Detección y Respuesta a Incidentes

SESIÓN 01 – Presentación y Primer Contacto (SOC Básico)

Carlos Melero 2026

Monitorización

Reciben flujos de datos de toda la empresa (firewalls, EPP, servidores, correos).

Detección

Identifican anomalías o ataques en tiempo real.

Análisis

Determinan si una alerta es un ataque real o un 'falso positivo'.

Respuesta

Si hay un incidente, actúan para contenerlo (por ejemplo, aislando un PC infectado de la red desde su consola central).

PERSONAS

Analistas (Tier 1, 2, 3).
Investigación y respuesta.

PROCESOS

Protocolos de actuación
(Playbooks) para incidentes.

TECNOLOGÍA (SIEM)

Recolección y correlación
de logs en una plataforma.

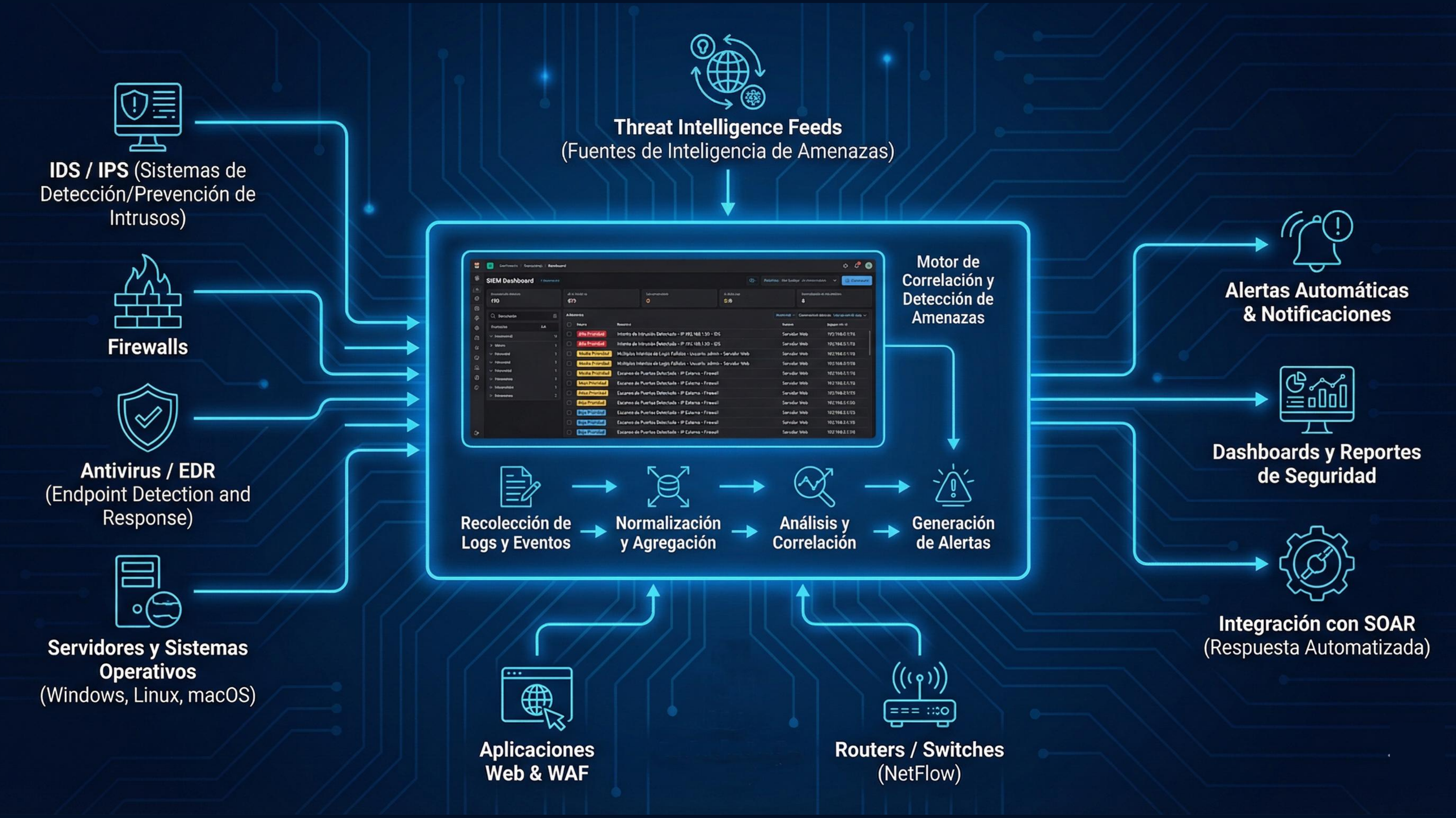
> LOGIN EXITO. OPERACIONES MEDDATA // NIVEL DE CONFIDENCIALIDAD: INTERNO

[SYS] Kernel loaded...
[NET] eth0 up, link established
[SEC] Audit daemon started
[INIT] Loading SOC services...

Visibilidad en la Oscuridad

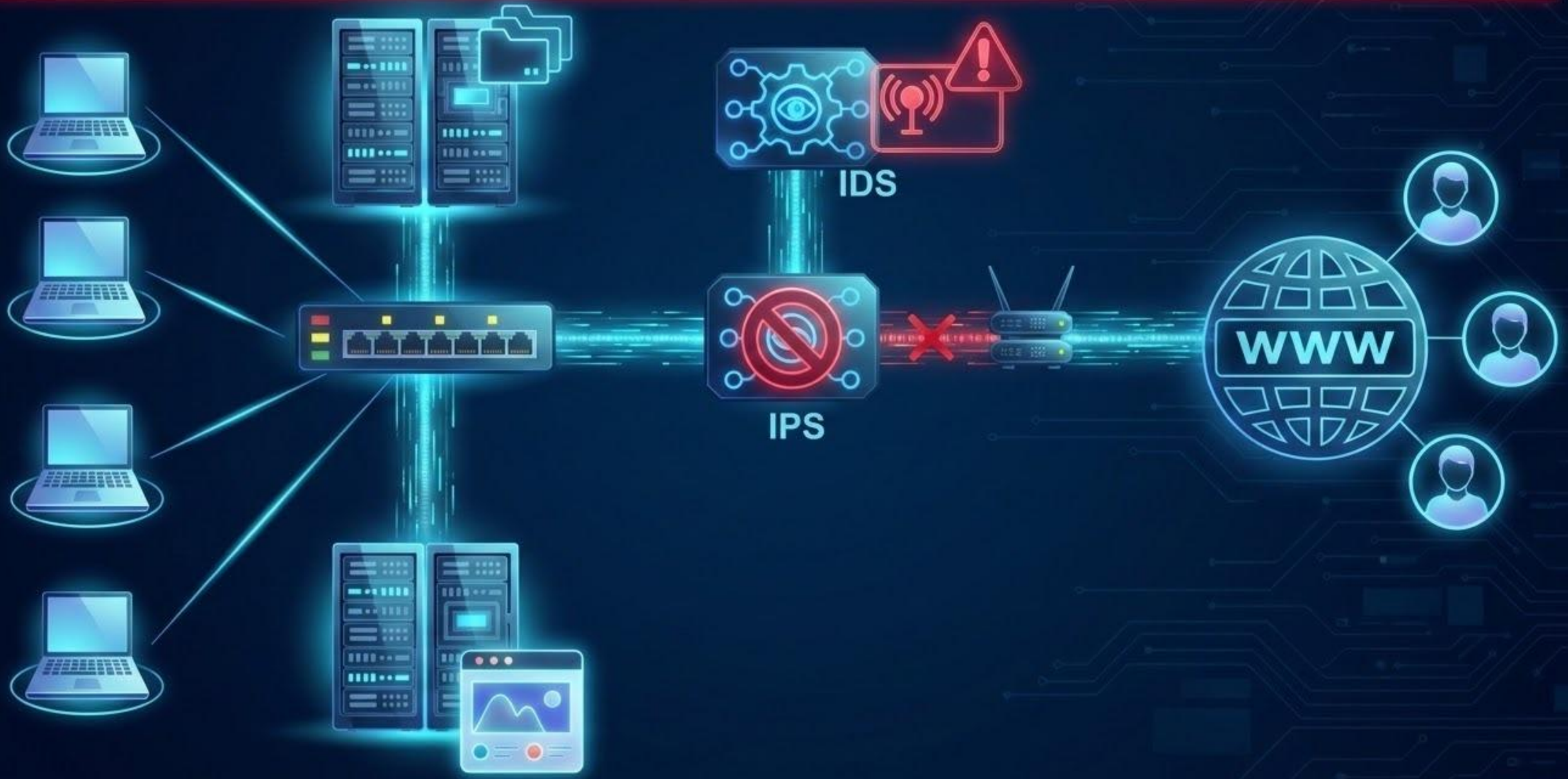
Herramientas, Monitoreo y Correlación de Eventos en el SOC

