banyax

M/XDR

Managed Extended Detection & Response

NO PUEDES PELEAR CONTRA LO QUE NO PUEDES VER.

Usamos Inteligencia Artificial para detectar, notificar, y mitigar comportamientos anómalos de tus usuarios y sistemas que puedan representar una amenaza cibernética.

INGESTIÓN

Recolección de eventos en tiempo real desde cualquier punto de su organización.

DETECCIÓN E INVESTIGACIÓN DE AMENAZAS

Investigación detallada y detección de ciber anomalías, en tiempo real, para detectar rápidamente intrusiones mediante Inteligencia Artificial.

RESPUESTA

Contención oportuna ante amenazas.

banyax Quest

Active Member of XDR Alliance MEMBER

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.

Visibilidad el nombre del juego en Ciberseguridad.

- Plataforma de próxima generación de gestión de eventos e información de seguridad (SIEM) y (XDR) detección y respuesta ampliadas.
- CDC (Centro de Ciberdefensa).

FUNCIONALIDADES

Todo incluido (as a Service)
Servicio llave en mano: no se preocupe por instalaciones, compra de hardware, software, rotación de personal, actualizaciones y operación.

Cobertura 7×24×365
Contamos con personal dedicado y certificado al monitoreo y detección de amenazas cibernéticas en tiempo real en formato 7×24×365, nuestros agentes no se dedican a otras actividades que no sea el monitorear la seguridad de nuestros clientes.

Fuentes ilimitadas de datos
Se incluye cualquier fuente emisora de logs de seguridad que pueda ser alcanzable por la red.

Enriquecimiento de datos con contexto de negocio
Enriquecemos los datos con información de contexto enfocada a procesos de negocio, casos de uso específicos y peculiaridades tecnológicas específicas de su organización.

Meses de retención de datos en Data Lake
La información de logs en crudo se encuentra disponible en línea para búsquedas o investigaciones en data lake por la cantidad de tiempo seleccionada según las necesidades de su negocio.

Visibilidad completa de alertas
Centralizamos las alertas de tus dispositivos de seguridad en una sola vista por categorías y criticidad.

Cacería de amenazas (Threat Hunting)
Búsqueda iterativa y proactiva a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.

Detección avanzada de amenazas basado en comportamiento
UEBA (User and Entity Behavior Analitycs) se utiliza para la detección de amenazas, tanto para la detección de fallos externos como para la identificación de intrusos. Desde una perspectiva del comportamiento, aprende lo que las personas y las entidades hacen sobre una base "normal".

Reglas de correlación
Ligamos eventos de diferentes sistemas y sus datos relacionados que representan incidentes de seguridad reales, amenazas, vulnerabilidades o hallazgos forenses.

Casos de uso orientados a seguridad
Proporcionamos información del comportamiento de los usuarios y entidades que conforman la red corporativa, brindando monitoreo, detección y alertamiento de anomalías.

Casos de uso orientados a prevención de fraude
Le ayudamos a la creación de analíticos enfocados a prevenir y monitorear las desviaciones de comportamiento de sus usuarios y tecnologías con el objetivo de prevenir fraudes.

Casos de uso orientados a negocio
Organizamos sesiones con sus áreas (compras, administración, logística, auditoria, procesos, etc.) para el entendimiento de sus necesidades y/o preocupaciones a monitorear y desarrollamos analíticos bajo este enfoque, creando soluciones a la medida para cada uno de ellos.

Meses de línea de tiempo en Analítico
La información de metadatos se encuentra disponible en línea para búsquedas o investigaciones en analítico por la cantidad de tiempo seleccionada según las necesidades de su negocio.

Escuadrón especializado
Personal entrenado como "Certified SOC Analyst" y alineado a los procesos de "Mitre Att&ck" operando 7×24×365, orquestando la pronta detección y resolución de las amenazas cibernéticas.

“Bots” especializados
Nuestros bots, Bany & Yax, automatizan procesos de detección, investigación y reporteo, para que nuestro escuadrón humano sea más productivo. También se les puede programar para que realicen actividades específicas que cada cliente requiera.

FUNCIONALIDADES

Portal UEBA (Analítico) y Data Lake
Le brindamos acceso permanente para realizar las consultas en las consolas que utilizamos para realizar el monitoreo, obteniendo una mejor colaboración entre cliente-banyax y transparencia de nuestro servicio.

Portal Banyax Quest™ - Security
Portal personalizado con información acerca de métricas, incidentes, seguimiento y gráficas de seguridad. En esta sección se puede consultar la información de los casos generados a través del CDC (Cyber Defense Center) de Banyax “On Demand”, así mismo, las vulnerabilidades más significativas de su infraestructura descritas por sus tecnologías de seguridad ingestadas, métricas de ingesta y almacenamiento de datos.

Portal Banyax Quest™ - Productivity
Portal personalizado con información de nuestros clientes que brinda un dashboard interactivo en el cual se pueden consultar métricas respecto la productividad diaria de cada empleado, por ejemplo: horario de Login-Logout, páginas web visitadas, envío de correo a dominios externos, aplicaciones más utilizadas e interacción con sus suites de productividad (G-Suite, Office 365, etc.).

Acceso al cliente a todas las herramientas y dashboards
Nuestro modelo de operación "Clear Box" permite a nuestros clientes el acceso a todas las herramientas operadas por nuestro personal, garantizando la transparencia en la operación y servicio.

SLA
Niveles de servicio adecuados para cada vertical de negocio y alineados con los requerimientos de su organización.

Orquestación de respuesta a incidentes
Nos encargamos de coordinar el seguimiento a los tickets en todo el proceso, desde su notificación, escalación, mitigación y documentación

Automatización de respuesta a incidentes
Mitigación automática de incidentes sobre casos de uso programados, la cual apoya a reducir la carga de trabajo para los equipos de IT de nuestros clientes, al automatizar con "playbooks" la respuesta ante amenazas cibernéticas.

Extended CISO as a Service
Consultoría activa y constante en la cual se emiten recomendaciones y planes de mejora continua con el fin de aumentar su nivel de madurez en ciberseguridad.

Apoyo en cumplimiento de auditorías y regulaciones
Proporcionamos la evidencia necesaria en los rubros de detección, investigación y respuesta de incidentes cibernéticos requeridos por estos marcos de referencia.

Red Team
Equipo de hackers éticos encargados de probar las estrategias de defensa y monitoreo de nuestros clientes, encontrando áreas de oportunidad y puntos de mejora.

Client Services Manager
Profesional encargado de maximizar la experiencia del servicio contratado, asegurándose de la correcta implementación y ejecución de todas las funcionalidades.

Tus logs están tratando de decirte algo...