



European NetAcad Instructor Training

Gestión de Incidentes con Security Onion 2.4

Alberto Aparicio Vila

Instructor Cisco

Universidad Miguel Hernández

Elche (Alicante)

alapvi@yahoo.com

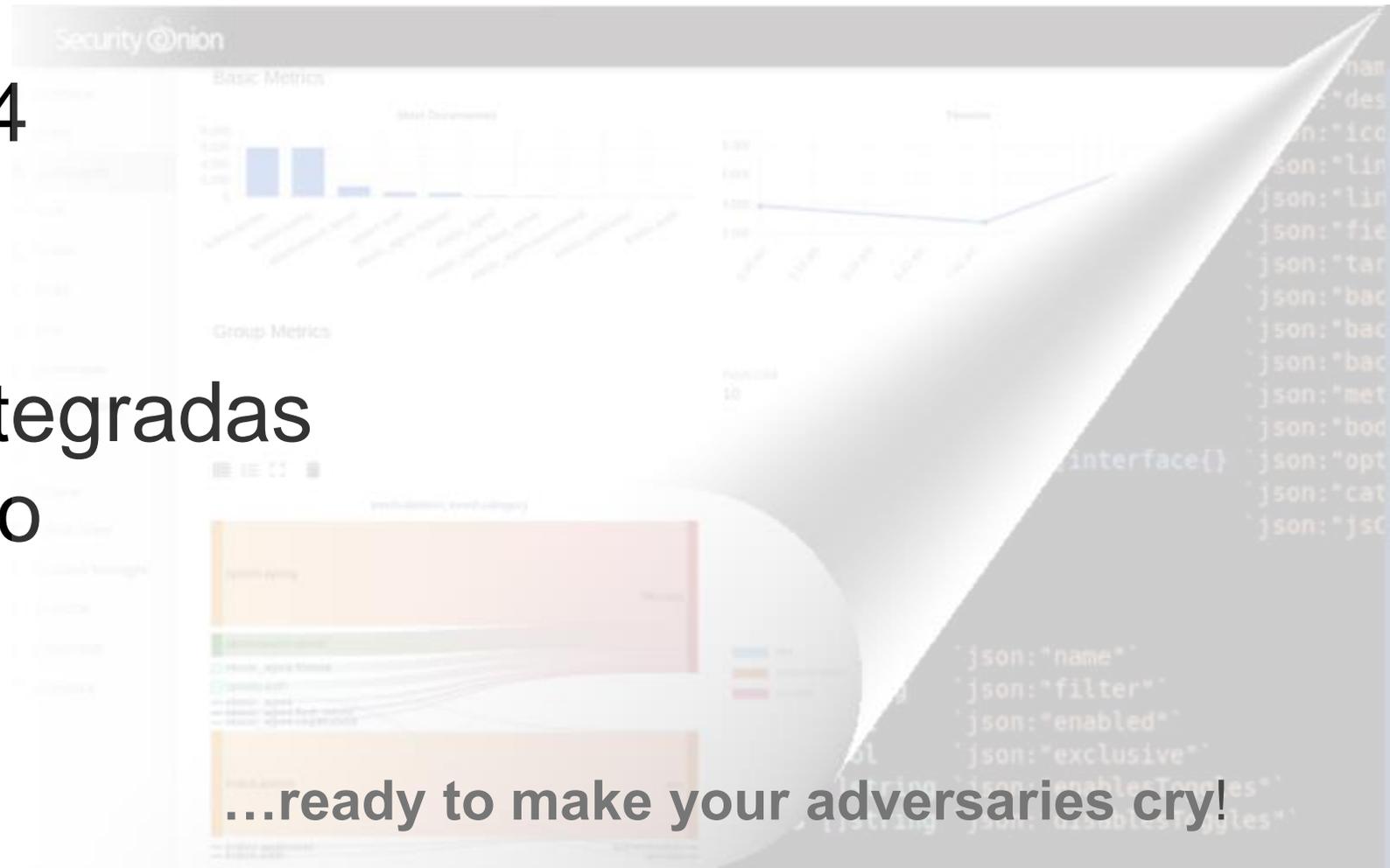
- 19/05/2025 – Cisco Netacad
- 26/05/2025 – Networking
- 02/06/2025 – Ciberseguridad
- 09/06/2025 – Ciencia de datos e IA



2 de junio, 2025

Índice

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



...ready to make your adversaries cry!

