Soluciones por Industria

Cómo se aplica la prevención autónoma a sectores específicos: salud, manufactura y OT, servicios financieros, gobierno, educación, marítimo y proveedores de servicios gestionados.

¿Cómo protege Cyber Crucible los entornos de manufactura, OT e ICS?

Respuesta breve: Se ejecuta completamente en el endpoint sin dependencia de la nube, por lo que protege la tecnología operativa y los sistemas de control industrial que están sin conexión, aislados (air-gapped) o con conectividad intermitente — y suspende únicamente el proceso malicioso, de modo que la producción continúa.

Por qué las herramientas convencionales tienen dificultades aquí

Los entornos OT e ICS no pueden tolerar ni una comunicación de ida y vuelta con la nube ni un bloqueo total de la red. Muchos están deliberadamente desconectados. Los modelos de seguridad que asumen conectividad constante y un SOC remoto simplemente no se aplican.

Qué cambia

- **100 % capaz de operar sin conexión** — protección completa sin necesidad de señal, preparado para entornos air-gapped.
- **Sin bloqueos** — los procesos maliciosos se suspenden en memoria mientras la producción continúa.
- **Un solo agente en todo el entorno** — el mismo agente ligero protege los PLC en la planta de producción, los vehículos en una red logística y los buques en el mar, sin necesidad de un analista en el circuito ni suposiciones sobre conectividad.

¿Cómo protege Cyber Crucible a las empresas de servicios financieros?

Respuesta breve: Detiene el robo de información (infostealers) y el robo de tokens de sesión a nivel de kernel, antes de que comience la exfiltración, y analiza todo de forma local para que las claves y los tokens nunca tengan que subirse a una nube de terceros.

La amenaza que realmente enfrentan las empresas financieras

Los ataques hiperautomatizados de "entrar y arrasar" (smash and grab) se dirigen a tokens de sesión y claves de API. Estos pasan de la infiltración a la autoeliminación en segundos, más rápido de lo que tarda una alerta en la nube en salir del edificio. Un token de sesión robado a menudo elude por completo las contraseñas y la MFA, dándole al atacante una forma aparentemente legítima de volver a entrar en cualquier momento.

El caso documentado

Una importante empresa de servicios financieros utilizaba tres EDR líderes de la industria y un MSSP subcontratado entre los 50 principales. Se implementó Cyber Crucible para encontrar el punto ciego. En un plazo de 60 días, había interceptado de forma autónoma casi 10,000 procesos maliciosos, el 98% de ellos en el conjunto de servidores Microsoft SQL altamente privilegiados de la empresa, sin ninguna alerta por parte de la infraestructura heredada.

La causa raíz se remontó a una credencial de monitoreo remoto probablemente comprometida. Meses después, la industria reportó una ola global de ransomware que instalaba puertas traseras en servidores SQL en todo el mundo. El sector financiero sufrió graves brechas de seguridad. Este cliente nunca fue una víctima.

¿Cómo respalda Cyber Crucible a los entornos gubernamentales y de alta seguridad?

Respuesta breve: Mediante la soberanía total de los datos — instalación completamente local (on-premises) en racks físicamente protegidos, operación en redes aisladas (air-gapped) y arquitectura multiinquilino — sin nube pública, sin SOC de terceros y sin intercambio de datos.

Soberanía por diseño arquitectónico

Para las organizaciones que requieren un control absoluto, no es necesario que nada salga del entorno. No existen plataformas de terceros en la ruta, ni acceso externo, ni análisis de sus datos alojado por el proveedor.

Esto es importante porque muchos proveedores suben datos de identidad sensibles — claves privadas, tokens de sesión — a sus equipos de SOC alojados. Ese almacenamiento centralizado es un único punto de fallo y un objetivo de alto valor para atacantes patrocinados por estados, y puede ser accedido mediante compulsión legal sin su conocimiento.

Silencioso por defecto

Las amenazas se neutralizan de forma silenciosa a nivel del kernel. Solo usted sabe que se intentó un ataque, y si no se accedió a ningún dato, normalmente no se generan alertas externas ni se requieren divulgaciones.

Multiinquilino

La arquitectura admite implementaciones multiinquilino, lo cual resulta adecuado para gestionar múltiples departamentos o agencias desde una única instancia local segura.

