DATA SHEET Servicio Cyberdefense

Solución

Cyberdefense es una plataforma web de seguimiento y patrullaje digital que fortalece las estrategias de seguridad de las organizaciones contra la actividad maliciosa externa a su perímetro de ciberseguridad, mediante la inteligencia de amenazas cibernéticas, también conocida como Cyber Threat Intelligence, que de manera general, es el conocimiento basado en el contexto del adversario (APT, crimen organizado, ataques hacia determinado sector, hacktivistas, por mencionar algunos), que incluye información de actores maliciosos, descripción de los mismos, indicadores de compromiso y recomendaciones orientadas en acción sobre una amenaza, peligro existente o emergente para los activos. **La inteligencia de amenazas realizada por MNEMO es el producto resultante del análisis de la información disponible (no siempre pública) a un proceso conocido como "El Ciclo de Inteligencia" y apegado a diferentes metodologías de CTI como modelo diamante, Cyber Kill Chain y Mitre ATT&CK principalmente. Este proceso permite generar información de valor las organizaciones y útil para la toma de decisiones en distintos niveles operativos.**

La inteligencia de amenazas permite generar diversos tipos de entregables, considerando las categorías de estratégicos, tácticos y operacionales, los cuales que pueden ser aprovechados por los distintos equipos de seguridad y a todos los niveles de las organizaciones. Los informes estratégicos contienen información de alto nivel, con poco detalle técnico, que abarca aspectos como el impacto financiero, las tendencias de ataque y las áreas que pueden afectar las decisiones de negocio, mientras que los documentos tácticos contienen información sobre cómo los actores maliciosos realizan sus ataques. Finalmente, los documentos técnicos contienen indicadores de compromiso que pueden ayudar al personal de SOC, Blue Team, IR y al equipo de TI.

Los productos de inteligencia de amenazas hacen uso y generan varios insumos que pueden ayudar a identificar actividad maliciosa en las organizaciones, entre estos se encuentran:
IOC. Indicadores de Compromiso que definen las características y datos técnicos de una amenaza por medio de las evidencias existentes en un equipo comprometido, algunos ejemplos de estos indicadores incluyen:

- oValores hash
- oDirecciones IP / Puertos
- oNombres de dominio
- oURLs
- oArtefactos (Nombres de archivos, DLLs, Llaves de registro, direcciones de correo electrónico)
- oHerramientas
- oTTP

A partir de los IOCs es posible realizar un intercambio sencillo y práctico de información con otros grupos de ciberseguridad e implementarlos en herramientas de detección y prevención de amenazas.
TTP
Las Tácticas, Técnicas y Procedimientos (TTPs) describen un enfoque de análisis mucho más completo para comprender la operación de las Amenazas Persistentes Avanzadas (APTs), pueden utilizarse para perfilar a un determinado actor de amenazas. La táctica es el mayor nivel de descripción en este contexto, mientras que la técnica ofrece una descripción detallada del comportamiento del atacante en el contexto de una táctica y los procedimientos una descripción aún más detallada y de menor nivel en el contexto de una técnica.
APT
Las amenazas persistentes avanzadas (APTs) hacen referencia a los adversarios que poseen sofisticados niveles de experiencia y recursos significativos los cuales les permiten crear oportunidades para alcanzar sus objetivos mediante el uso de distintos vectores de ataque. Estos objetivos generalmente incluyen establecer y expandir puntos de apoyo en la infraestructura tecnológica de las víctimas para realizar distintos tipos de actividades maliciosas como podrían ser la exfiltración de información, la modificación de archivos, la instalación de malware, la minería de criptomonedas o el espionaje.
Algunas de las características principales de este tipo de amenazas incluyen el acecho de sus objetivos durante largos periodos de tiempo, su adaptabilidad a las defensas de sus víctimas y la determinación para mantener un nivel de interacción necesario para alcanzar sus objetivos.

DATA SHEET Servicio Cyberdefense

Beneficios

MNEMO ofrece un conjunto de servicios de inteligencia de amenazas externas con base en el monitoreo especializado del CERT de MNEMO, el cual cuenta con acceso a distintas fuentes de información, tanto públicas como privadas, que le ofrecen visibilidad en Internet, Dark y Deep Web, así como su participación en una red de colaboración global al ser un miembro de FIRST (una red de colaboración entre CERTs/ CSIRTs de todo el mundo).

Con MNEMO Cyberdefense, una organización amplía su visibilidad de las amenazas cibernéticas que pueden derivar en un riesgo y representar un impacto negativo en sus procesos de negocio a través de la identificación u obtención de:

Información de interés con base en los criterios de búsqueda definidos por cada organización, que pueden estar relacionados principalmente con:

- Direcciones IP homologadas.
- Nombres de dominio.