[AUTH] User MedData_OP verified
[NET] Connecting to central log server...
[SYS] Initializing data ingestion pipelines...
[SEC] Threat intelligence feed updated
[MON] Real-time dashboards loading...


Threat Intelligence Feeds
(Fuentes de Inteligencia de Amenazas)
IDS / IPS (Sistemas de Detección/Prevención de Intrusos)
Firewalls
Antivirus / EDR
(Endpoint Detection and Response)
Servidores y Sistemas Operativos
(Windows, Linux, macOS)
SIEM Deshboard
Motor de Correlación y Detección de Amenazas
Recolección de Logs y Eventos
Normalización y Agregación
Análisis y Correlación
Generación de Alertas
Alertas Automáticas & Notificaciones
Dashboards y Reportes de Seguridad
Integración con SOAR
(Respuesta Automatizada)
Aplicaciones Web & WAF
Routers / Switches
(NetFlow)

Timestamp	event.dataset	source.ip	source.port	destination.ip	destination
2026-04-17 14:40:30.807 +02:00	zeek.conn	10.60.10.22	55628	216.239.36.223	443
2026-04-17 15:15:37.784 +02:00	zeek.conn	10.60.40.10	5055	10.60.10.23	60058
2026-04-17 15:32:50.165 +02:00	zeek.conn	10.60.10.23	60107	10.60.40.10	5055
2026-04-17 15:33:16.167 +02:00	zeek.conn	10.60.20.20	62622	10.60.40.10	5055
2026-04-17 15:33:36.974 +02:00	zeek.conn	10.60.20.20	62623	10.60.20.10	135
2026-04-17 15:34:31.942 +02:00	zeek.conn	10.60.10.22	54651	10.60.40.10	5055
2026-04-17 15:35:57.468 +02:00	zeek.conn	10.60.10.22	54654	10.60.40.10	5055
2026-04-17 15:35:58.658 +02:00	zeek.conn	10.60.10.23	60114	10.60.40.10	5055
2026-04-17 15:36:01.454 +02:00	zeek.conn	10.60.10.23	60115	10.60.40.10	5055
2026-04-17 15:36:01.980 +02:00	zeek.conn	10.60.20.10	51431	10.60.40.10	5055
2026-04-17 15:36:39.156 +02:00	zeek.conn	10.60.10.21	50821	10.60.40.10	5055
2026-04-17 15:36:56.330 +02:00	zeek.conn	10.60.10.21	50822	10.60.40.10	5055
2026-04-17 15:37:24.476 +02:00	zeek.conn	10.60.40.10	8220	10.60.20.10	51436
2026-04-17 15:37:54.305 +02:00	zeek.conn	10.60.20.20	62638	10.60.40.10	8220
2026-04-17 15:37:55.098 +02:00	zeek.conn	10.60.10.21	50824	10.60.40.10	8220
2026-04-17 15:38:07.506 +02:00	zeek.conn	10.60.10.22	54662	10.60.40.10	5055
2026-04-17 15:38:26.205 +02:00	zeek.conn	10.60.10.22	54664	10.60.40.10	5055
2026-04-17 15:38:31.210 +02:00	zeek.conn	10.60.20.30	36802	10.60.20.10	53
2026-04-17 15:38:31.210 +02:00	zeek.conn	10.60.20.30	42183	10.60.20.10	53
2026-04-17 15:38:33.624 +02:00	zeek.conn	10.60.20.20	55275	10.60.20.10	53
2026-04-17 15:38:35.237 +02:00	zeek.conn	10.60.40.10	5055	10.60.10.23	60117
2026-04-17 15:38:35.510 +02:00	zeek.conn	10.60.10.21	57635	10.60.20.10	53
2026-04-17 15:38:35.513 +02:00	zeek.conn	10.60.10.21	50825	72.154.7.108	443

