA u otros informes de cumplimiento normalmente reportan poca o ninguna violación de confidencialidad, debido a la velocidad de la respuesta automatizada. Muchas veces, el MSSP informa "nada que reportar", lo cual hace felices a todos los involucrados. Bueno, excepto al criminal.

Revision #1
Created 2026-07-24 01:45:43 UTC by Dennis Underwood
Updated 2026-07-24 01:45:44 UTC by Dennis Underwood