¿Puede Cyber Crucible proteger buques y operaciones remotas o desconectadas?

Respuesta breve: Sí, y lo ha demostrado. En un despliegue marítimo, Cyber Crucible funcionó de forma autónoma durante travesías de varios días sin personal de TI a bordo, adaptándose a enlaces satelitales de bajo ancho de banda y a largos periodos de desconexión, mientras protegía todo, desde terminales de pasajeros hasta controles marítimos de misión crítica.

Lo que demostró el despliegue

- **Respuesta autónoma** sin equipo de TI presente durante días seguidos.
- **Funcionamiento consciente del enlace satelital** a través de conexiones intermitentes, de bajo ancho de banda e interrumpidas por el clima.
- **Retención forense** — registros detallados preservados durante la desconexión para su análisis posterior a la travesía.
- **Resiliencia ante ataques** — se mantuvo firme cuando los adversarios intentaron desactivarlo o degradar su rendimiento.

La parte inusual

Los registros revelaron actividad compatible con la participación de un actor estatal, y el objetivo fue selectivo: solo se vieron afectados los buques que operaban en aguas internacionales, mientras que los buques turísticos nacionales no fueron alcanzados.

Cuando los intentos convencionales de intrusión fallaron, los adversarios escalaron: secuestraron las credenciales de inicio de sesión de Windows y luego llegaron a configuraciones a nivel de BIOS para bloquear los sistemas antes del arranque. Incluso con los sistemas detenidos antes de que el sistema operativo pudiera cargarse, el despliegue continuó defendiendo la línea donde las pilas de seguridad tradicionales ya habían fallado.

¿Por qué los MSP y revendedores se asocian con Cyber Crucible?

Respuesta breve: Porque la prevención autónoma permite que un socio conserve el margen, la relación con el cliente y el SLA, en lugar de revender un SOC alojado por el proveedor y asumir la culpa cuando ese SOC no detecta un ataque a velocidad de máquina.

La trampa de revender detección

La industria empujó a los socios a revender servicios de MDR y SOC alojados por proveedores. Cuando el monitoreo impulsado por humanos inevitablemente pasa por alto un ataque automatizado, el proveedor pasa por alto la brecha, y el cliente no despide al proveedor. Despiden al socio.

Qué cambia a nivel operativo

- Las amenazas se neutralizan de inmediato, antes de que los analistas reciban una alerta.
- El volumen de alertas se reduce drásticamente respecto a las más de 100 por endpoint al día que provocan fatiga de alertas.
- No hay ajuste de reglas YARA ni búsqueda manual de amenazas.
- Los socios capturan el flujo de ingresos en lugar de conformarse con comisiones de proveedor.

Y en cuanto al riesgo

Un socio cuya oferta de seguridad previene ataques en lugar de documentarlos mantiene una conversación fundamentalmente distinta con los clientes sobre resultados y responsabilidad.

Sufrimos una brecha recientemente. ¿Se puede desplegar Cyber Crucible en un entorno que ya podría estar comprometido?

Respuesta breve: Sí. Cyber Crucible evalúa lo que están haciendo los programas en tiempo real, en lugar de buscar archivos que ya se sabe que son maliciosos, por lo que comienza a detener el comportamiento malicioso desde el momento de su despliegue, incluso frente a un atacante que ya cuenta con un punto de apoyo.

Por qué un compromiso previo no lo deja ciego

Dado que la prevención se basa en la intención conductual a nivel del kernel, un atacante que ya está presente en el entorno de todos modos tiene que *actuar*: acceder a datos de identidad, inyectarse en procesos, iniciar el cifrado o mover datos. Esas acciones son precisamente las que activan la intercepción.

Así fue como el despliegue en el sector de servicios financieros reveló una intrusión activa y en curso sobre la que la pila de seguridad existente nunca había generado una alerta. Cyber Crucible no se implementó para investigar una brecha ya conocida; se desplegó para buscar un punto ciego, y encontró casi 10,000 procesos maliciosos ya en marcha.

Qué esperar

Desplegar la solución en un entorno comprometido a menudo genera actividad de intercepción inmediata y de gran volumen. Eso es la herramienta funcionando tal como está diseñada, y con frecuencia constituye la primera evidencia sólida que tiene una organización de que algo ya estaba en curso.