UNIVERSITAS Miguel Hernández

Networking Academy

Networking Academy

European NetAcad Instructor Training

Gestión de Incidentes con Security Onion 2.4

- 19/05/2025 – Cisco Netacad
- 26/05/2025 – Networking
- 02/06/2025 – Ciberseguridad
- 09/06/2025 – Ciencia de datos e IA

Alberto Aparicio Vila
Instructor Cisco
Universidad Miguel Hernández
Elche (Alicante)
alapvi@yahoo.com

RECORD

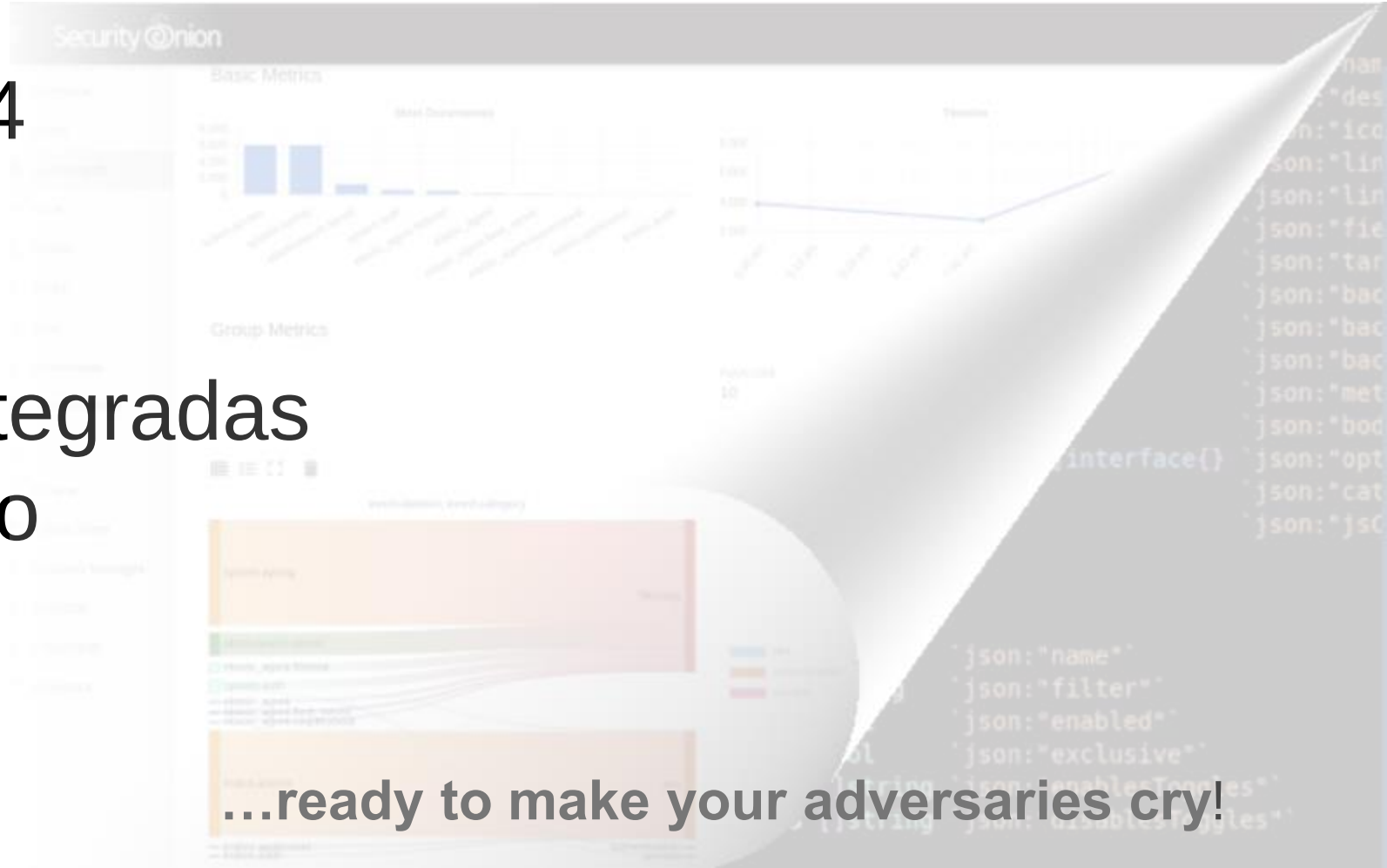
2 de junio, 2025

UNIVERSITAS Miguel Hernández

Networking Academy

Índice

- Motivación
- Security Onion 2.4
- Arquitecturas
- Instalación
- Características integradas
- Security Onion Pro



…ready to make your adversaries cry!

UNIVERSITAS Miguel Hernández

Networking Academy

Motivación

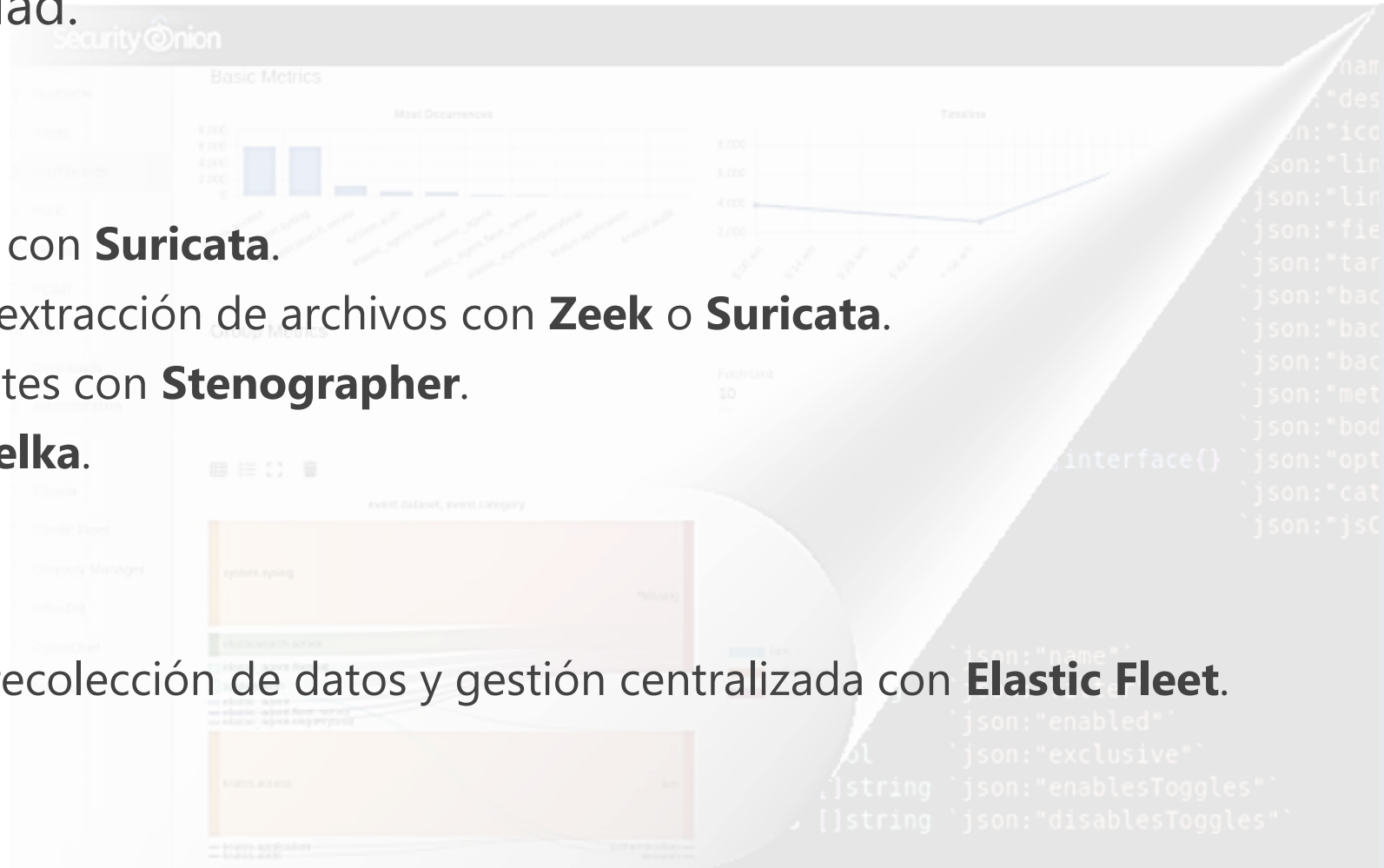
	Security Onion 2016	Security Onion 2.4.150 (2025)
Arquitectura	Monolítica	Modular y distribuida
Sistema Operativo Base	Ubuntu 14.04 LTS	Oracle Linux 9
Motores de detección	Bro (ahora Zeek), Snort	Suricata, Zeek, Strelka
Almacenamiento logs	ELSA (MySQL + Sphinx)	Elastic Stack (Elasticsearch, Logstash, Kibana)
Interfaz de usuario	ELSA (búsqueda de logs), interfaces separadas	Consola web unificada con múltiples vistas (Alerts, Hunt, Cases, etc.)
Herramientas de análisis	Logs y alertas básicas	Análisis avanzado de tráfico, alertas, PCAP, gestión de casos, playbooks, Elast Agents,…
Opciones de despliegue	Local, en una sola máquina	Local, distribuido, nube (AWS, Azure,...),
Soporte en la nube	No	Sí, con plantillas y documentación oficial
Actualizaciones	No	Automatizadas con soup y control de versiones

UNIVERSITAS Miguel Hernández

Networking Academy

Security Onion 2.4

Security Onion es una plataforma gratuita y de código abierto diseñada para defensores de la ciberseguridad.