Productos, servicios, ejecutivos, tipos particulares de publicaciones, entre otros. Vulnerabilidades de infraestructura de TI expuesta a Internet.

- Principales protocolos vulnerables.
- Fallas en las implementaciones de certificados de cifrado.
- Problemas comunes de configuración en sitios web.
- Uso de protocolos vulnerables.
- Sistemas con fallas de seguridad a raíz de configuraciones.

Incidentes.

- Phishing.
- Suplantación de identidad, dominios, certificados, redes sociales.
- Productos ilegales.
- Credenciales comprometidas.
- Bases de datos expuestas.
- Venta de información.
- Amenazas internas.
- Malware.
- Entre otros.

Avisos de seguridad.

- Vulnerabilidades críticas.
- Campañas de ataque emergentes.
- Vulnerabilidades aprovechadas por los actores maliciosos.
- Información referente a muestras de malware.

Información respecto a campañas de ataque.

- IOC.
- TTP.
- APT.
- Amenazas cibernéticas sectoriales.

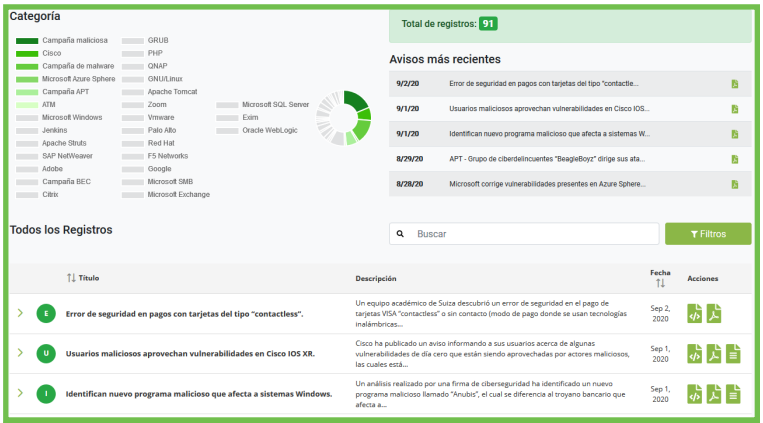
Acceso a plataforma MISP (Malware Information Sharing Platform)

contodas las fuentes de información de IOC de MNEMO conectadas(España, Colombia y México), TIP Kaspersky y FIRST principalmente, los cuales se pueden exportar en los principales formatos utilizados.

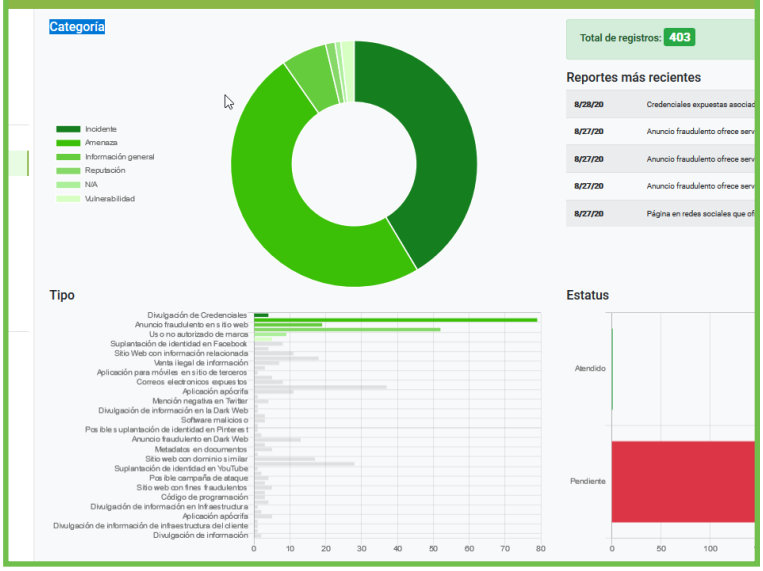
Boletines mensuales de la inteligencia relevante a nivel mundial y local.