IDS / IPS



BASADO EN FIRMAS - SURICATA

Regla de Detección

```
alert
tcp any any -> any 80
(
msg:"Potential web server attack";
flow:established,to_server;
content:"/etc/passwd";
)
```

BASADO EN FIRMAS - YARA

Yet
Another
Recursive
Acronym

YARA

Copy View Analyze

```
rule Malware_Sencillo
{
meta: description = “Detecta un malware básico por un texto”
strings: $secreto = “Has sido infectado”
ascii wide
condition: $secreto }
```

BASADO EN FIRMAS - SIGMA

Sigma Rule Editor

Copy View Analyze

```
title: Whoami.exe
description: Detecta la ejecución de whoami.exe
logsource: category: process_creation # Tipo de evento que buscamos: creación de un proceso
product: windows # Sistema operativo del que vienen los logs
detection: selection: Image|endswith: '\whoami.exe' # Buscar si el nombre del ejecutable termina en '\whoami.exe' condition: selection
```

BASADO EN ANOMALÍAS

Línea base

Establecimiento del comportamiento normal

Monitorización

Supervisión continua del tráfico y sistemas

Detección

Identificación de desviaciones y amenazas

Aviso / intervención

Notificación y respuesta automática

BASADO EN ANOMALÍAS

- Línea base
- Monitorización
- Detección
- Aviso / intervención

Conexión anómala

El 10 de octubre a las 10:26 se produjo un pico de alertas inusual por tráfico entre 1 8 y 3 2. Se enviaron 500MB y recibieron 30MB. La conexión duró 2,5 horas.

En un primer análisis, parece que se subieron 500Mb de datos a un servidor Amazon.

Recomendación y acciones

Revisar si esta transferencia estaba autorizada.

Lota ID	Tima	Pico	Recibieron	Duró hora	Amazon
	1 10:26	500MB	30MB	2,5	17 Sep

ENFOQUES DE DETECCIÓN EN EL SOC

[SOC_PROFILE]

Enfoques de Detección en un Security Operations Center (SOC)

Dirigida a analistas de SOC

Enfoques de Detección: Visión General

[FIRMA]

[QUÉ BUSCA]
Patrones exactos conocidos

[DETECCIÓN]
Detecta bien amenazas conocidas

[DEBILIDAD]
No ve lo nuevo

[HEURÍSTICA]

[QUÉ BUSCA]
Rasgos sospechosos

[DETECCIÓN]
Detecta variantes y artefactos dudosos

[DEBILIDAD]
Más falsos positivos

[COMPORTAMIENTO]

[QUÉ BUSCA]
Acciones y contexto

[DETECCIÓN]
Detecta TTPs, abuso y amenazas nuevas

[DEBILIDAD]
Más complejidad y tuning

DETECCIÓN POR FIRMA

[DEFINICIÓN_Y_TIPOS]

Busca patrones conocidos y exactos.
Idea central: "Si veo esto exacto, es malicioso".

Tipos de firma:

- Hash de malware
- Cadena concreta en un archivo
- Regla YARA
- IP o dominio malicioso conocido
- Secuencia de eventos asociada a un ataque

[ANÁLISIS]

Ventajas

- Muy precisa cuando la firma es buena
- Baja tasa de falsos positivos
- Fácil de explicar y de operar

Limitaciones

- Solo detecta lo ya conocido
- Cambios pequeños pueden evadirla
- Requiere actualización constante

[APLICACIÓN_Y_EJEMPLOS]

Cuándo funciona mejor:

Malware conocido, campañas repetidas, IoCs confirmados, detección rápida y concreta.