- **Visibilidad de red**
  - ✓ Detección basada en firmas con **Suricata**.
  - ✓ Metadatos de protocolos y extracción de archivos con **Zeek** o **Suricata**.
  - ✓ Captura completa de paquetes con **Stenographer**.
  - ✓ Análisis de archivos con **Strelka**.

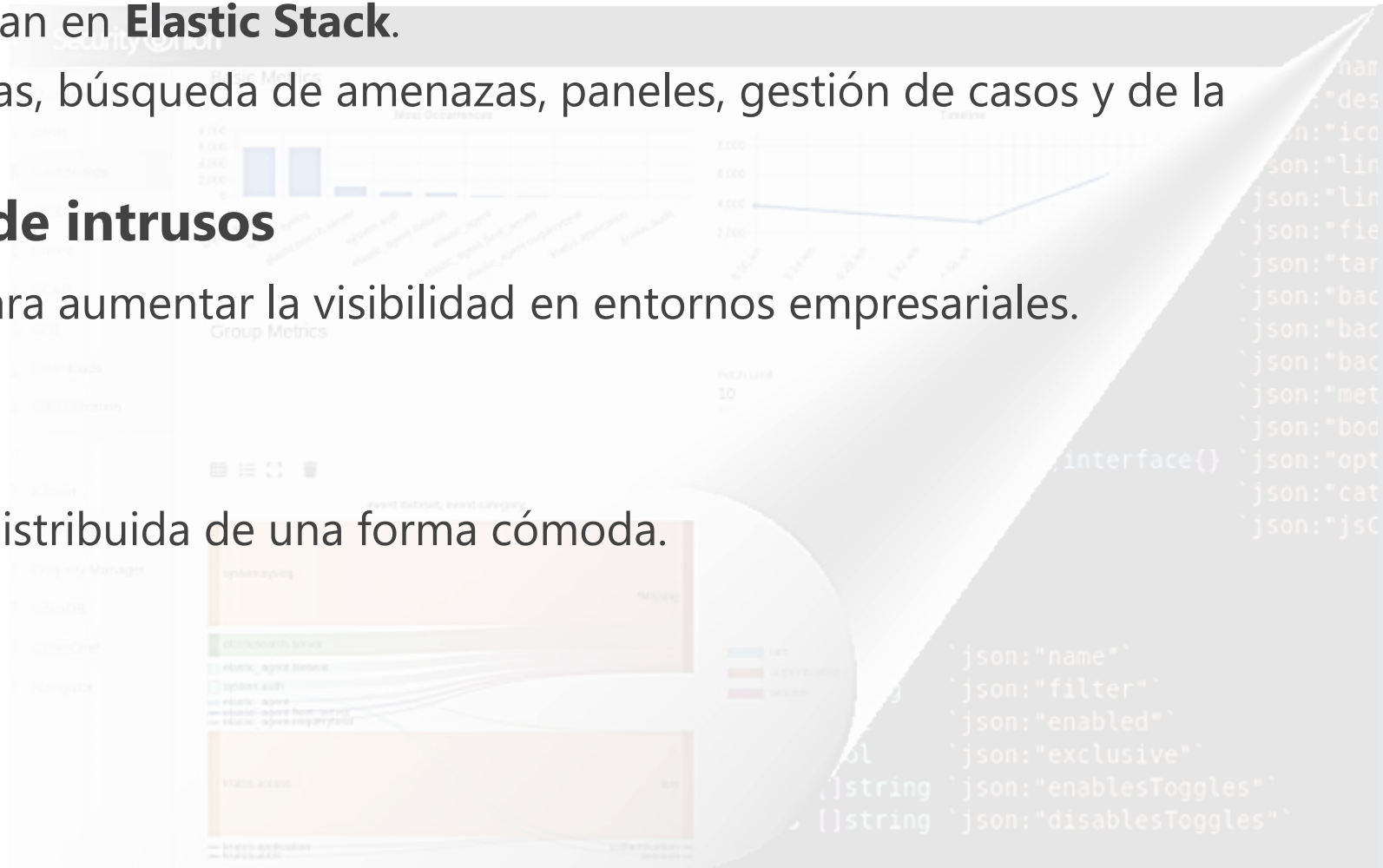
- **Visibilidad de hosts**
  - ✓ Uso de **Elastic Agent** para recolección de datos y gestión centralizada con **Elastic Fleet**.

UNIVERSITAS Miguel Hernández

Networking Academy

Security Onion 2.4

- **Gestión de registros y casos**:
  - Todos los registros se integran en **Elastic Stack**.
  - Interfaces propias para alertas, búsqueda de amenazas, paneles, gestión de casos y de la red.
- **Honeypots de detección de intrusos**
  - Basados en **OpenCanary**, para aumentar la visibilidad en entornos empresariales.
- **Facilidad de uso**
  - Permite desplegar una red distribuida de una forma cómoda.



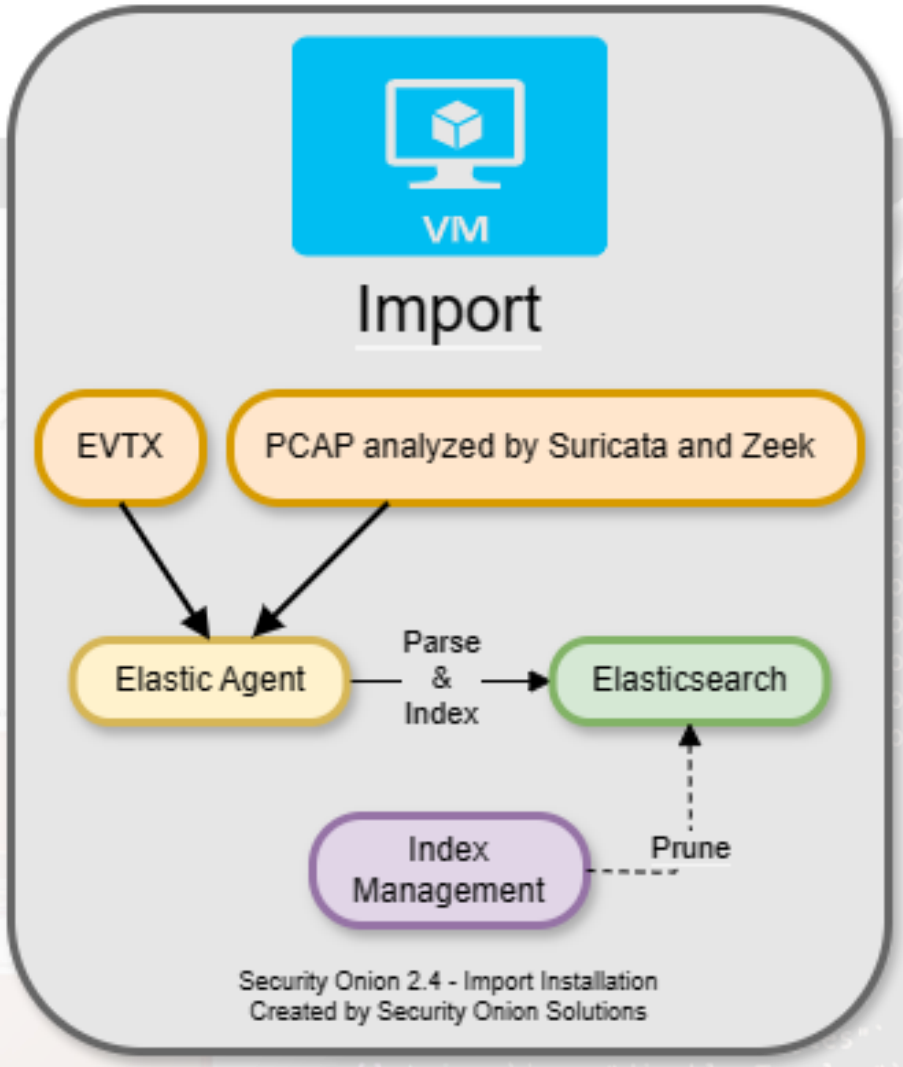
UNIVERSITAS Miguel Hernández

Networking Academy

Arquitecturas

Nodo Import

- ✓ Arquitectura más simple: nodo único y autónomo.
- ✓ Permite importar archivos **pcap** o **evtx** desde la página **Grid**.
- ✓ **No admite** agentes Elastic ni nodos adicionales.
- ✓ Ideal para análisis forense puntual o entornos de prueba.



