NOVASIGHT
Powered by EAGLESIGHT

MNEMO

La ciberseguridad del futuro es hoy;
agentes IA que piensan, aprenden y actúan por ti

mnemo.com/eaglesight-nova

*La **ciberseguridad del futuro** es hoy; agentes IA que piensan, aprenden y actúan por ti*

NOVASIGHT
Powered by EAGLESIGHT

iXDR – Extended Detect & Response (Endpoint)

Threat Detection & Prevent

Motor de detección de amenazas y prevención que utiliza técnicas avanzadas para identificar malware mediante el análisis de comportamientos y la detección de vulnerabilidades de día cero, asegurando una protección proactiva contra ataques desconocidos.

Endpoint Advanced Threat Intelligence

Motor que potencia el análisis de amenazas mediante inteligencia avanzada y modelado de amenazas, permitiendo la detección temprana de riesgos emergentes y proporcionando una visión detallada de los riesgo con capacidad de respuesta inmediata.

Endpoint Infrastructure Security

Protección integral para infraestructuras en la nube y contenedores, asegurando configuraciones de seguridad robustas, gestión de vulnerabilidades y una respuesta ágil ante incidentes en entornos críticos. Adaptado para entornos OT/IOT con conexión y sin ella.

Extended AI Agents (Endpoint Protection)

Los agentes aplican IA especialmente entrenada directamente en los endpoints para ofrecer una protección autónoma y adaptativa, detectando y respondiendo ante amenazas actuales y escenarios prospectivos, con aprendizaje automático real-time.

Smart Response Orchestration and Automation

SOAR con conectores avanzados y playbooks automatizados que optimiza la orquestación de respuestas ante incidentes con IA, garantizando rapidez y eficiencia, integrando diferentes herramientas y procesos en una única solución.

Innovación en la defensa con **iXDR**, diseñado para **detectar, prevenir y responder** ante las amenazas más sofisticadas en tiempo real. Con **inteligencia artificial, análisis predictivo, y protección autónoma** que se adapta continuamente a **nuevas amenazas**, sus motores ofrecen seguridad integral, en toda la **infraestructura** más allá de las capacidades tradicionales.

PROTECCIÓN INTELIGENTE

iXDR redefine la protección inteligente, ofreciendo una defensa integral que abarca desde la detección proactiva de malware hasta la respuesta automatizada ante incidentes. Con capacidades de identificación de amenazas basadas en el comportamiento y el análisis de día cero, la plataforma ofrece un enfoque holístico para mitigar las amenazas emergentes.
A través de la inspección profunda de muestras y el análisis avanzado de vulnerabilidades en tiempo real, cada capa de la infraestructura es protegida mediante la implementación de defensas adaptativas que se ajustan dinámicamente según las características de las amenazas. Las infraestructuras críticas, incluidas las cargas de trabajo en la nube, contenedores y sistemas locales. La integración de múltiples módulos de seguridad, como la monitorización de endpoints, la gestión de configuraciones de seguridad, y la respuesta a incidentes mediante SOAR, ofrece capacidades nativas sin depender de soluciones externas. Motores de análisis forense y threat hunting, permiten realizar
consultas complejas sobre endpoints remotos y conjuntos de datos identificando anomalías y amenazas en fase temprana.

DEFENSA ELEVADA POR IA

iXDR IA es el corazón de nuestra solución, optimizando cada aspecto de la detección, respuesta y análisis. Mediante el uso de modelos de aprendizaje automático y la correlación de grandes volúmenes de datos, la IA permite la identificación de malware mediante patrones de comportamiento y la generación de defensas autónomas que se inyectan automáticamente en los EDRs. La integración con EDRs privados y públicos proporciona telemetría completa que alimenta el sistema mejorando la capacidad de respuesta con predicciones avanzadas. iXDR IA facilita la generación automática de reglas de firewall, scripts de aislamiento, y playbooks defensivos, adaptándose continuamente a las
nuevas TTPs de los atacantes. Además, los agentes IA especializados permiten una evaluación prospectiva y retrospectiva de los incidentes, proporcionando inteligencia contextualizada que mejora las capacidades de investigación, optimizando la generación de alertas enriquecidas, con un análisis automatizado de anomalías, creando modelos de ataque y planes de acción adaptados a cada incidente, garantizando una respuesta más rápida y precisa en tiempo real, anticipando las amenazas.