Ejemplos:

Antivirus detecta hash de ransomware catalogada

IDS detecta exploit de regla conocida

DETECCIÓN POR FIRMA: EJEMPLO

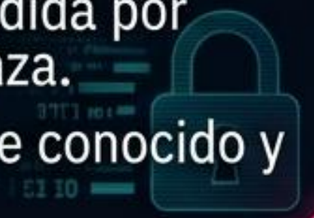
[HERRAMIENTA: SURICATA]

Herramienta: Suricata

```
alert http $HOME_NET any ->
$EXTERNAL_NET any
  (msg:"ET MALWARE Ransomware
LockBit User-Agent";
  flow:established,to_server;
  http.user_agent;
  content:"LockBit";
  sid:1000001; rev:1;)
```

[ANÁLISIS DE LA REGLA]

- Esta regla alerta si un host interno realiza una petición HTTP al exterior y la cabecera User-Agent contiene exactamente la cadena “LockBit”.
- Se basa en detectar un artefacto de una amenaza ya catalogada.
- Es una regla muy precisa y con baja tasa de falsos positivos.
- [LIMITACIÓN TÉCNICA] Sin embargo, si el malware cambia su User-Agent por uno legítimo, esta firma será evadida por completo y no verá la amenaza.
- Funciona mejor para malware conocido y campañas repetidas.



DETECCIÓN HEURÍSTICA

[CONCEPTO CLAVE]

No es idéntico a algo conocido, pero se parece lo suficiente como para levantar alerta.

[CÓMO FUNCIONA] JetBrains Mono

IDENTIFICA INDICIOS SOSPECHOSOS

- Atributos y estructura anómala
- Empaquetado y ofuscación
- Combinaciones raras de APIs
- Patrones parcialmente coincidentes

[CASO DE USO Y VENTAJAS]

Macro de Office + PowerShell
→ Puntuación ALTA

[PUNTOS FUERTES]

- Detecta nuevas variantes de amenazas
- Más flexible que las firmas tradicionales
- Efectivo contra ofuscación básica

[DESAFÍOS Y MEJOR USO]

[LIMITACIONES]

- Tasa de FALSOS POSITIVOS más alta
- Certeza a veces opaca (parece malo)

[MEJOR APLICACIÓN]

- Variantes de malware
- Documentos con rasgos sospechosos
- Casos sin IoCs sutiles

Detección Heurística: ejemplo

[DETECTION_FRAMEWORK]

Herramienta: YARA (aplicado a heurística estructural de archivos)

Ejemplo de regla:

[ANÁLISIS_DETECCION]

En este caso, no buscamos un hash asociado a un ataque. Analizamos atributos del archivo y macros sospechosas. La regla clasifica el archivo como sospechoso porque cumple varias condiciones: es un documento de Office, tiene rutinas de autoejecución y contiene cadenas relacionadas con PowerShell o CMD.
Este enfoque es más flexible que la firma y detecta variantes nuevas. Su debilidad principal es que genera más falsos positivos; si en la empresa los administradores usan macros que legítimamente llaman a PowerShell, esta regla generará ruido.

[YARA_RULE_DEFINITION]

Code snippet

```
rule Heuristica_Documento_Sospechoso {
    meta:
        description = "Detecta documentos Office
con macros que llaman a intérpretes de comandos"

    strings:
        $magic = { D0 CF 11 E0 A1 B1 1A E1 } //
Firma cabecera Office
        $macro1 = "AutoOpen" ascii wide nocase
        $macro2 = "Document_Open" ascii wide nocase
        $sus1 = "powershell.exe" ascii wide nocase
        $sus2 = "cmd.exe" ascii wide nocase
    condition:
        $magic at 0 and (1 of ($macro*)) and (1 of
($sus*))
}
```

Detección Basada en Comportamiento

Observa lo que hace un usuario, proceso, host o cuenta, no cómo se ve. Idea central: “Aunque no reconozca el artefacto, su actividad encaja con un patrón de ataque o se desvía de la normalidad”.

[FUENTES Y TELEMETRÍA]

- Secuencia de eventos y procesos.
- Actividad de red y cambios en ficheros.
- Uso de credenciales y desviaciones.
- Analítica UEBA / EDR / XDR.