Requisitos:

2 CPUs cores	4GB RAM	50GB	1 NIC

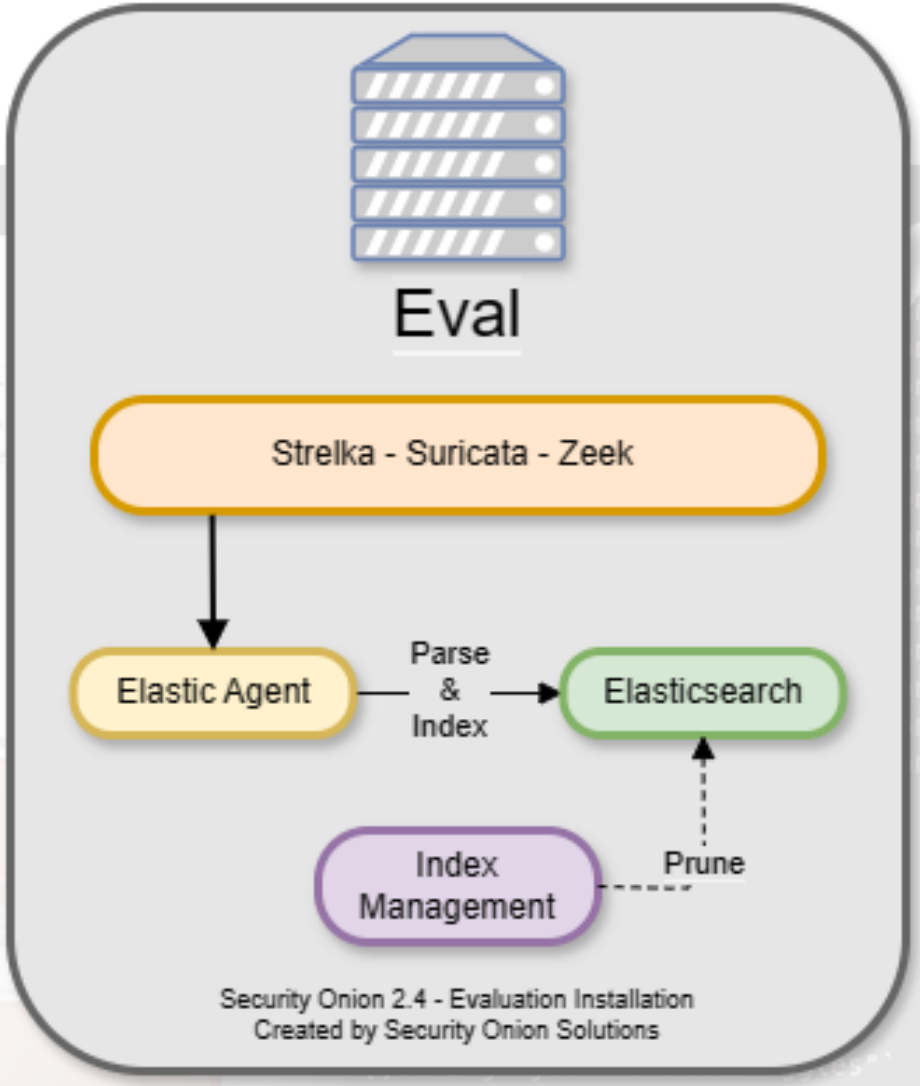
UNIVERSITAS Miguel Hernández

Networking Academy

Arquitecturas

Evaluation

- ✓ Arquitectura intermedia con interfaz dedicada a capturar tráfico en vivo (TAP o SPAN).
- ✓ Genera y recolecta logs en tiempo real mediante **Elastic Agent**.
- ✓ Los logs se envían directamente a **Elasticsearch** para su análisis.
- ✓ Diseñado para **pruebas temporales**, **no apto para producción**.
- ✓ No permite añadir agentes Elastic ni nodos adicionales.



Requisitos:

4 CPUs cores	8GB RAM	200GB	2 NIC

UNIVERSITAS Miguel Hernández

Networking Academy

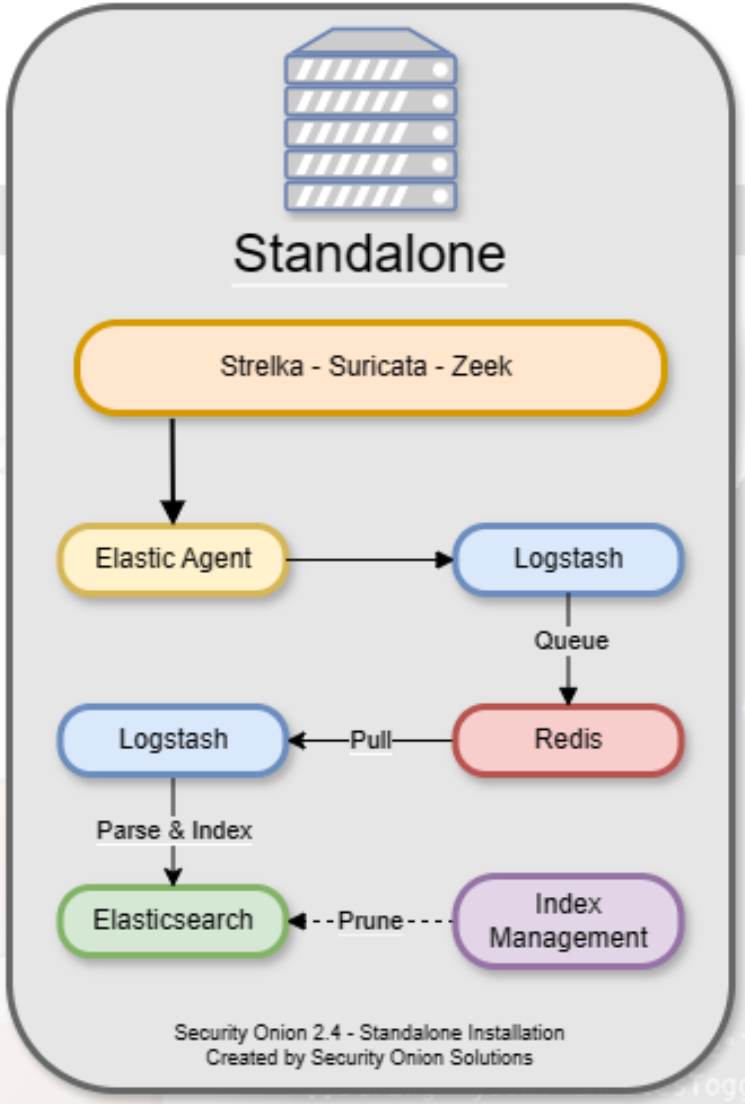
Arquitecturas

Standalone

- ✓ Similar a **Evaluation**, pero con flujo de logs más completo.
- ✓ **Elastic Agent** envía logs a **Logstash**, que los pasa a **Redis**.
- ✓ Otro pipeline de Logstash los extrae de Redis y los envía a **Elasticsearch**.
- ✓ Ideal para **pruebas, laboratorios** o entornos de bajo tráfico.
- ✓ **No escalable** como una arquitectura distribuida.

Requisitos:

4 CPUs cores	24GB RAM	200GB	2 NIC

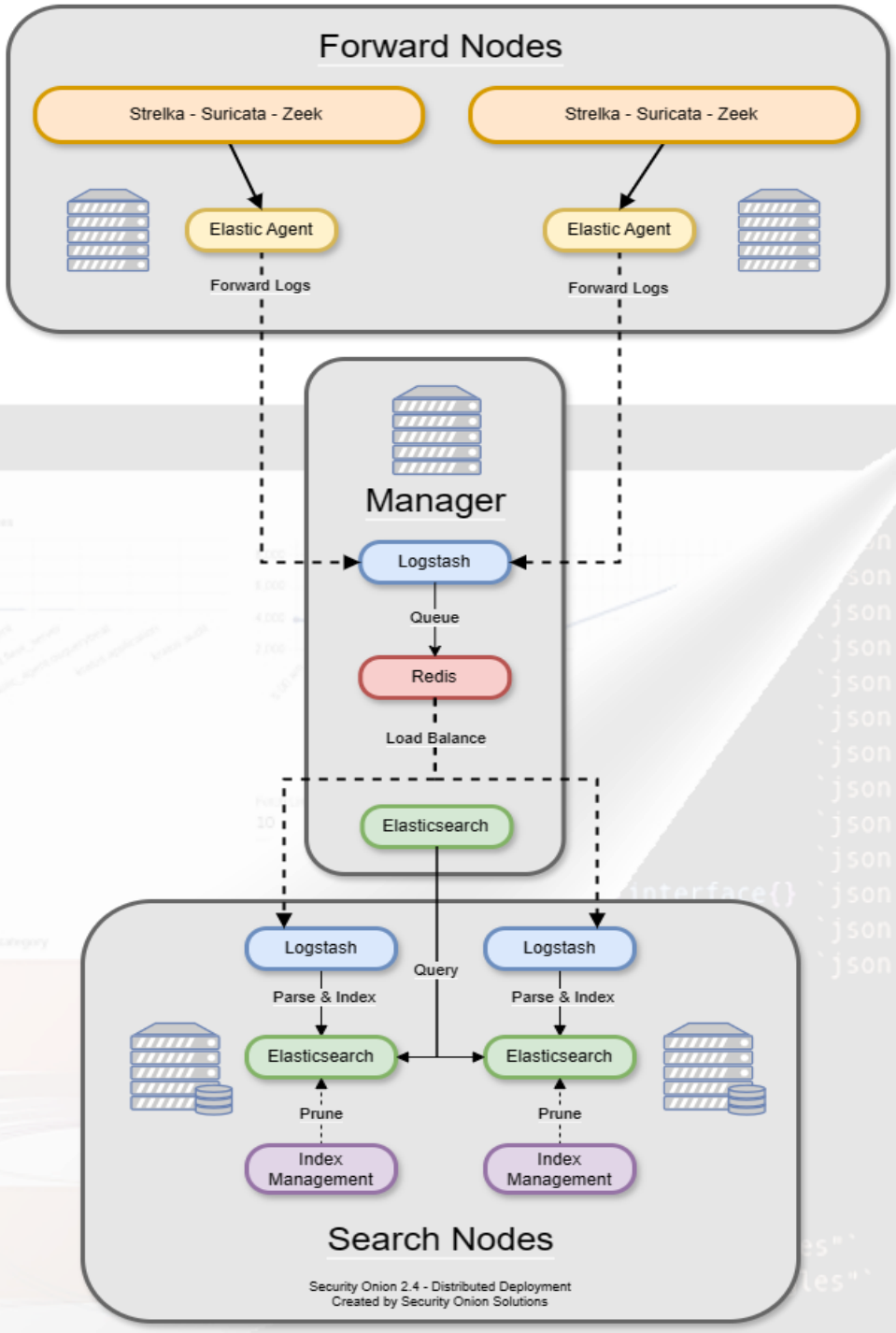


UNIVERSITAS Miguel Hernández

Arquitecturas

Distributed

- ✓ Arquitectura recomendada para entornos de producción.
- ✓ Incluye:
  - **Nodo Manager** (gestión central).
  - Uno o más **nodos Forward** (sensores de red).
  - Uno o más **nodos Search** (componentes de búsqueda con Elasticsearch).
- ✓ Mayor **escalabilidad y rendimiento**.
- ✓ Permite añadir nodos fácilmente para manejar más tráfico o fuentes de logs.
- ✓ Requiere más recursos, pero ofrece mejor capacidad a largo plazo.



Requisitos:

Forward node	4 Cores	12GB RAM	200GB	2 NIC
Manager	8 Cores	16GB RAM	200GB	1 NIC
Search node	4 Cores	16GB RAM	200GB	1 NIC

UNIVERSITAS Miguel Hernández

Networking Academy

Instalación

- **Proceso de instalación**:
  - ✓ Iniciar desde la ISO en una máquina compatible.
  - ✓ Seguir los pasos del instalador gráfico.
  - ✓ Establecer nombre de host correctamente (no se puede cambiar después).
  - ✓ Reiniciar y acceder con las credenciales configuradas.
- **Opciones en la nube**:
  - ✓ Imágenes oficiales disponibles para AWS, Azure y Google Cloud.

UNIVERSITAS Miguel Hernández

Networking Academy

Características Integradas

- **Alerts**

✓ Interfaz de **Alertas** para visualizar eventos generados por Security Onion.

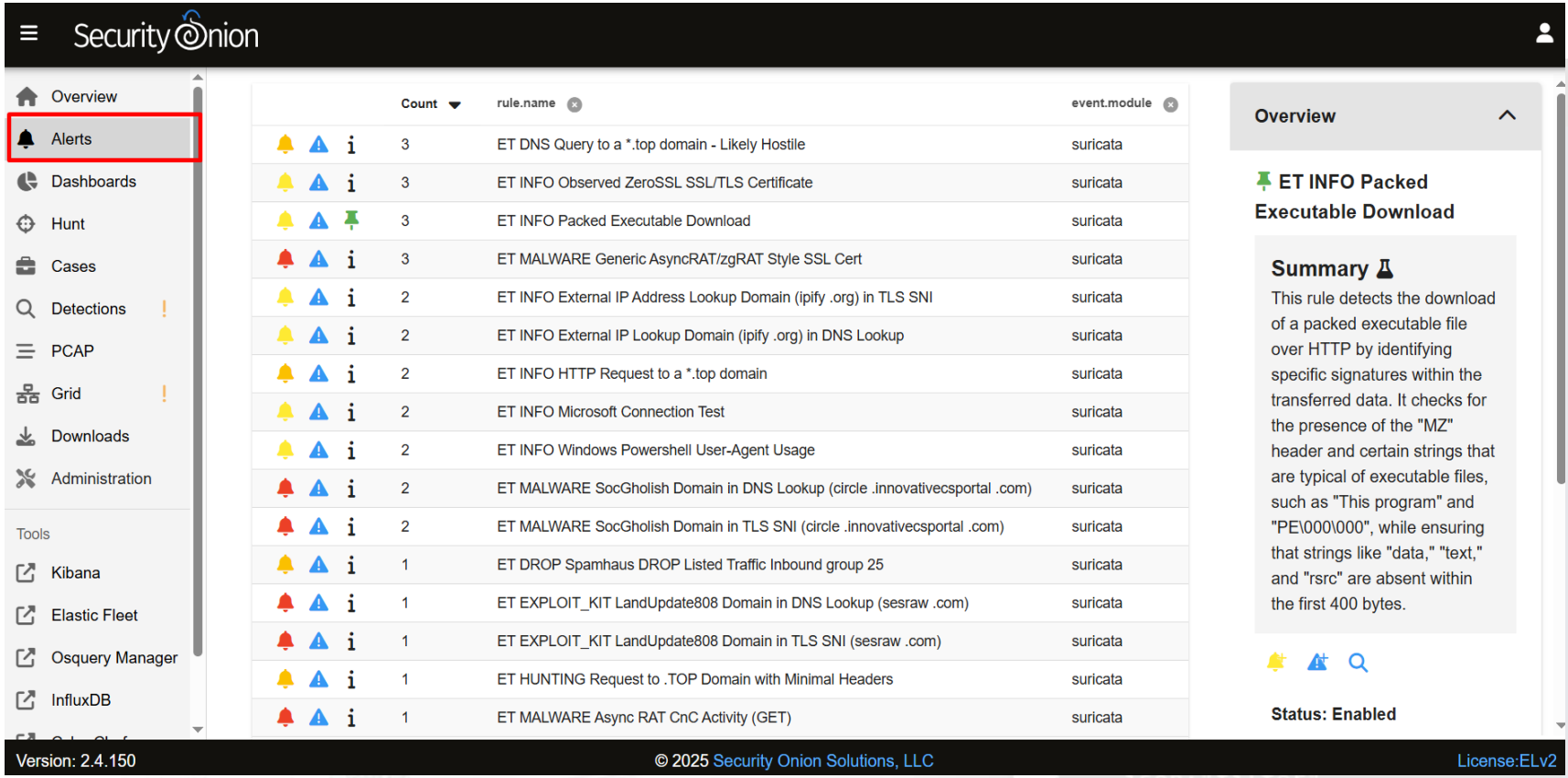
✓ Permite análisis detallado con un solo clic.

✓ Posibilidad de **pivotar** hacia:

  ✓ **Hunt** (búsqueda avanzada).

  ✓ **PCAP** (análisis de paquetes).

✓ Escalado de alertas a **Casos** para su gestión y seguimiento.