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

Security Onion 2.4

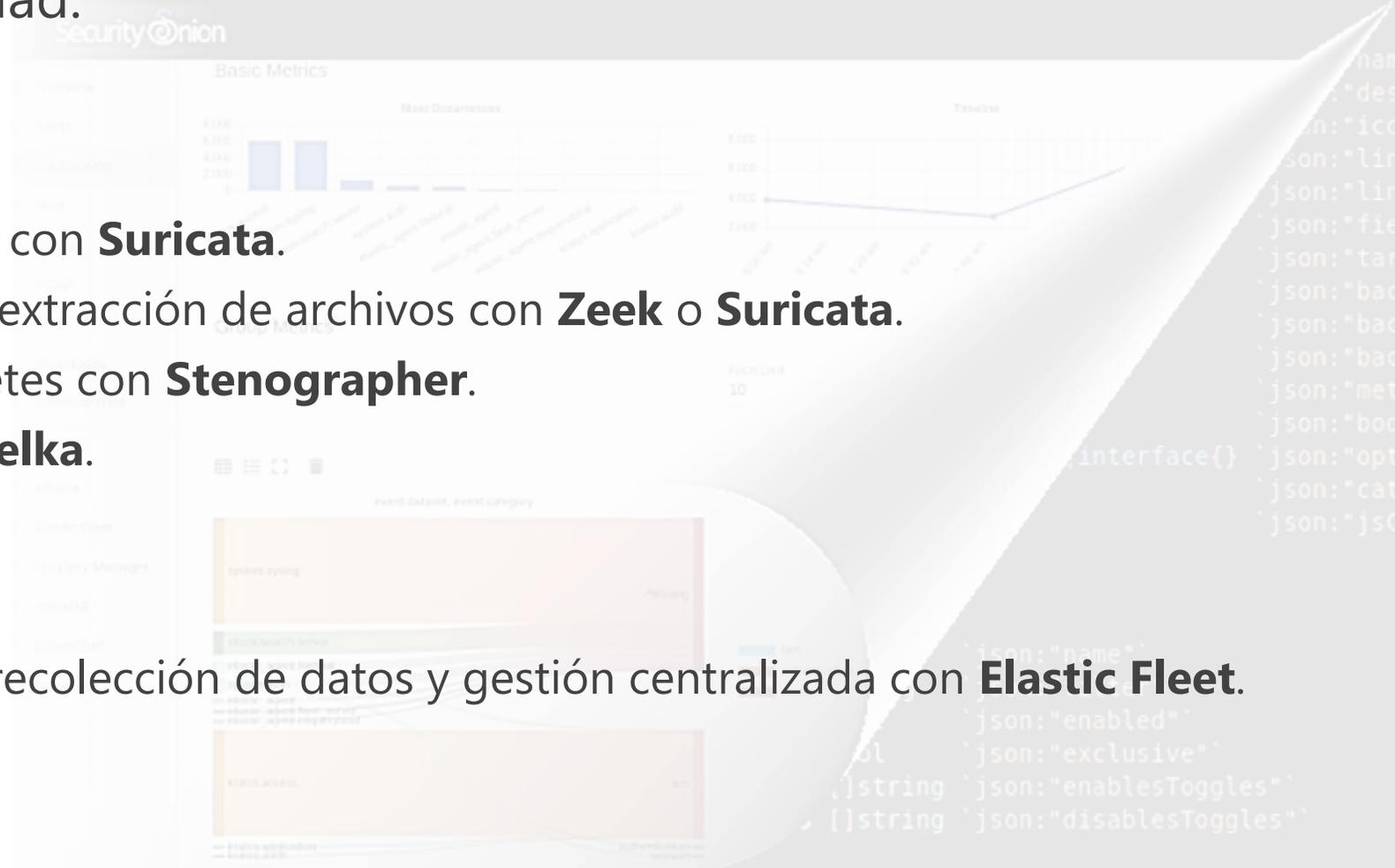
Security Onion es una plataforma gratuita y de código abierto diseñada para defensores de la ciberseguridad.

- **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**.



Security Onion 2.4

- **Gestión de registros y casos:**

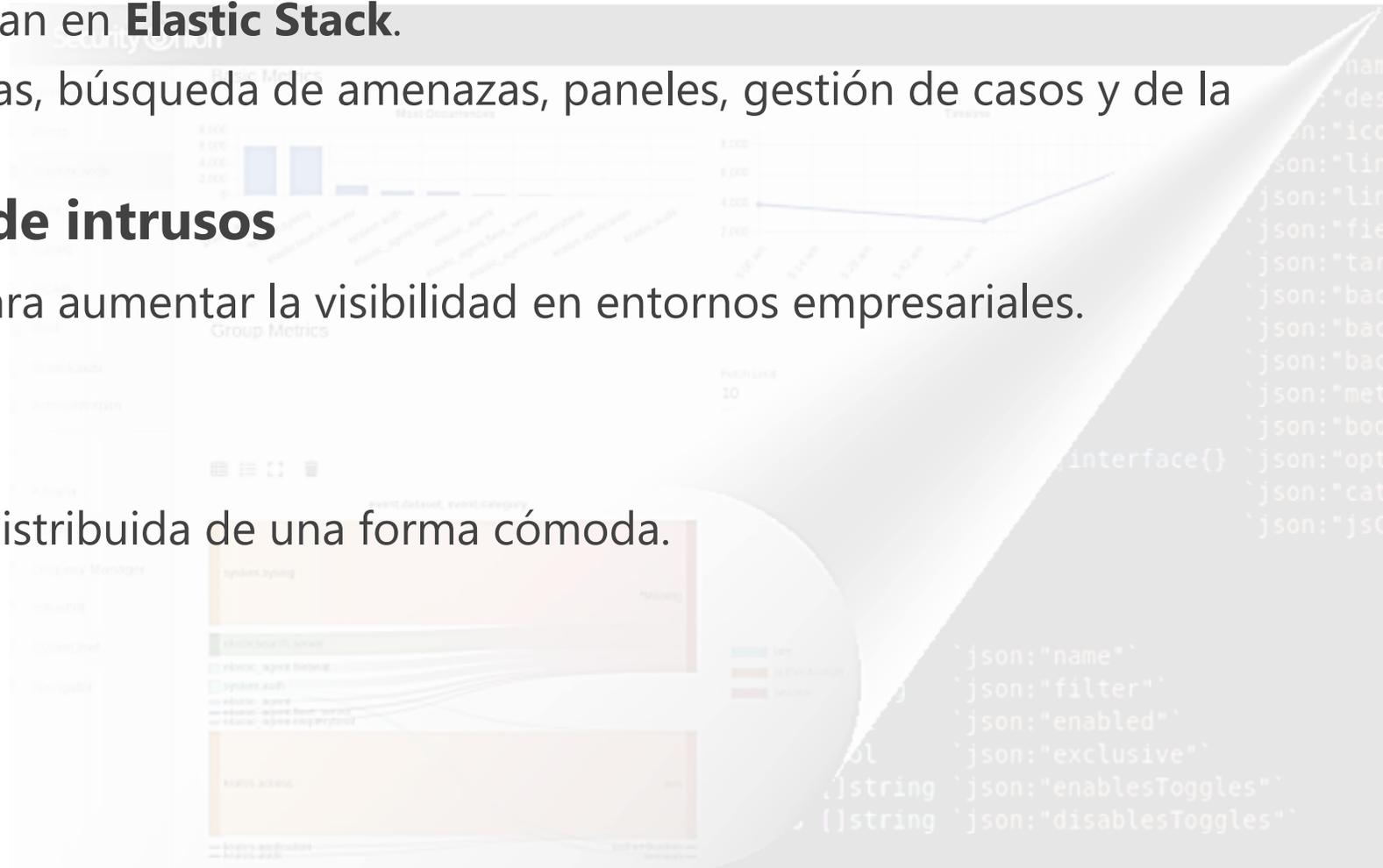
- Todos los registros se integran en **Elastic Stack**.
- Interfaces propias para alertas, búsqueda de amenazas, paneles, gestión de casos y de la red.

- **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.



