CHANNEL News
Fecha: 28/08/2024 Audiencia: 18.000 Sección: ACTUALIDAD
Vpe: $572.360 Tirada: 6.000 Frecuencia: MENSUAL
Vpe pág: $783.027 Difusión: 6.000
Vpe portada: $783.027 Ocupación: 73,1%

Aprovechando procesos y tecnologías avanzadas para la detección y mitigación acelerada de brechas

Los CISO pueden aprovechar procesos avanzados y tecnologías de última generación para acelerar la detección y mitigación de brechas, fortaleciendo así la seguridad empresarial en un entorno digital cada vez más desafiante. En esta columna, exploramos las herramientas y procedimientos para hacerlo.

Por Gonzalo García,
Vicepresidente de Ventas de Fortinet para Sudamérica.

En el panorama digital actual, las empresas se encuentran con un alto nivel de amenazas cibernéticas. Estas amenazas se están volviendo progresivamente sofisticadas y dirigidas, desafiando a las organizaciones a fortificar su postura de seguridad. Uno de los obstáculos significativos es la prolongada duración que toma detectar y mitigar brechas, con un promedio de 280 días para la detección y 90 días para la contención, según la retroalimentación que recibimos del mercado. Esta latencia crea una ventana sustancial para que los atacantes roben datos, inflijan daño e interrumpan operaciones.

Para las empresas, cerrar este gran agujero es primordial. La introducción de nuevos procesos y tecnologías, diseñadas para mejorar la visibilidad en el tráfico de la red, analizar comportamientos sospechosos y automatizar la respuesta a incidentes, es imperativa. Entre las plataformas clave para lograr estos objetivos se encuentran las herramientas de Operaciones de Seguridad (SecOps) que asisten a las organizaciones en automatizar y optimizar sus operaciones de seguridad, reduciendo así el tiempo para detectar y contener brechas.

Fortaleciendo la seguridad de la empresa

Las herramientas SecOps más populares incluyen Gestión de Información y Eventos de Seguridad (SIEM), Orquestación de Seguridad, Automatización y Respuesta (SOAR), Análisis de Comportamiento de Usuario y Entidad (UEBA) y Análisis de Tráfico de Red (NTA). Estas soluciones pueden acelerar significativamente el proceso de identificación, priorización y respuesta ante amenazas.

Pero ¿cuáles son las medidas adicionales que un CISO debiera considerar para fortalecer la resiliencia cibernética de la empresa?

Integración de análisis avanzado y machine learning: utilizar algoritmos de machine learning para analizar conjuntos colosales de datos para identificar rápidamente patrones anómalos es crucial. Los análisis avanzados pueden fortalecer significativamente la capacidad de las herramientas SIEM y UEBA, mejorando así la detección de amenazas y la respuesta.

Adopción de la arquitectura de confianza cero (ZTA): el mantra de "nunca confiar, siempre verificar" sustenta la ZTA, minimizando la superficie de ataque y asegurando que los recursos de la red sean accesibles solo en base a la necesidad, un paso proactivo hacia una ciberseguridad mejorada.

Caza proactiva de amenazas: complementar las medidas de seguridad reactivas con la caza proactiva de amenazas puede descubrir indicadores de compromiso temprano. Este enfoque proactivo enriquece las funcionalidades de las herramientas SecOps, conduciendo a una postura de seguridad más robusta.

Tecnologías de detección y respuesta en el endpoint (EDR): asegurar un análisis comprensivo y una visibilidad en el

nivel de endpoint es vital. Las tecnologías EDR sirven como una extensión del ecosistema de seguridad, asistiendo en la detección, investigación y mitigación de actividades sospechosas en los endpoints de la red.

Incorporación de plataformas de inteligencia de amenazas: obtener perspectivas de varias fuentes de datos para proporcionar inteligencia accionable sobre amenazas emergentes es esencial. Esta medida proporciona contexto alrededor de actividades sospechosas, ayudando en la priorización y mitigación rápida de amenazas.

Plataformas de seguridad nativas de la nube: con la adopción de la nube en aumento, tener una plataforma de seguridad nativa de la nube asegurará una postura de seguridad coherente en los entornos de la nube y en los locales.

Programas regulares de capacitación y concientización: el error humano es un contribuyente significativo a las brechas de seguridad. La capacitación regular asegura que el personal permanezca como una fuerte primera línea de defensa contra el phishing y otros ataques dirigidos a los usuarios.

Monitoreo continuo y evaluación: una revisión regular de los controles y procesos de seguridad, junto con un monitoreo continuo, asegura la resiliencia del sistema ante las amenazas en evolución.

A la hora de planificar las inversiones, adoptar un modelo de consumo híbrido es una estrategia viable y robusta. Este modelo permite al CISO aprovechar lo mejor de ambos mundos: la tecnología propia de la organización y la seguridad como servicio (Security as a Service, SECaaS).

Las ventajas de un modelo de consumo híbrido

A la hora de planificar las inversiones, adoptar un modelo de consumo híbrido es una estrategia viable y robusta. Este modelo permite al CISO aprovechar lo mejor de ambos mundos: la tecnología propia de la organización y la seguridad como servicio (Security as a Service, SECaaS). Mediante el despliegue de tecnologías propias, el CISO puede personalizar las soluciones de seguridad para satisfacer las necesidades específicas de la organización, mientras mantiene un control directo sobre los sistemas críticos. Por otro lado, al incorporar SECaaS, el CISO puede acceder a asesoramiento experto y a tecnologías avanzadas sin la necesidad de una gran inversión inicial, además de beneficiarse de las actualizaciones continuas y el soporte especializado que proveen los proveedores de servicios de seguridad.

En conclusión, es esencial para los CISO combinar estos procesos avanzados, tecnologías y herramientas SecOps para crear un mecanismo de defensa avanzado e integral contra las ciberamenazas. Este enfoque híbrido no sólo mitigará los riesgos asociados con las brechas de datos, sino que también reducirá significativamente el tiempo que toma detectar y responder a los ciberataques, fomentando así una postura de seguridad empresarial robusta, resiliente y confiable. /ChN