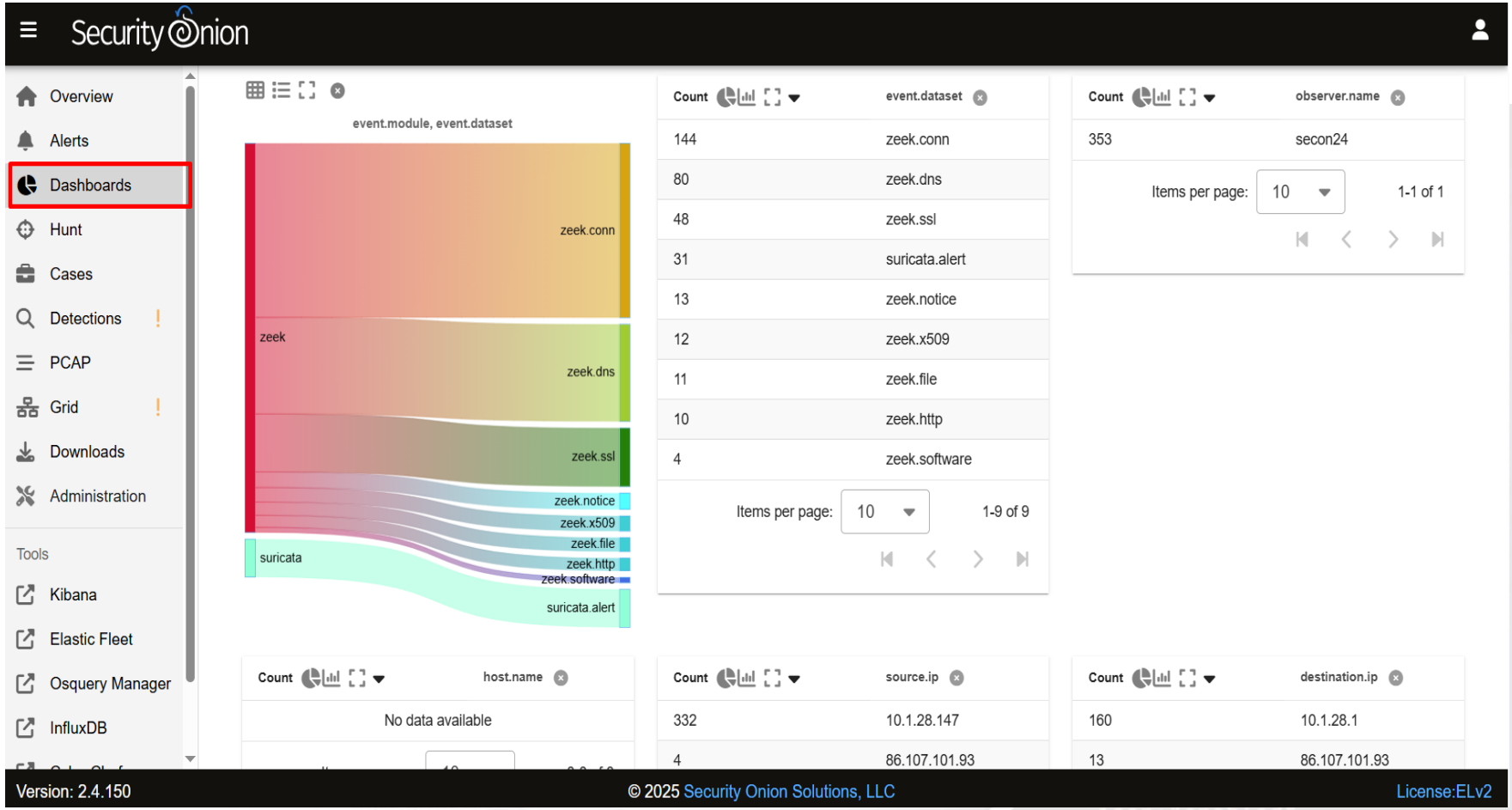
Características Integradas

- **Dashboards**

✓ Interfaz con paneles preconfigurados.

✓ Visualización clara y rápida de los **tipos de datos estándar**.

✓ Facilita el monitoreo y análisis de seguridad en tiempo real.



UNIVERSITAS Miguel Hernández

Networking Academy

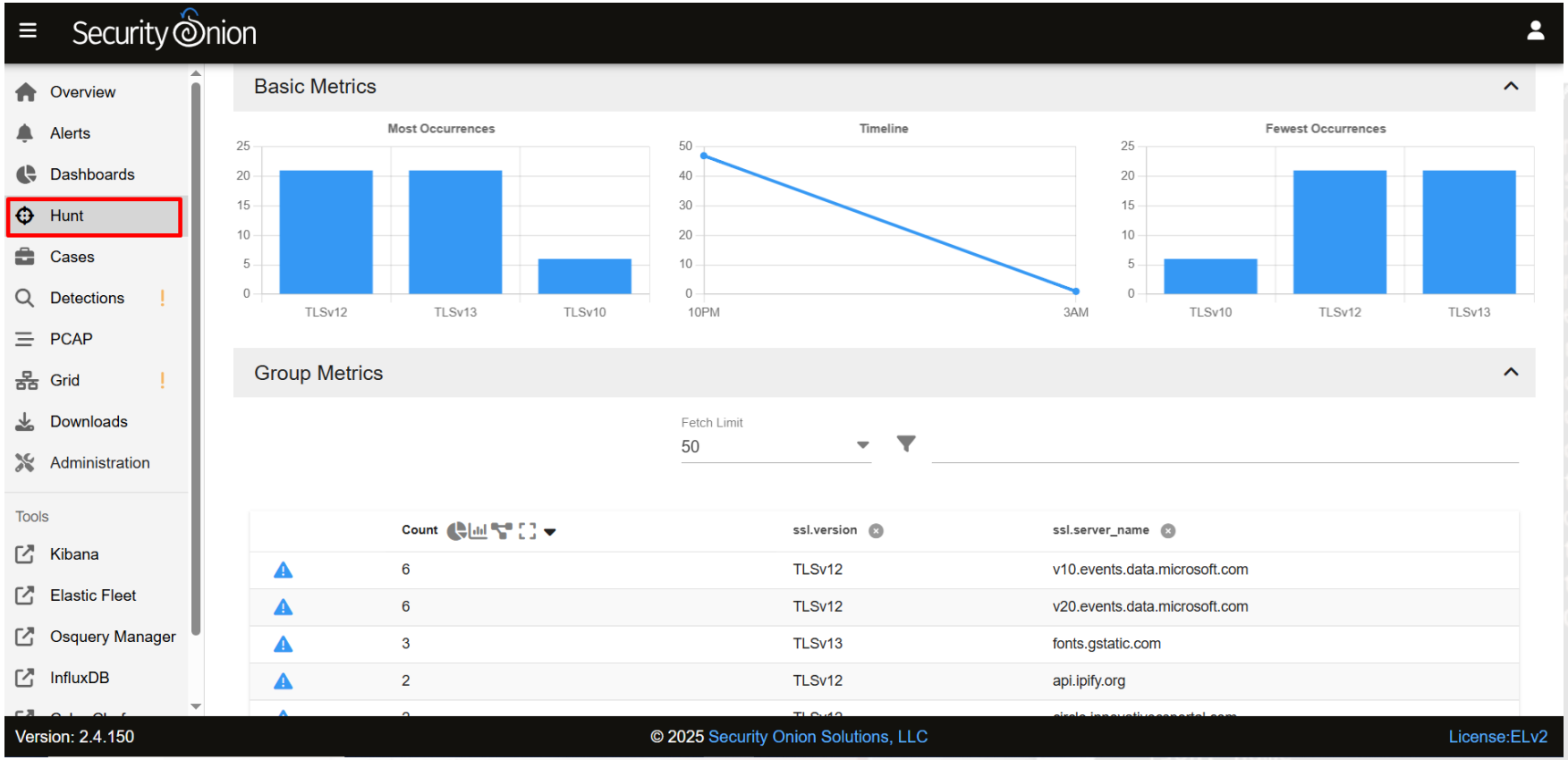
Características Integradas

- **Hunt**

✓ Consultas más **específicas** y enfocadas.

✓ Hunt **agrega múltiples campos** en una sola tabla (útil para detectar actividad inusual).

✓ Ambos son similares en funcionalidad general.