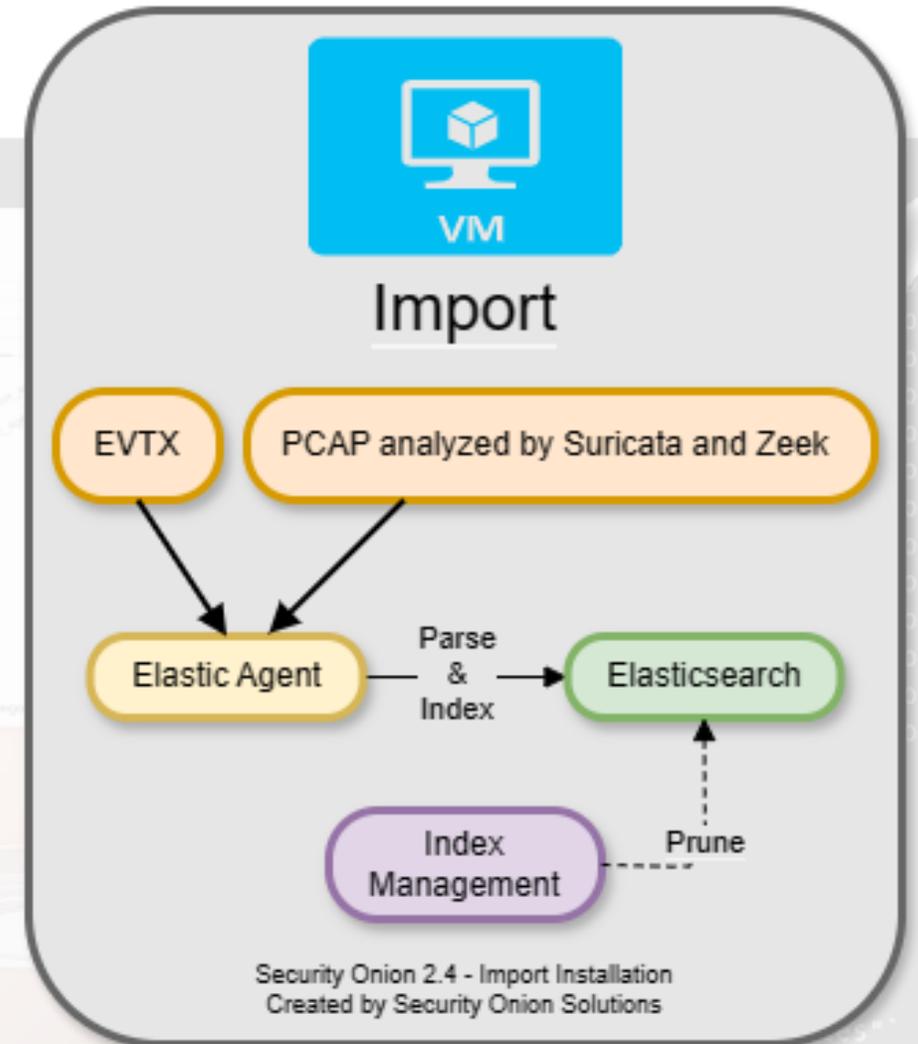
Arquitecturas

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
--------------	---------	------	-------



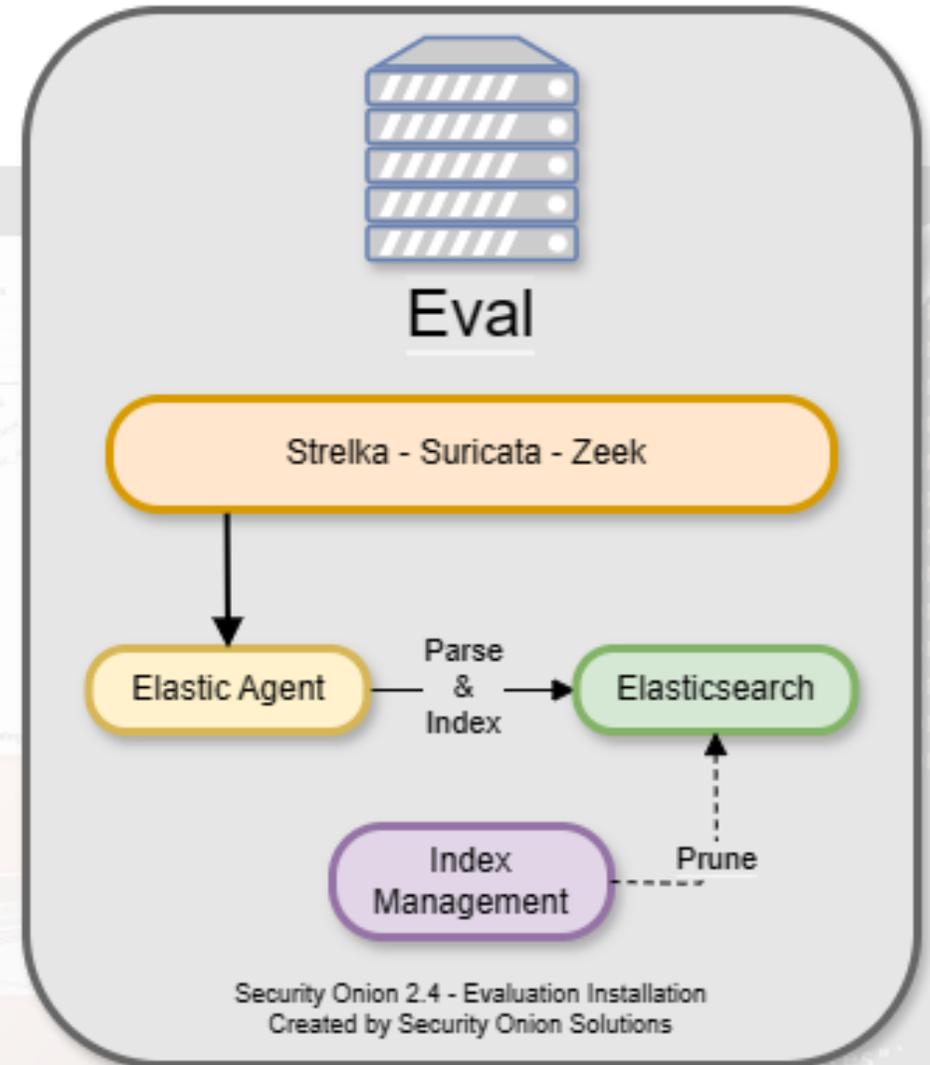
Arquitecturas

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
--------------	---------	-------	-------



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.

