banyax

M/ETI

Managed External Threat Intelligence

Powered by Cyberint

OBSERVA Y PROTEGE A TU ORGANIZACIÓN MÁS ALLÁ DE TU PERÍMETRO DE DEFENSA CIBERNÉTICA.

Se enfoca en descubrir riesgos ocultos o factores externos como filtraciones de terceros, vertederos de datos, abuso de dominios y suplantación de identidad de ejecutivos en la Deep y Dark Web, permitiendo tomar acciones rápidas para proteger tu información sensible.

MONITOREO DE LA SUPERFICIE DE ATAQUE

Identificación y evaluación de todos los posibles puntos de entrada en los sistemas de una organización que podrían ser explotados por atacantes, con el objetivo de reducir vulnerabilidades y mejorar la seguridad.

INTELIGENCIA DE AMENAZAS

Recopilación y análisis de información sobre amenazas de seguridad potenciales y activas para ayudar a las organizaciones a anticipar, prevenir y responder a ciberataques.

DETECCIÓN DE AMENAZAS EXTERNAS

Identificación y monitoreo de amenazas de seguridad provenientes del exterior de una organización para prevenir o mitigar posibles daños.

banyax Quest

Plataforma Banyax Quest™

Transparencia y comunicación son básicas para responder rápido a las amenazas cibernéticas. Banyax Quest™ es la plataforma colaborativa donde su equipo de trabajo podrá ver exactamente lo mismo que nuestros analistas e interactuar en tiempo real para contener las amenazas. En esta plataforma podrá encontrar respuestas al qué, quién, cómo, cuándo y dónde está sucediendo una amenaza, así como, que hacer para contenerla y como solucionar la causa raíz.

La visibilidad es clave en ciberseguridad

- Plataforma de Inteligencia de Amenazas.

24×7×365 Real-Time Cyber Defense Services
Monterrey, México | CDMX, México | Dallas, Texas
info@banyax.com
www.banyax.com
banyax

FUNCIONALIDADES

banyax

Protección Proactiva de Marca e Imagen

Búsqueda, monitoreo y detección temprana de la presencia de la marca e imagen en internet, con el fin de encontrar un uso no autorizado, sitios web falsos o perfiles engañosos que puedan hacerse pasar por la marca o imagen con fines fraudulentos.

Escaneo de Foros Encubiertos y Plataformas para Detectar Conversaciones y Abuso de Marca

Búsqueda en una amplia variedad de foros en línea, redes sociales y otros sitios web, identificando conversaciones, comentarios, publicaciones y reseñas donde se mencione la marca o se haga alusión a la imagen de la organización. Analizando dichas conversaciones para identificar posibles abusos de marca, falsificaciones, difamaciones o impersonificaciones que puedan confundir a empleados o consumidores.

Protección contra la Suplantación de Identidad de Ejecutivos Clave

Búsqueda en redes sociales, foros, sitios web y Deep web de cualquier mención del nombre del ejecutivo, su cargo y la marca, con el fin de identificar perfiles apócrifos con la intención de suplantar, defraudar o dañar la reputación del ejecutivo o la organización difundiendo información falsa o difamatoria.

Detección y Protección contra el Abuso de Dominios e Intentos de Suplantación (sitios web falsos)

Evaluación y monitoreo de la web en busca de nuevos dominios que contengan el nombre de la marca, sus variaciones o palabras clave que faciliten su asociación, con la intención de suplantar y defraudar (robo de información personal o financiera, venta desleal o daño a la reputación de la marca).

Notificaciones y Dashboards

Se proporciona un panel de control centralizado y notificaciones por correo electrónico en tiempo real, lo que permite acceder rápidamente a las alertas y al análisis de incidentes, garantizando que ninguna amenaza pase desapercibida.

Derribos de Contenido Malicioso

Con herramientas avanzadas y un equipo de expertos, gestionamos todo el proceso, para proteger contra las amenazas digitales eliminando contenidos maliciosos como sitios de phishing, cuentas falsas en redes sociales y aplicaciones fraudulentas.

Notificación y Monitoreo de Credenciales Expuestas en la Dark Web

Búsqueda en redes sociales, foros, sitios web y Deep Web de cualquier mención en la que se comercien datos robados, con el fin de hallar las credenciales (combinaciones de correo electrónico y contraseña) de empleados o clientes relacionados con la organización o la marca.

Identificación de Código Fuente de Aplicaciones Expuesto a través de un Identificador Único

Monitoreo de identificadores únicos de código y APIs para la detección de código fuente expuesto en la web, con el fin de evitar suplantación con la intención de defraudar o engañar a los empleados o consumidores.

Identificación de Equipos de Cómputo Iinfectados a través de la Búsqueda de Logs de Infostealers y Otros Tipos de Malware

Mediante monitoreo y búsqueda especializada de actividad sospechosa en diversos feeds de inteligencia de amenazas y el escaneo proactivo de eventos generados por Infostealers y otros tipos de malware permiten identificar, mediante indicadores de compromiso (IoCs), las actividades de Botnet, lo que proporciona una defensa temprana contra posibles amenazas de red y ataques cibernéticos.

Identificación de Herramientas de Reconocimiento, Scanner de Vulnerabilidades y/ Ransomware buscando atacar a la Organización

A través del monitoreo de la superficie de ataque expuesta de la organización, se identifican las herramientas de los atacantes y/o terceros que intentan afectar al sistema mediante escaneos de vulnerabilidades, reconocimiento de tecnologías e infecciones de malware.

FUNCIONALIDADES

banyax

Inteligencia y Consejos de Seguridad

Ofrecemos informes mensuales de ciberinteligencia que detallan las vulnerabilidades identificadas, los actores de amenazas y las tácticas, técnicas y procedimientos (TTPs) predominantes en la dark web. Esta información nos permite anticiparnos a las amenazas y adoptar medidas proactivas para proteger a la organización.

Identificación de Configuraciones Erróneas en Dominios de la Compañía que Pudieran Derivar en Incidentes

Monitoreo proactivo de la superficie de ataque dentro del alcance público de la organización, que detecta desviaciones en las configuraciones al compararlas con las bases de datos de CVE conocidas y recomienda acciones de remediación para fortalecer la postura de ciberseguridad.

Identificación de Servidores de Correo en Listas Negras

Consultas periódicas en bases de datos de servidores de correo en lista negra en busca de coincidencias entre las direcciones IP o los dominios de los servidores de correo de la organización que puedan indicar un posible compromiso del sistema, como el envío de spam desde servidores comprometidos.

Identificación de Interfaces Web para Empleados y/o Clientes Expuestas con Problemas de Seguridad

Monitoreo de la web en busca de interfaces de acceso que coincidan con el dominio, la IP o la marca de la organización dentro del alcance, que cuenten con formularios de acceso vulnerables y/o expuestos a problemas de ciberseguridad.

Monitoreo de Almacenamientos Externo en la Nube

Búsqueda proactiva de exfiltraciones de información relacionados con almacenamientos en nube externos al dominio principal de la organización.

Identificación de Vulnerabilidades en Puertos y Servicios del Dominio Monitoreado

Busca vulnerabilidades existentes en puertos y servicios del dominio monitoreado, comparándolas con vulnerabilidades conocidas comúnmente explotadas por actores de amenazas, con capacidad para identificar y analizar las tecnologías expuestas, su gravedad según el riesgo que representan para los sistemas, compartiendo recomendaciones para robustecer la postura de ciberseguridad de la organización.