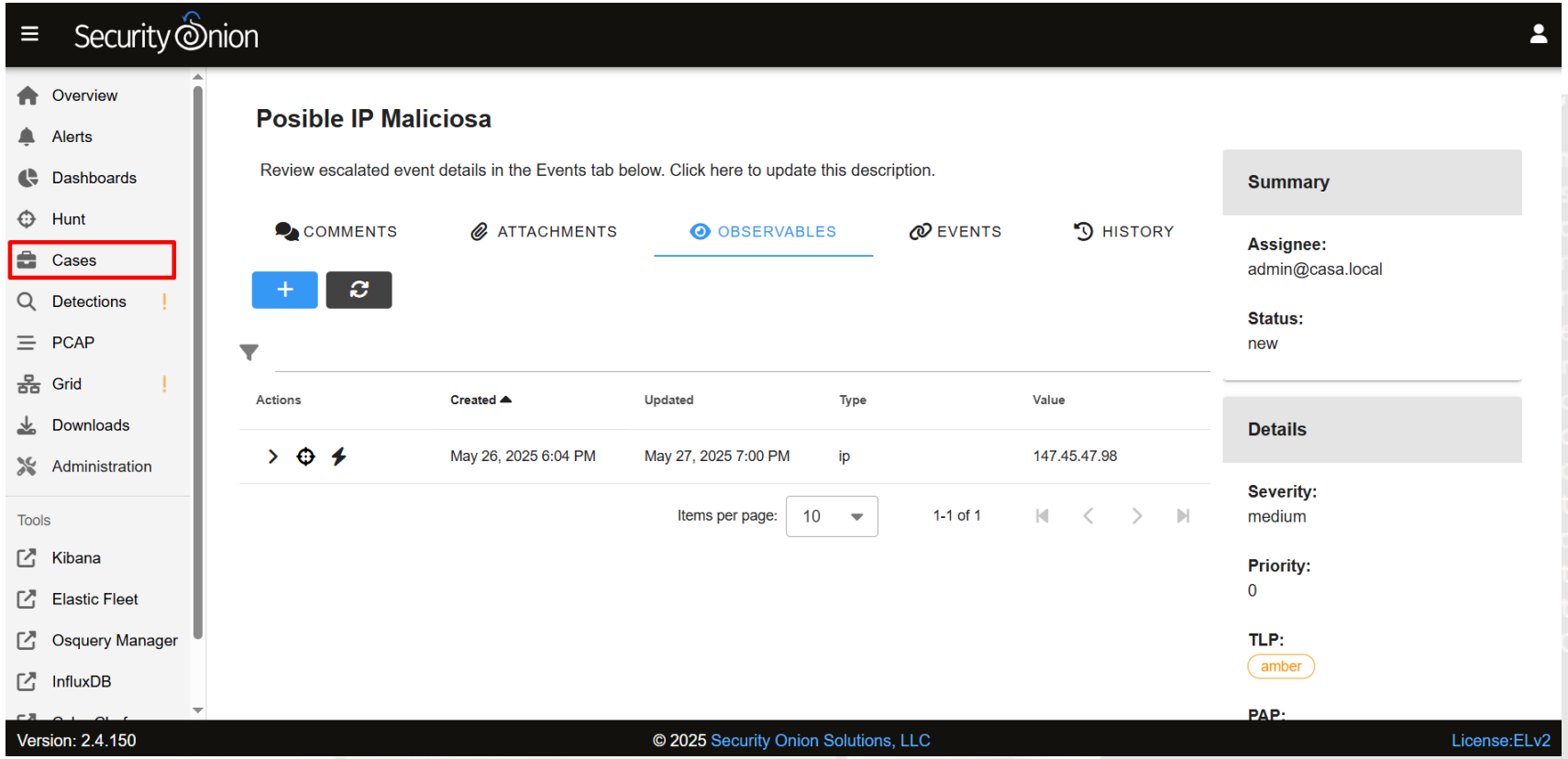


Características Integradas

- **Cases**

✓ Permite escalar registros desde *Alerts*, *Dashboards* y *Hunt*.

✓ Facilita la gestión colaborativa de incidentes mediante asignación de analistas, comentarios, adjuntos y seguimiento de observables.



UNIVERSITAS Miguel Hernández

Networking Academy

Características Integradas

- **Detections**

✓ **NIDS (Suricata)**: Reglas de detección de intrusos en red.

✓ **Sigma (ElastAlert 2)**: Reglas para eventos sospechosos en logs.

✓ **YARA (Strelka)**: Reglas para análisis de archivos y malware.

UNIVERSITAS Miguel Hernández

Networking Academy

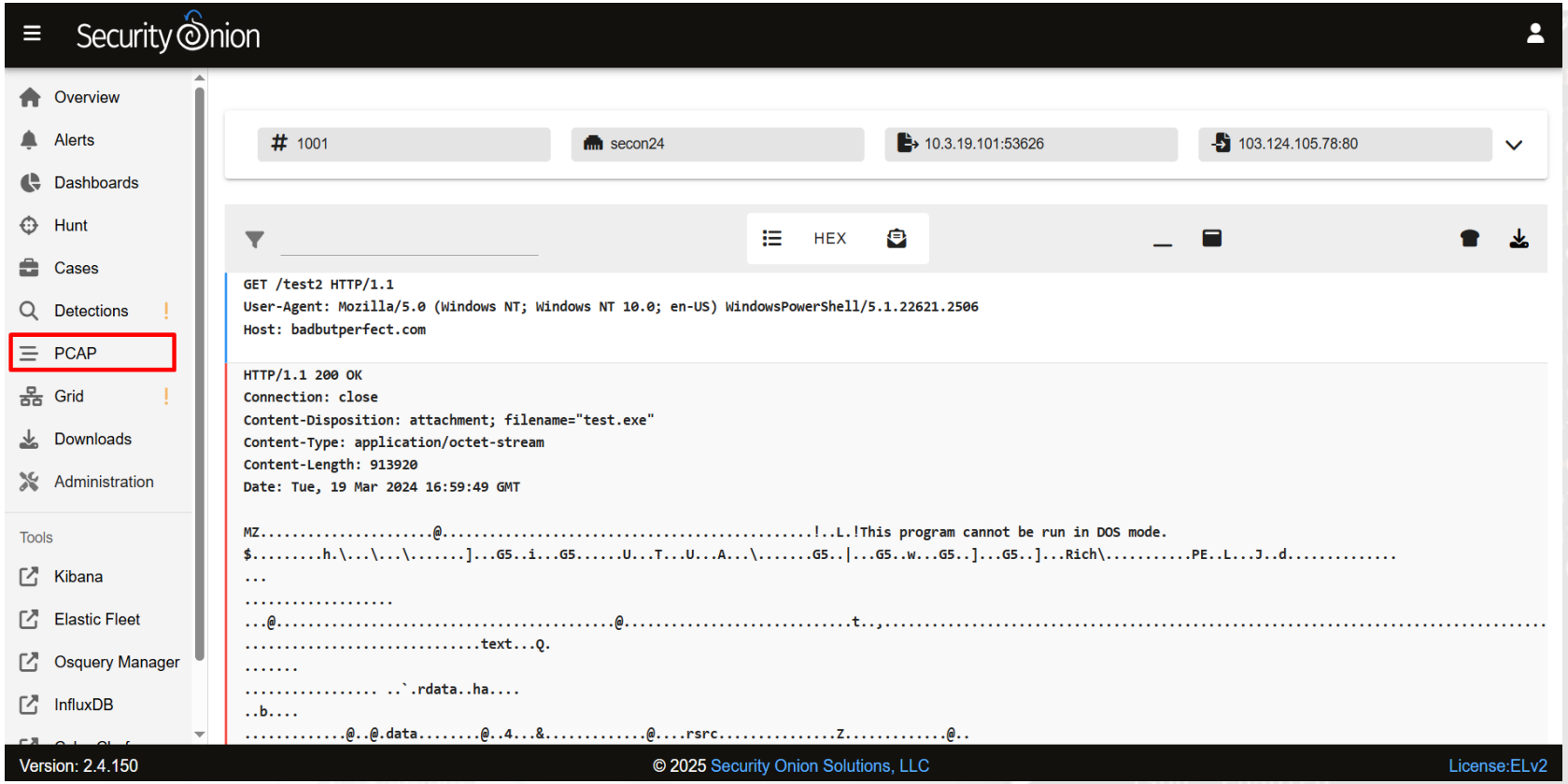
Características Integradas

- **PCAP**

✓ **Acceso completo a capturas de paquetes (PCAP)** almacenadas por **Stenographer** o **Suricata**.

✓ **Dos formas de acceso**:

- **A través de** *Alerts*, *Dashboards* o *Hunt* usando la acción **PCAP**.
- **Acceso directo** a la interfaz PCAP para búsquedas manuales.



UNIVERSITAS Miguel Hernández

Networking Academy

Características Integradas

- **Kibana**

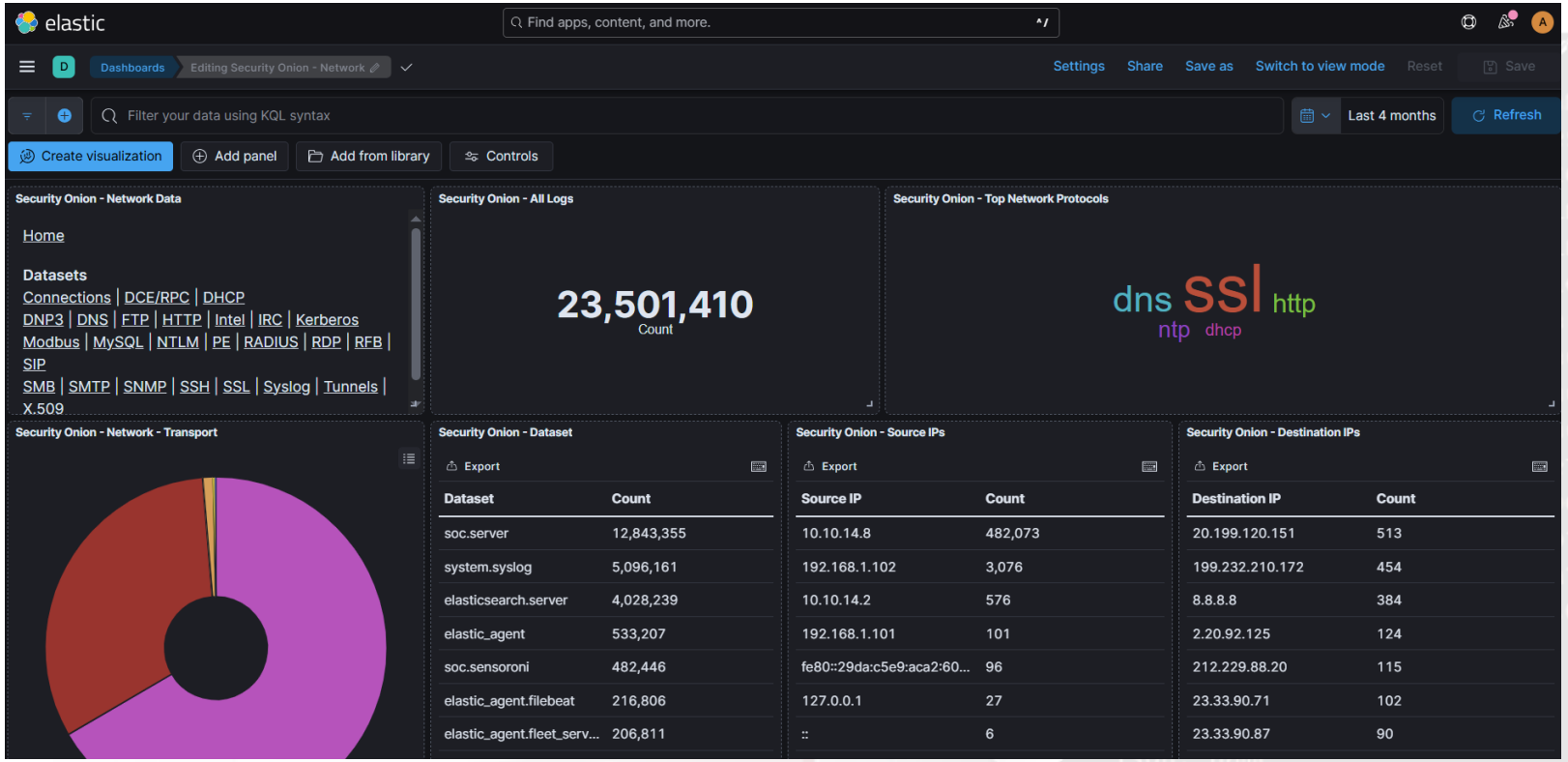
✓ Kibana actúa como interfaz para visualizar datos recolectados por Elastic Agents (Fleet).