[EJEMPLOS DE COMPORTAMIENTO]

- winword.exe → powershell.exe → descarga → persistencia.
- Usuario inusual (país, acceso, descarga masiva).
- Cifrado masivo de archivos.

[VENTAJAS CLAVE]

- Útil contra amenazas nuevas, fileless y living-off-the-land.
- Difícil de evadir.
- Detecta etapas completas de intrusión, no solo artefactos.

[LIMITACIONES]

- Complejo de diseñar y afinar.
- Riesgo de ruido si la línea base es incorrecta.
- Requiere telemetría rica y contexto.
- Detecta más tarde que firmas.

Cuándo Funciona Mejor: Ataques sin malware conocido, abuso de herramientas legítimas, movimiento lateral, persistencia, exfiltración y ransomware.

DETECCIÓN BASADA EN COMPORTAMIENTO: EJEMPLO

[EJEMPLO_REGLA_SIGMA_EDR]

YAML

```yaml
title: Proceso hijo sospechoso desde Microsoft Word
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentImage|endswith: '\WINWORD.EXE'
        Image|endswith:
            - '\powershell.exe'
            - '\cmd.exe'
            - '\wscript.exe'
    condition: selection
```

[ANÁLISIS_Y_SIGNIFICADO]

Esta regla evalúa la relación entre procesos y la secuencia de eventos.

Detecta el comportamiento en el que winword.exe lanza powershell.exe.

COMPORTAMIENTO SOSPECHOSO

No importa si el archivo de Word original es indetectable por el antivirus; la acción que realiza activa la alerta. Este enfoque es

crítico para detectar el abuso de herramientas legítimas (living-off-the-land) y ataques sin malware conocido.

ENFOQUES DE DETECCIÓN EN EL SOC

YARA: Archivos

Firma y Patrón: Identifica familias de malware mediante cadenas de texto, expresiones regulares o secuencias hexadecimales en el código.

Heurística: Detecta amenazas desconocidas analizando la estructura y capacidades del archivo (ej. un PDF con código ejecutable oculto).

SIGMA: Eventos

Comportamiento: Su punto fuerte. Detecta TTPs (Tácticas y Técnicas) analizando logs de eventos (ej. un proceso legítimo realizando acciones inusuales).

Firma y Patrón: Busca indicadores específicos (IOCs) como nombres de procesos maliciosos o argumentos de comando sospechosos registrados en los logs.

SURICATA: Red

Firma y Patrón: Filtra el tráfico buscando huellas exactas de ataques conocidos en los payloads de los paquetes.

Heurística y Comportamiento: Identifica anomalías de protocolo (tráfico mal formado) y patrones de actividad sospechosa en la red, como escaneos de puertos o exfiltración de datos.

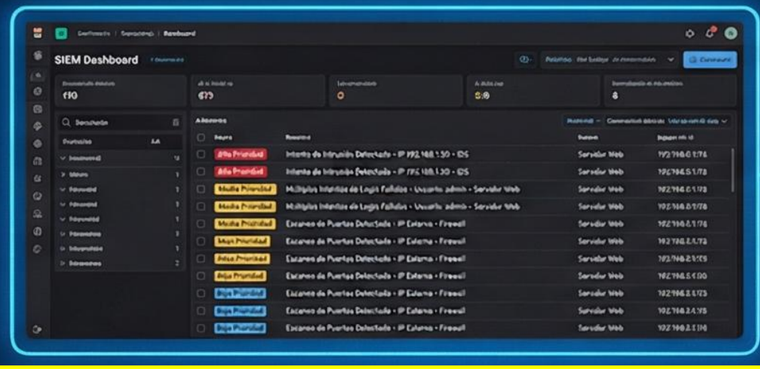
Threat Intelligence Feeds
(Fuentes de Inteligencia de Amenazas)

IDS / IPS (Sistemas de Detección/Prevención de Intrusos)

Firewalls

Antivirus / EDR
(Endpoint Detection and Response)

Servidores y Sistemas Operativos
(Windows, Linux, macOS)



Motor de Correlación y Detección de Amenazas

Recolección de Logs y Eventos → Normalización y Agregación → Análisis y Correlación → Generación de Alertas