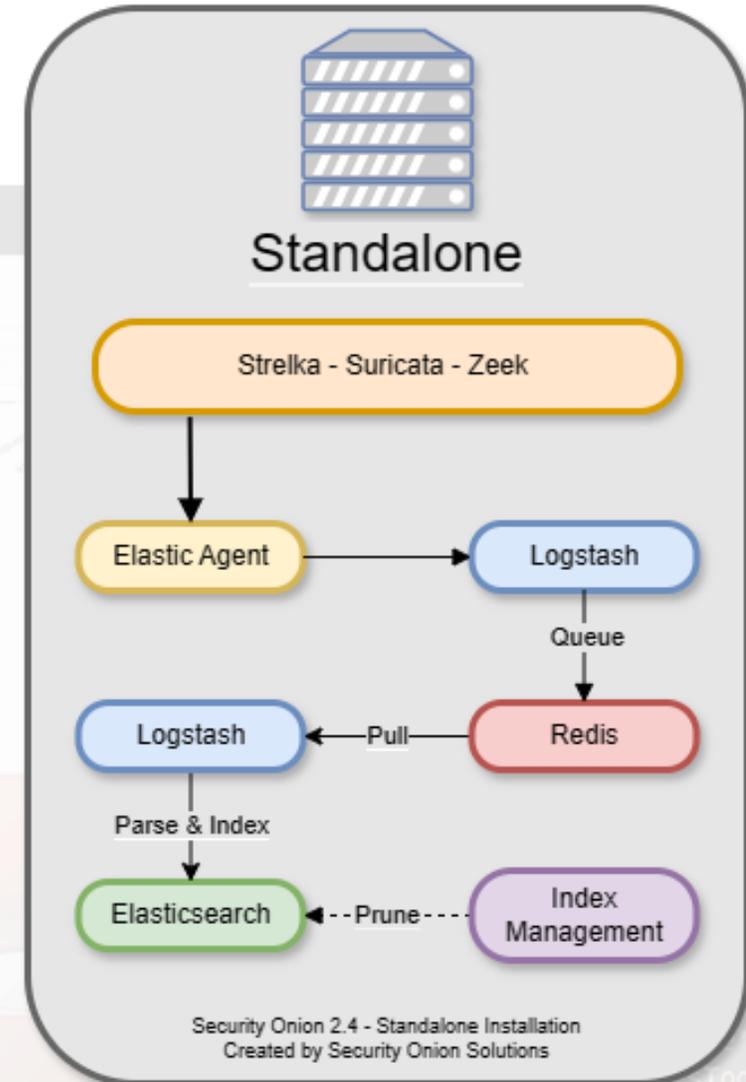
Requisitos:

4 CPUs cores

24GB RAM

200GB

2 NIC



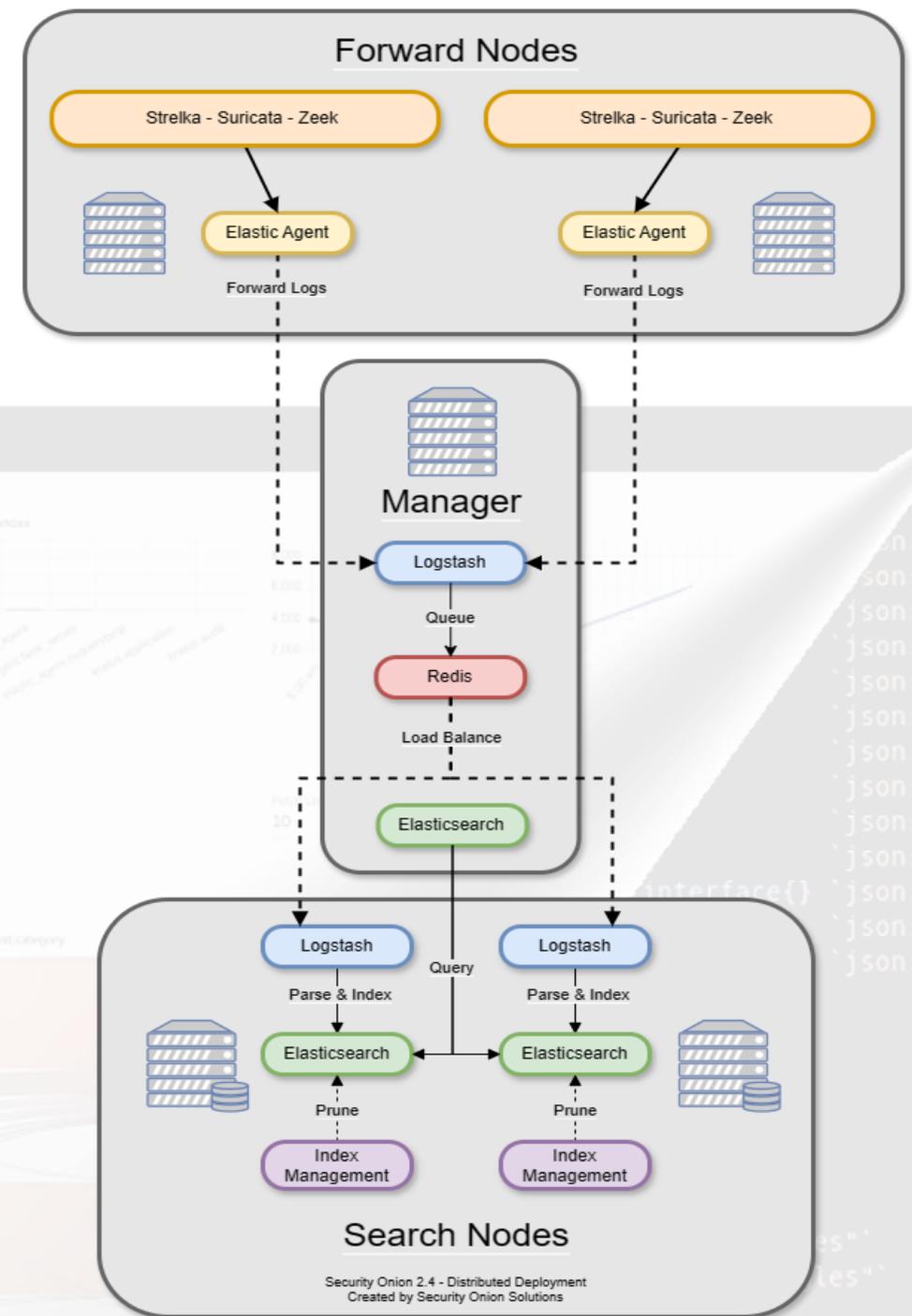
Arquitecturas

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



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.