✓ Acceso mediante las credenciales del SOC; gestión de sesiones unificada.

✓ Incluye paneles para Suricata, Zeek, Sysmon, y otros logs relevantes.

✓ Stack Management:

- ✓ Configuración de índices y patrones de búsqueda.
- ✓ Ajustes de zona horaria, tamaño de muestra y formato de datos.



UNIVERSITAS Miguel Hernández

Networking Academy

Características Integradas

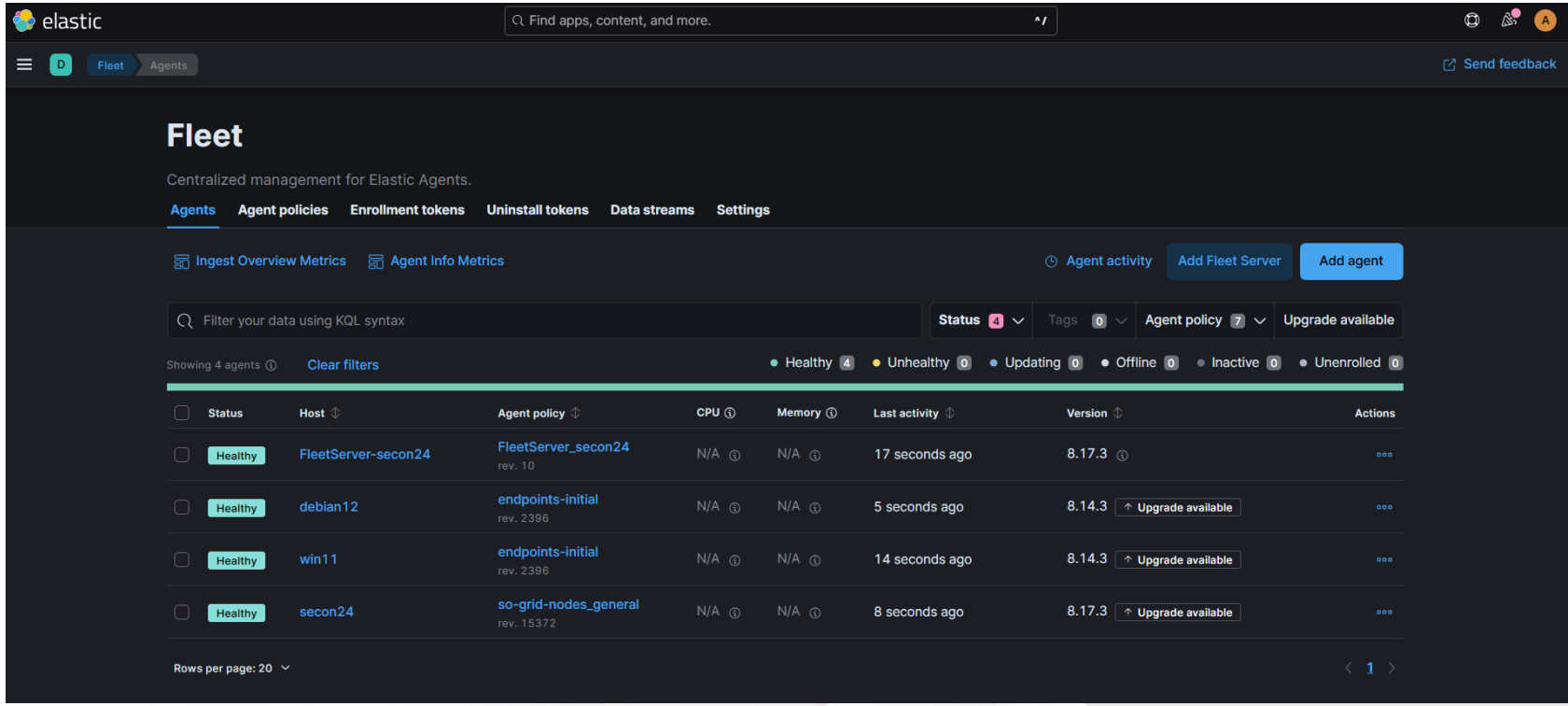
- **Elastic Fleet**

✓ Elastic Fleet se configura durante la instalación de Security Onion.

✓ Visualiza, actualiza o reasigna agentes desde la pestaña *Agents*.

✓ Definen qué datos recolecta cada agente (logs de Suricata, Zeek, Syslog, etc.).

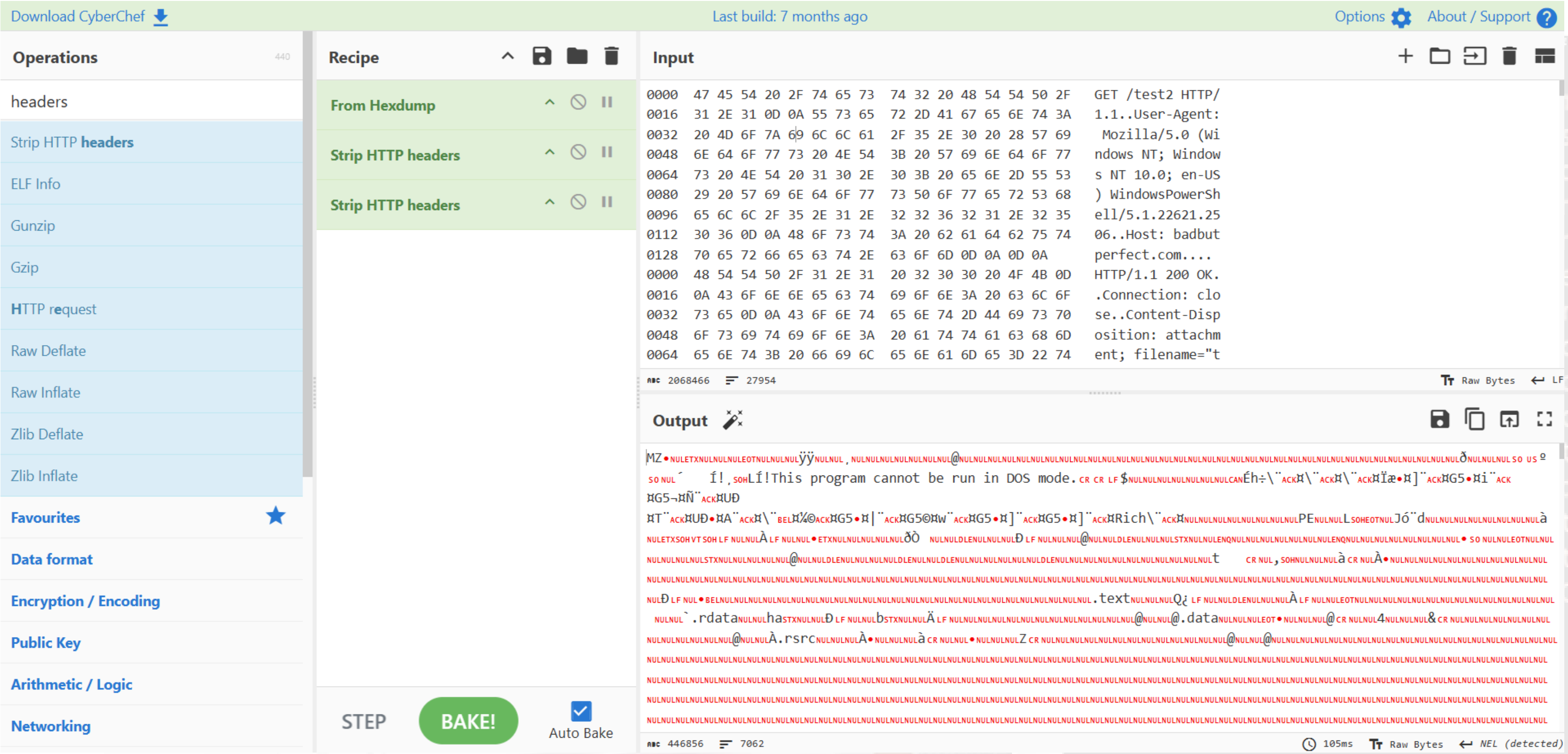
✓ Fleet detecta versiones antiguas y permite actualizaciones seguras.