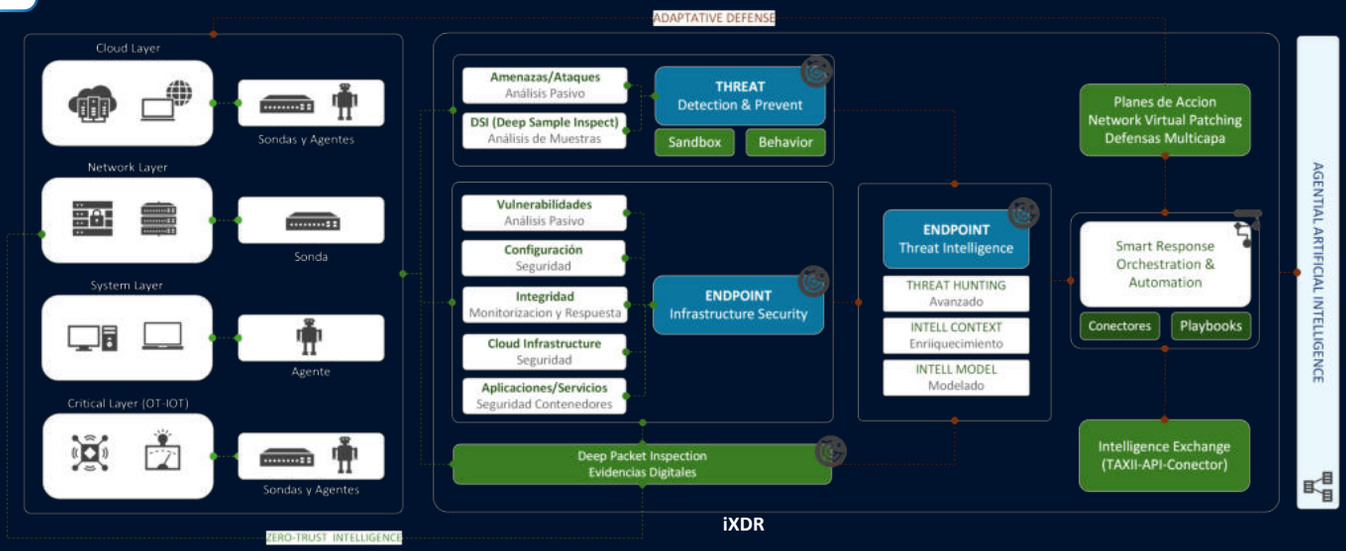
Tecnología que se despliega en entornos cloud, on-premise, híbridos, y desconectados (air-gap). Diseñada con capacidades específicas para cada uno de los ecosistemas IT, OT, IOT, Infraestructuras Críticas y entornos Militares, con modelos IA embebidos, dedicados y aislados. Integración y accesibilidad completa a nivel de API, BBDD y código.

MNEMO
mnemo.com
info@mnemo.com

*La **ciberseguridad del futuro** es hoy; agentes IA que piensan, aprenden y actúan por ti*

NOVASIGHT
Powered by EADLESIGHT

iXDR – Extended Detect & Response (Endpoint)



ENDPOINT INFRASTRUCTURE SECURITY

ANÁLISIS PASIVO DE VULNERABILIDADES

Monitorización continua de inventario y análisis cruzado de vulnerabilidades actuales con afectación, tiempo que llevan explotándose y criticidad, con desarrollo automático de un plan de remediación priorizado.

SEGURIDAD EN LA CONFIGURACIÓN

Monitorización del grado de riesgo y criticidad de la configuración y hardening, y estado del sistema según estándares. El módulo esta integrado con el sistema IA agencial para que de forma automática se evalue el nivel deadecuación, mejoras y posibles debilidades.