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.

Count	rule.name	event.module
3	ET DNS Query to a *.top domain - Likely Hostile	suricata
3	ET INFO Observed ZeroSSL SSL/TLS Certificate	suricata
3	ET INFO Packed Executable Download	suricata
3	ET MALWARE Generic AsyncRAT/zgRAT Style SSL Cert	suricata
2	ET INFO External IP Address Lookup Domain (ipify .org) in TLS SNI	suricata
2	ET INFO External IP Lookup Domain (ipify .org) in DNS Lookup	suricata
2	ET INFO HTTP Request to a *.top domain	suricata
2	ET INFO Microsoft Connection Test	suricata
2	ET INFO Windows Powershell User-Agent Usage	suricata
2	ET MALWARE SocGhosh Domain in DNS Lookup (circle .innovatecsportal .com)	suricata
2	ET MALWARE SocGhosh Domain in TLS SNI (circle .innovatecsportal .com)	suricata
1	ET DROP Spamhaus DROP Listed Traffic Inbound group 25	suricata
1	ET EXPLOIT_KIT LandUpdate808 Domain in DNS Lookup (sesraw .com)	suricata
1	ET EXPLOIT_KIT LandUpdate808 Domain in TLS SNI (sesraw .com)	suricata
1	ET HUNTING Request to .TOP Domain with Minimal Headers	suricata
1	ET MALWARE Async RAT CnC Activity (GET)	suricata

Overview

ET INFO Packed Executable Download

Summary

This rule detects the download of a packed executable file over HTTP by identifying specific signatures within the transferred data. It checks for the presence of the "MZ" header and certain strings that are typical of executable files, such as "This program" and "PE\000\000", while ensuring that strings like "data," "text," and "rsrc" are absent within the first 400 bytes.

Status: Enabled

Version: 2.4.150 © 2025 Security Onion Solutions, LLC License:ELv2

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.

The screenshot displays the Security Onion dashboard. On the left is a navigation sidebar with 'Dashboards' highlighted in red. The main area features a Sankey diagram titled 'event.module, event.dataset' showing data flow from 'zeek' to various datasets like 'zeek.conn', 'zeek.dns', and 'zeek.ssl'. Below the diagram are four data tables:

Count	event.dataset
144	zeek.conn
80	zeek.dns
48	zeek.ssl
31	suricata.alert
13	zeek.notice
12	zeek.x509
11	zeek.file
10	zeek.http
4	zeek.software

Count	observer.name
353	secon24

Count	host.name
No data available	

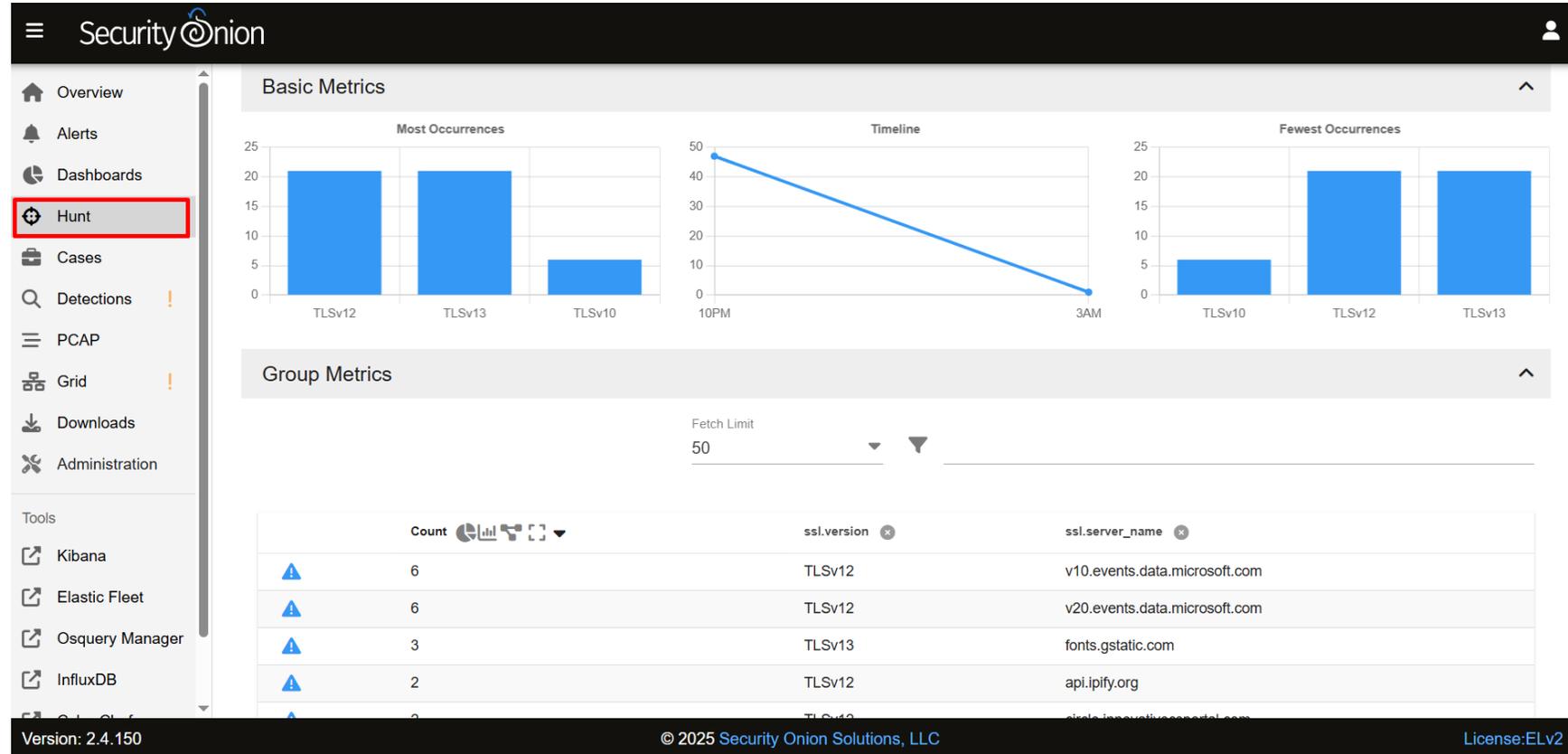
Count	source.ip
332	10.1.28.147
4	86.107.101.93

Count	destination.ip
160	10.1.28.1
13	86.107.101.93

Footer: Version: 2.4.150 | © 2025 Security Onion Solutions, LLC | License:ELV2

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.