Características Integradas

- **Cyberchef**

✓ Web app para realizar operaciones de análisis y transformación de datos: Codificación/decodificación (Base64, XOR, etc.)
✓ Hashes y checksums
✓ Análisis de hexdumps y binarios
✓ Extracción de archivos desde PCAP



UNIVERSITAS Miguel Hernández

Networking Academy

Características Integradas

- **ATT&CK Navigator**

✓ Herramienta simple y flexible para navegar y anotar matrices ATT&CK.

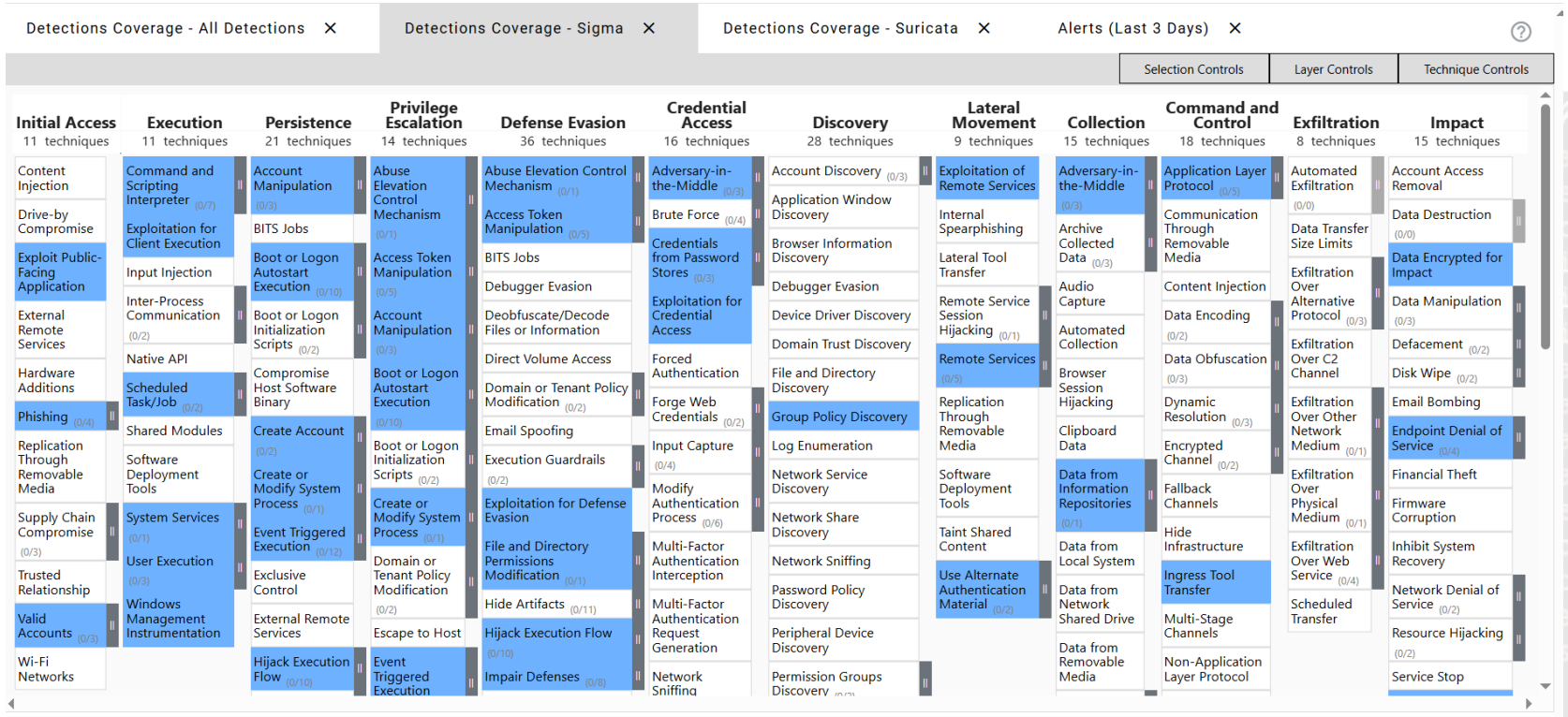
✓ Manipulación de celdas (colores, comentarios, valores numéricos).

✓ Visualización de cobertura defensiva.

✓ Análisis de frecuencia de técnicas detectadas.

✓ Vistas específicas por plataforma o adversario.

✓ https://attack.mitre.org/resources/versions/



UNIVERSITAS Miguel Hernández

Networking Academy

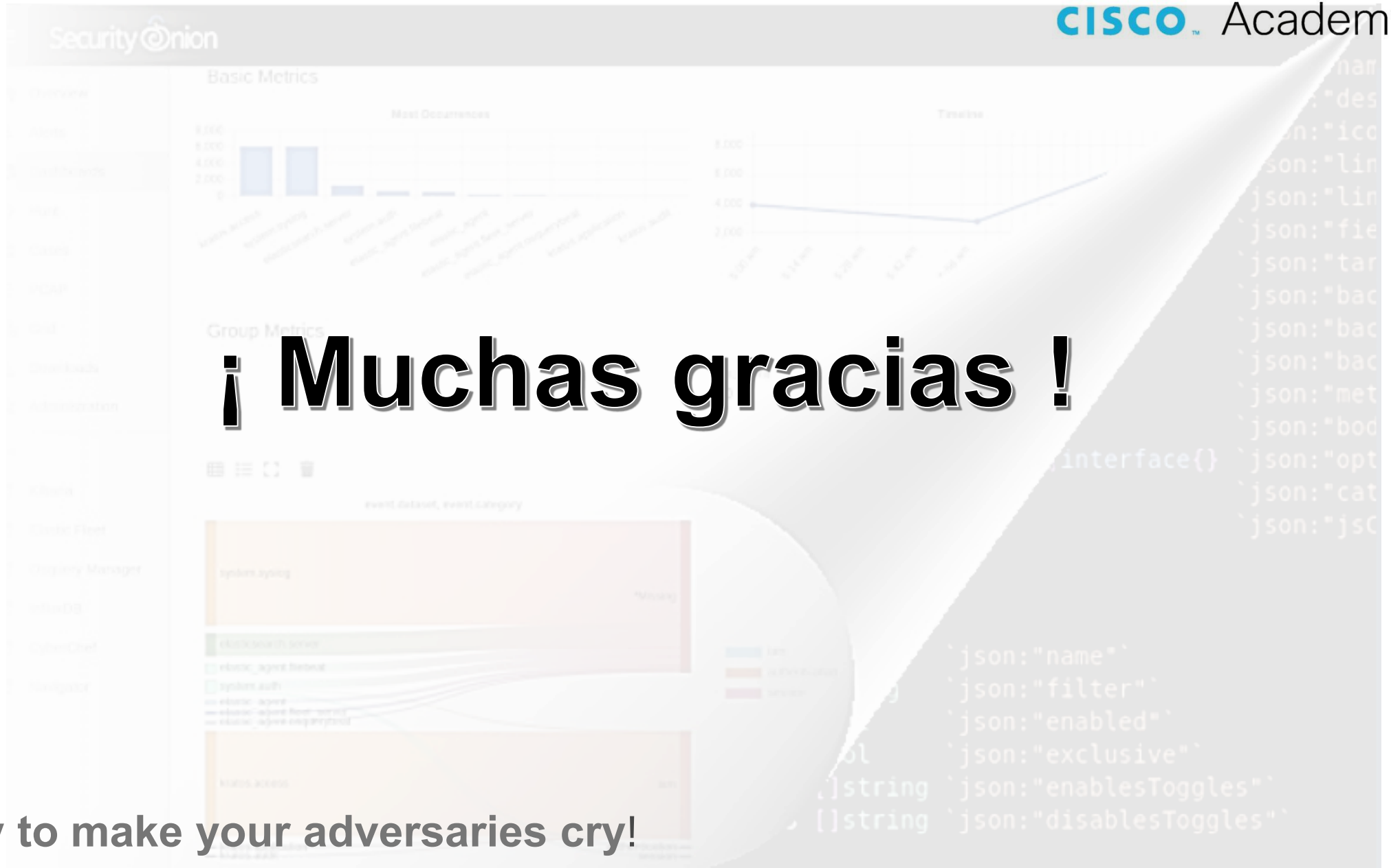
Security Onion Pro

- Soporte para alertas por email, Slack, y más.
- Integración con OIDC (Google, GitHub, AD, Auth0...).
- SLA de respuesta en 1 día hábil (o 4h opcional).
- Servicios para despliegue, tuning, parsing, soporte técnico.
- Licencias por nodo: Hasta 10 nodos por licencia estándar, ampliable.

https://securityonionsolutions.com/pro

UNIVERSITAS Miguel Hernández

Networking Academy



¡ Muchas gracias !

…ready to make your adversaries cry!