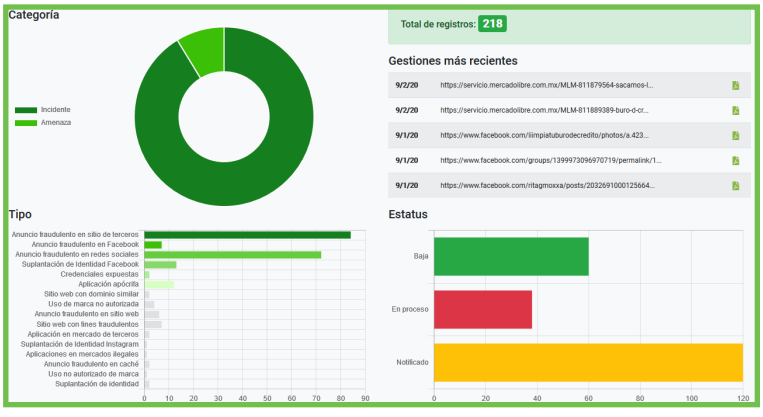
- Boletín de ciberseguridad; reportes periódicos sobre nuevas amenazas, nuevas variantes de malware, instituciones comprometidas, casos de estudio, tendencias, entre otros.

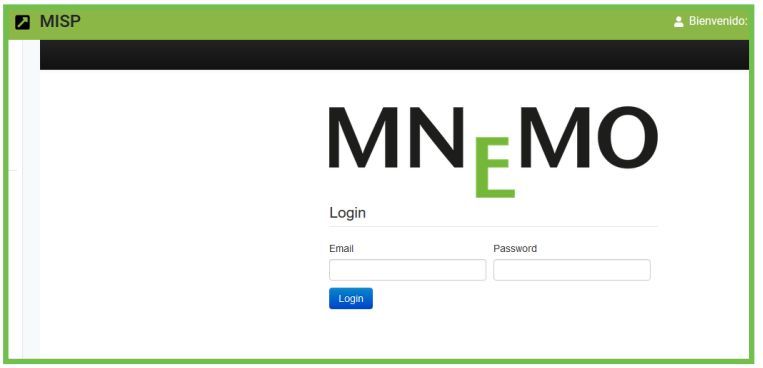
- Boletín financiero; reportes periódicos de amenazas y



VIGILANCIA DIGITAL



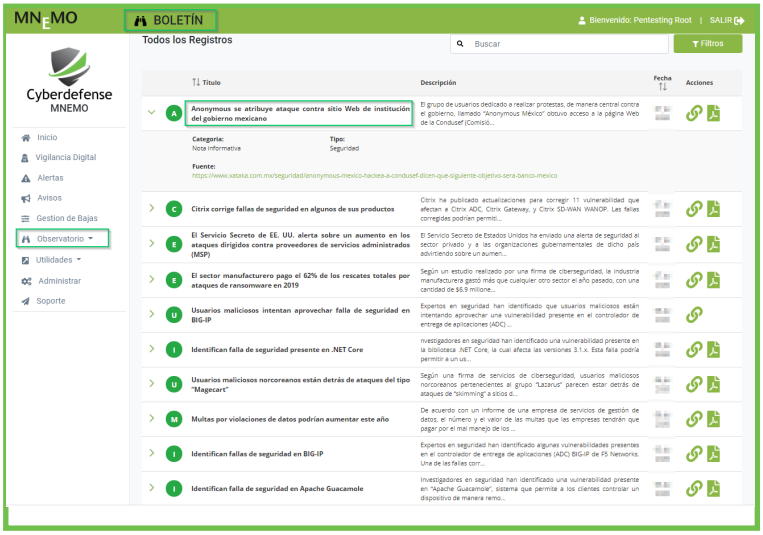




DATA SHEET Servicio Cyberdefense

soluciones de ciberseguridad con un enfoque dirigido al sector financiero.

- Boletín Dark Web; reportes generados de la vigilancia digital en Dark Web para la identificación de amenazas y detección de productos y servicios que se comercializan de forma no autorizada.



Boletines periódicos con fines de concientización.

Contiene información respecto a los casos más representativos identificados y atendidos por Mnemo en el mes previo a su liberación, considerando tema de interés del mes, las vulnerabilidades de TI críticas aprovechadas, Inteligencia de amenazas e información de concientización de ciberseguridad general.

Reportes de C&C con actividad en México.

Información respecto a las principales direcciones IP empleadas como equipos de Comando y Control (C&C), relacionado con redes botnet maliciosas.

Por último, la gestión de baja de actividad maliciosa en Internet.

Sección del servicio enfocado en la gestión de baja de contenido malicioso, considerando el seguimiento hasta la notificación a EL CLIENTE cuando la actividad identificada ha sido dada de baja o cuando se requiere de algún procedimiento adicional. Entre la actividad maliciosa considerada para su baja están:

- Sitios Phishing.
- Malware.
- Suplantación de identidad.
- Abuso de marca.
- Perfiles apócrifos.
- Anuncios fraudulentos.