Security Onion

Overview
Alerts
Dashboards
Hunt
Cases
Detections
PCAP
Grid
Downloads
Administration

Tools
Kibana
Elastic Fleet
Osquery Manager
InfluxDB

Posible IP Maliciosa

Review escalated event details in the Events tab below. Click here to update this description.

COMMENTS ATTACHMENTS **OBSERVABLES** EVENTS HISTORY

+ ↻

Actions	Created ▲	Updated	Type	Value
> ⚙️ ⚡	May 26, 2025 6:04 PM	May 27, 2025 7:00 PM	ip	147.45.47.98

Items per page: 10 1-1 of 1

Summary

Assignee: admin@casa.local

Status: new

Details

Severity: medium

Priority: 0

TLP: amber

PAP:

Version: 2.4.150 © 2025 Security Onion Solutions, LLC License:ELv2

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.

The screenshot displays the Security Onion web interface. On the left is a navigation sidebar with options like Overview, Alerts, Dashboards, Hunt, Cases, Detections (highlighted with a red box), PCAP, Grid, Downloads, and Administration. The main content area is titled "Detecting Hash Autokey DarkGate" and shows a "DETECTION SOURCE" tab with a YAML rule template. The rule includes a title, ID, status, description, author, logsource, and detection logic. On the right, there are "Operations" and "Details" panels. The "Operations" panel shows the rule is "Status: Enabled" with a toggle switch and buttons for "DUPLICATE" and "DELETE". The "Details" panel shows the "Public Id" and "Severity: High".

```
# This is a Sigma rule template, which uses YAML. Replace all template values with your own values.
# The id (UUIDv4) is pregenerated and can safely be used.
# Click "Convert" to convert the Sigma rule to use Security Onion field mappings within an EQL query
#
# Rule Creation Guide: https://github.com/SigmaHQ/sigma/wiki/Rule-Creation-Guide
# Logsources: https://sigmahq.io/docs/basics/log-sources.html

title: 'Detecting Hash Autokey DarkGate '
id: 268d7e20-8a99-4d9d-9a44-bd3eb06bf1de
status: experimental
description: Detecta MD5 Hashes
author: Alberto Aparicio Vila
logsource:
  product: zeek
  service: file
detection:
  selection:
    event.module: 'zeek'
    event.dataset: 'zeek.file'
    hash.md5: 'e930b05efe23891d19bc354a4209be3e'
  condition: selection
level: high
```

Version: 2.4.150 © 2025 Security Onion Solutions, LLC License:ELv2

Características Integradas

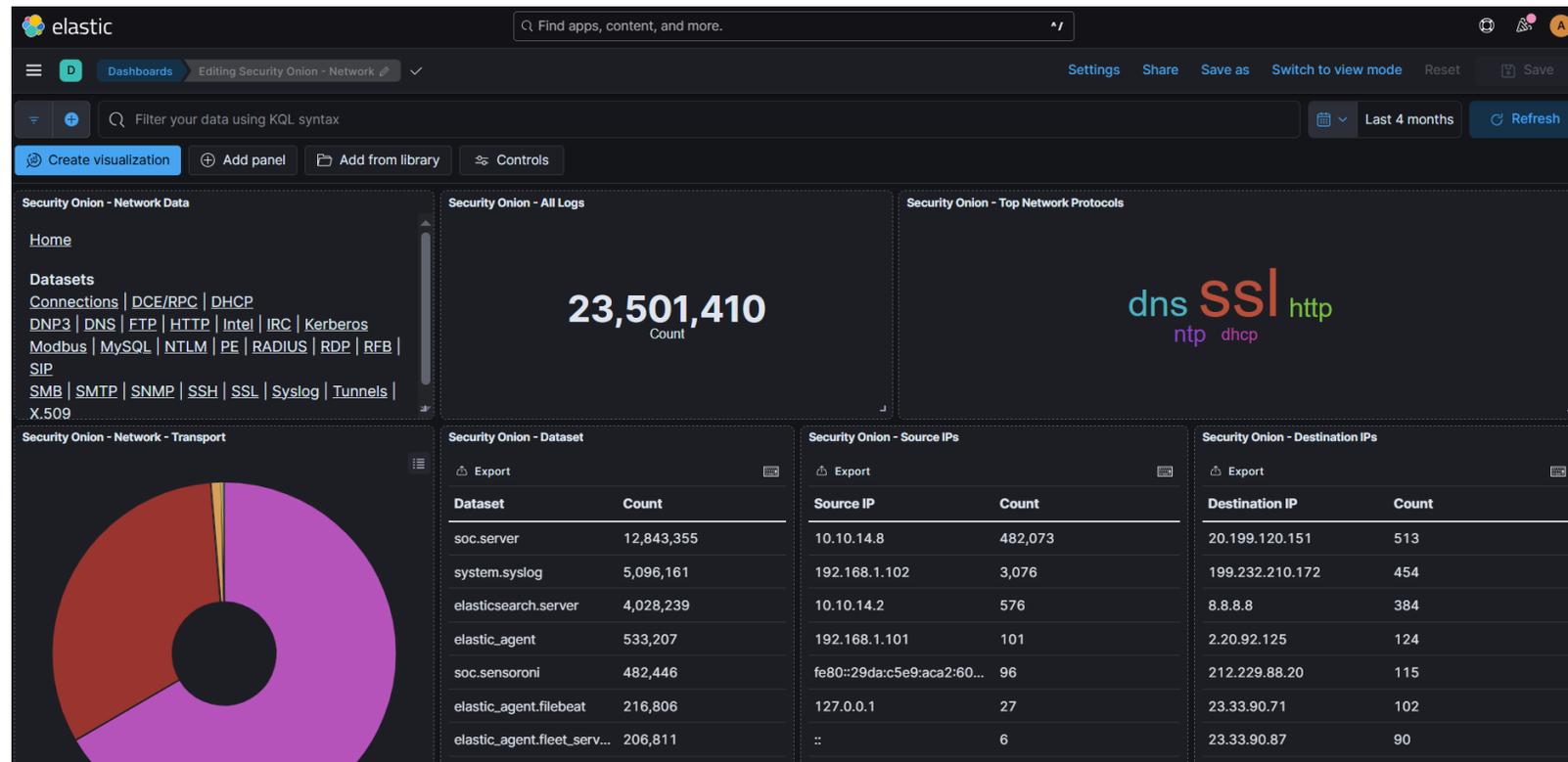
- **PCAP**
- ✓ **Acceso completo a capturas de paquetes (PCAP)** almacenadas por **Stenographer** o **Suricata**.
- ✓ **Dos formas de acceso:**
 - **A través de Alerts, Dashboards o Hunt** usando la acción **PCAP**.
 - **Acceso directo** a la interfaz **PCAP** para búsquedas manuales.