MONITORIZACIÓN DE LA INTEGRIDAD

Análisis permanente de la estructura de ficheros e identificación de cambios no autorizados con actividades anómalas verificables y correladas, y si se ha realizado aprobado por políticas. Cada cambio se correla con reglas comportamiento
YARA generadas de forma directa o dinámica por la IA.

SEGURIDAD INFRAESTRUCTURAS CLOUD

Combina un sistema de monitorización avanzada con visibilidad total en entornos de hiperescalar, como AWS, Azure y Google Cloud, permitiendo una supervisión profunda de las cargas de trabajo, recursos y configuraciones de
seguridad. Integra un servicio CSPM continuo y

THREAT DETECTION & PREVENT

COMPORTAMIENTO: Identificación de amenazas y malware a través de comportamiento y ML, identificación de las características, TTPs, conexiones de red, entro muchos otros aspectos del malware. Tiene conexión bidireccional con la mayoría de los EDRs privados y públicos.

INSPECCIÓN PROFUNDA DE MUESTRAS:

Inspección profunda de muestras (DSI), y análisis avanzados Zero-day, con análisis a través de sandbox propia interna para identificar firmas de amenazas, anomalías de TTPs y compromiso de comunicaciones.

SMART RESPONSE ORCHESTRATION

Respuesta a través de plataforma SOAR interna, con conectores predefinidos para, mas de 1000 integraciones, pudiendo realizar operaciones con los datos, generar planes de respuesta de forma automática, y establecer playbooks interactivos.

Generación de contramedidas: creación en tiempo real reglas de firewall, scripts de aislamiento, YARA, SIGMA o playbooks defensivos para desplegar directamente.

SEGURIDAD EN CONTENEDORES

Monitoriza activamente los eventos de ejecución de los contenedores y los registros de aplicaciones. Identificación de anomalías con registro de las acciones para detectar actividades no autorizadas en un entorno contenedorizado.

ENDPOINT THREAT INTELLIGENCE

THREAT HUNTING ADAPTADO

Lenguaje de consultas diseñado específicamente para análisis forense y threat hunting; permite construir queries complejas y precisas sobre endpoints remotos o conjuntos de datos en memoria/disco.

INTELIGENCIA CONTEXTUALIZADA

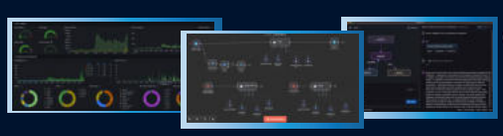
Generación de alertas enriquecidas, incluyendo contexto de activos, usuario y mapeo MITRE ATT&CK, y contramedidas a través MITRE DEFEND y CIS, con priorización inteligente, generando modelos de ataque y planes de acción adaptados.

ESTRUCTURAS MODULARES

Sistema modular de artefactos, conjunto de reglas y playbooks de aplicación, para definir colecciones, análisis y queries, pudiendo crear,
versionar, compartir y modificar artefactos
fácilmente.

ZERO-TRUST INTELLIGENCE

Capacidad interna de captura y análisis de configuraciones de sistemas, firewalling y networking, para la generación de patrones estructurales, rotura de integridad en la operativa de seguridad e identificación de
posibles ataques verticales y horizontales.



DEFENSA ADAPTATIVA

El sistema ajusta dinámicamente las políticas de adquisición y búsqueda en base a patrones **anómalos detectados, generando reglas y consultas específicas para investigar posibles** variantes de amenazas, con recomendaciones automáticas de contención.

**Integración de modelo inteligencia de amenazas (STIX/TAXII), se puede capturar y enviar datos de inteligencia STIX de forma directa, API, o por un servidor
interno TAXII. Generación dinámica de dashboards e informes en tiempo real (líneas de tiempo, IoCs, acciones) para auditorías y análisis. Binarios**

MNEMO
mnemo.com
info@mnemo.com


NOVASIGHT
Powered by EAGLESIGHT