The screenshot displays the Security Onion web interface. On the left, a navigation sidebar includes 'Overview', 'Alerts', 'Dashboards', 'Hunt', 'Cases', 'Detections', 'PCAP' (highlighted with a red box), 'Grid', 'Downloads', and 'Administration'. The main content area shows details for alert #1001, including the source IP 10.3.19.101:53626 and destination IP 103.124.105.78:80. The captured traffic is shown in a hex editor view, displaying an HTTP GET request for /test2 and a 200 OK response with a file attachment named 'test.exe'. The response body contains a DOS batch script. The footer of the interface shows 'Version: 2.4.150', '© 2025 Security Onion Solutions, LLC', and 'License:ELv2'.

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.



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.

The screenshot shows the Elastic Fleet management interface. At the top, there's a search bar and navigation tabs for 'Fleet' and 'Agents'. Below that, the 'Fleet' section is titled 'Centralized management for Elastic Agents.' and includes tabs for 'Agents', 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. There are also buttons for 'Add Fleet Server' and 'Add agent'. A search bar allows filtering by KQL syntax. A status filter shows 4 Healthy agents, 0 Unhealthy, 0 Updating, 0 Offline, 0 Inactive, and 0 Unenrolled. A table lists the agents with columns for Status, Host, Agent policy, CPU, Memory, Last activity, Version, and Actions.

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	FleetServer-secon24	FleetServer_secon24 rev. 10	N/A	N/A	17 seconds ago	8.17.3	...
Healthy	debian12	endpoints-initial rev. 2396	N/A	N/A	5 seconds ago	8.14.3 Upgrade available	...
Healthy	win11	endpoints-initial rev. 2396	N/A	N/A	14 seconds ago	8.14.3 Upgrade available	...
Healthy	secon24	so-grid-nodes_general rev. 15372	N/A	N/A	8 seconds ago	8.17.3 Upgrade available	...

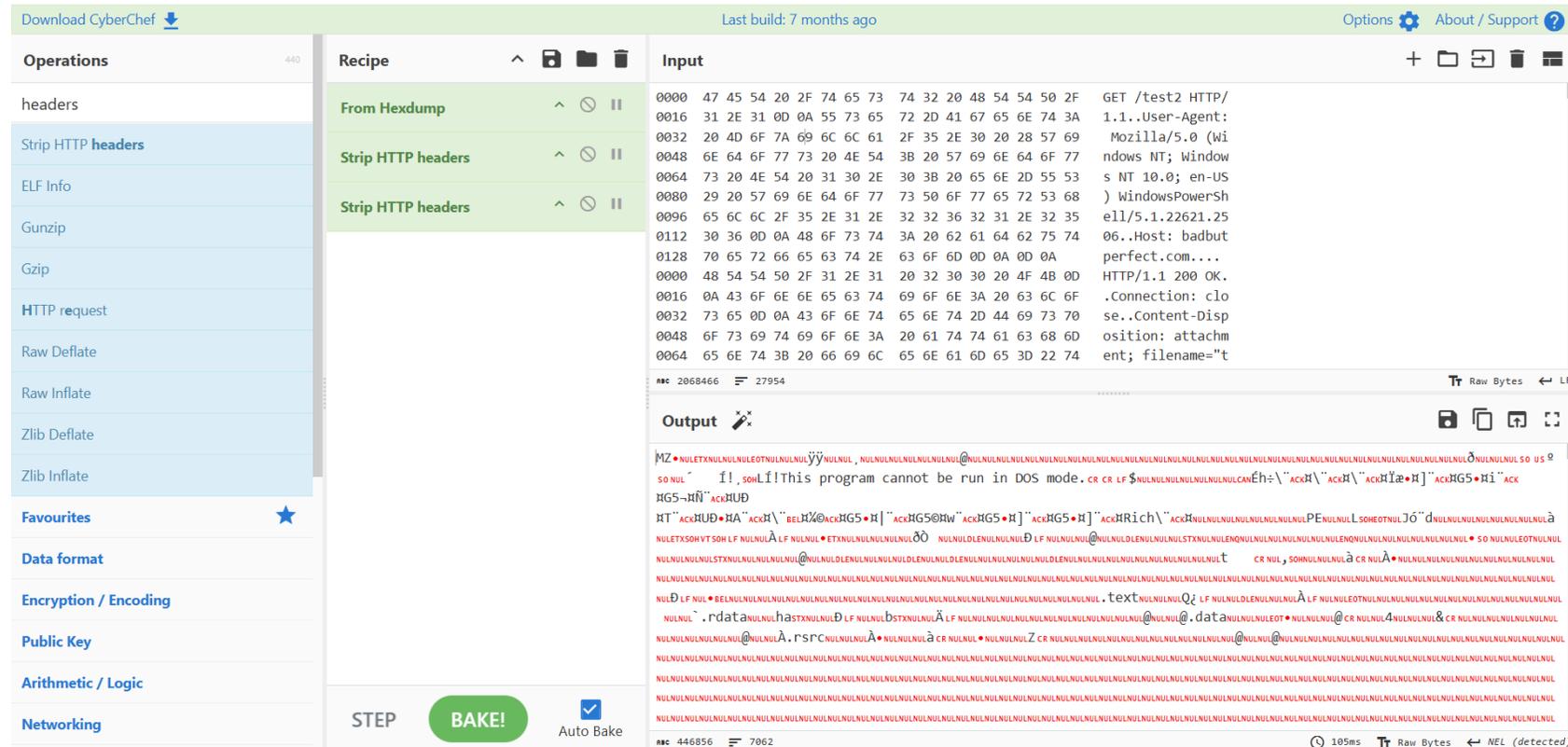
The diagram illustrates the relationship between Elastic Fleet, Elastic Agent, and Elastic Agent Policy. It shows a flow from Elastic Fleet to Elastic Agent, and then to Elastic Agent Policy. A JSON snippet is shown on the right, representing an agent policy configuration:

```
{  
  "name": "  
  "filter": "  
  "enabled": "  
  "exclusive": "  
  "enablesToggles": "  
  "disablesToggles": "
```

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



The screenshot shows the CyberChef interface with the following details:

- Operations List:** headers, Strip HTTP headers, ELF Info, Gunzip, Gzip, HTTP request, Raw Deflate, Raw Inflate, Zlib Deflate, Zlib Inflate, Favourites, Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, Networking.
- Recipe:** From Hexdump, Strip HTTP headers, Strip HTTP headers.
- Input:** Hex dump of an HTTP request:


```
0000 47 45 54 20 2F 74 65 73 74 32 20 48 54 54 50 2F GET /test2 HTTP/
0016 31 2E 31 0D 0A 55 73 65 72 20 41 67 65 6E 74 3A 1.1..User-Agent:
0032 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 Mozilla/5.0 (Wi
0048 6E 64 6F 77 73 20 4E 54 3B 20 57 69 6E 64 6F 77 ndows NT; Window
0064 73 20 4E 54 20 31 30 2E 30 3B 20 65 6E 2D 55 53 s NT 10.0; en-US
0080 29 20 57 69 6E 64 6F 77 73 50 6F 77 65 72 53 68 ) WindowsPowerSh
0096 65 6C 6C 2F 35 2E 31 2E 32 32 36 32 31 2E 32 35 ell/5.1.22621.25
0112 30 36 0D 0A 48 6F 73 74 3A 20 62 61 64 62 75 74 06..Host: badbut
0128 70 65 72 66 65 63 74 2E 63 6F 6D 0D 0A 0D 0A perfect.com....
0000 48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D HTTP/1.1 200 OK.
0016 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F .Connection: clo
0032 73 65 0D 0A 43 6F 6E 74 65 6E 74 2D 44 69 73 70 se..Content-Disp
0048 6F 73 69 74 69 6F 6E 3A 20 61 74 74 61 63 68 6D osition: attachm
0064 65 6E 74 3B 20 66 69 6C 65 6E 61 6D 65 3D 22 74 ent; filename="t
```
- Output:** A large block of redacted text (NUL characters) with a message: "This program cannot be run in DOS mode." and a file path: "C:\WINDOWS\system32\cmd.exe".
- Buttons:** STEP, BAKE!, Auto Bake.

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/>

Detections Coverage - All Detections X Detections Coverage - Sigma X Detections Coverage - Suricata X Alerts (Last 3 Days) X

Selection Controls Layer Controls Technique Controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
11 techniques	11 techniques	21 techniques	14 techniques	36 techniques	16 techniques	28 techniques	9 techniques	15 techniques	18 techniques	8 techniques	15 techniques
Content Injection	Command and Scripting Interpreter (0/7)	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Adversary-in-the-Middle (0/3)	Account Discovery (0/3)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/5)	Automated Exfiltration (0/0)	Account Access Removal
Drive-by Compromise	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/1)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits (0/0)	Data Destruction (0/0)
Exploit Public-Facing Application	Input Injection	Boot or Logon Autostart Execution (0/10)	Debugger Evasion	Debugger Evasion	Credentials from Password Stores (0/3)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Initialization Scripts (0/2)	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (0/1)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel (0/2)	Data Manipulation (0/3)
Hardware Additions	Native API	Compromise Host Software Binary	Direct Volume Access	Direct Volume Access	Forced Authentication	Device Driver Discovery	Remote Services (0/5)	Browser Session Hijacking	Data Obfuscation (0/3)	Defacement (0/2)	Defacement (0/2)
Phishing (0/4)	Scheduled Task/Job (0/2)	Create Account (0/2)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Forge Web Credentials (0/2)	File and Directory Discovery	Replication Through Removable Media	Dynamic Resolution (0/3)	Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	Email Bombing (0/2)
Replication Through Removable Media	Shared Modules	Create or Modify System Process (0/1)	Email Spoofing	Email Spoofing	Input Capture (0/4)	Group Policy Discovery	Software Deployment Tools	Encrypted Channel (0/2)	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Supply Chain Compromise (0/3)	System Services (0/1)	Event Triggered Execution (0/12)	Execution Guardrails (0/2)	Execution Guardrails (0/2)	Modify Authentication Process (0/6)	Log Enumeration	Taint Shared Content	Data from Information Repositories (0/1)	Hide Infrastructure	Exfiltration Over Web Service (0/4)	Financial Theft (0/1)
Trusted Relationship	User Execution (0/3)	Exclusive Control	File and Directory Permissions Modification (0/1)	File and Directory Permissions Modification (0/1)	Multi-Factor Authentication Interception	Network Service Discovery	Use Alternate Authentication Material (0/2)	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption (0/1)
Valid Accounts (0/3)	Windows Management Instrumentation	External Remote Services	Hide Artifacts (0/11)	Hide Artifacts (0/11)	Multi-Factor Authentication Request Generation	Network Share Discovery	Data from Network Shared Drive	Multi-Stage Channels	Non-Application Layer Protocol	Inhibit System Recovery (0/2)	Firmware Corruption (0/1)
Wi-Fi Networks	Hijack Execution Flow (0/10)	Hijack Execution Flow (0/10)	Hijack Execution Flow (0/10)	Hijack Execution Flow (0/10)	Network Sniffing	Network Sniffing	Data from Removable Media	Multi-Stage Channels	Non-Application Layer Protocol	Network Denial of Service (0/2)	Resource Hijacking (0/2)
			Impair Defenses (0/8)	Impair Defenses (0/8)						Service Stop	Service Stop



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>

The image shows a screenshot of the Security Onion Pro dashboard. The dashboard includes sections for 'Basic Metrics', 'Group Metrics', and 'App Use'. A large, semi-transparent white box is overlaid on the dashboard, containing the text 'Security Onion Pro' in a large, bold font, followed by 'Powerful features and personalized support offered for enterprise customers!'. The background of the dashboard shows various charts and data visualizations, including a bar chart for 'Basic Metrics' and a line chart for 'Group Metrics'. The text 'Security Onion Pro' is prominently displayed in the center of the overlay.