Alertas Automáticas & Notificaciones

Dashboards y Reportes de Seguridad

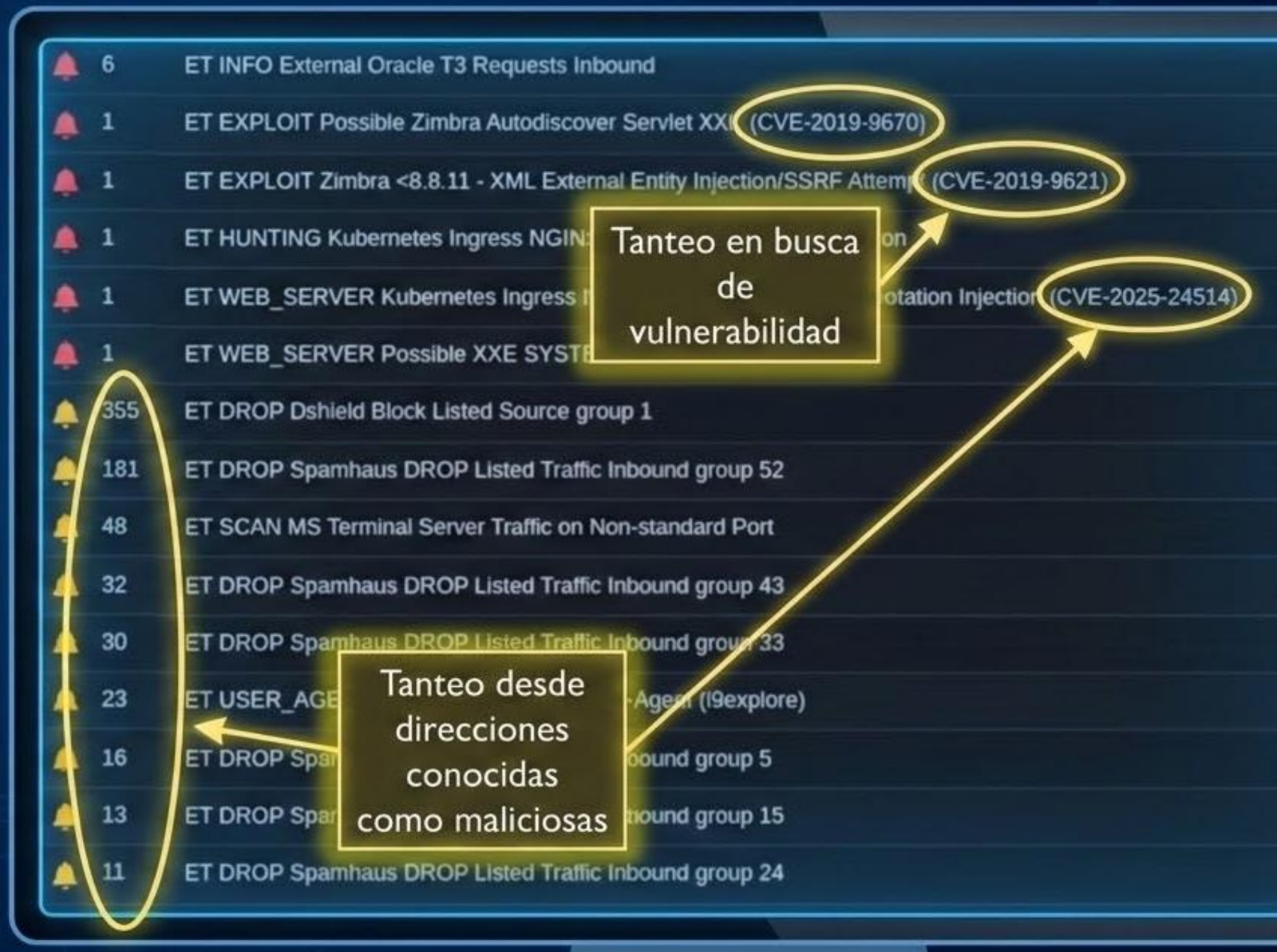
Integración con SOAR
(Respuesta Automatizada)

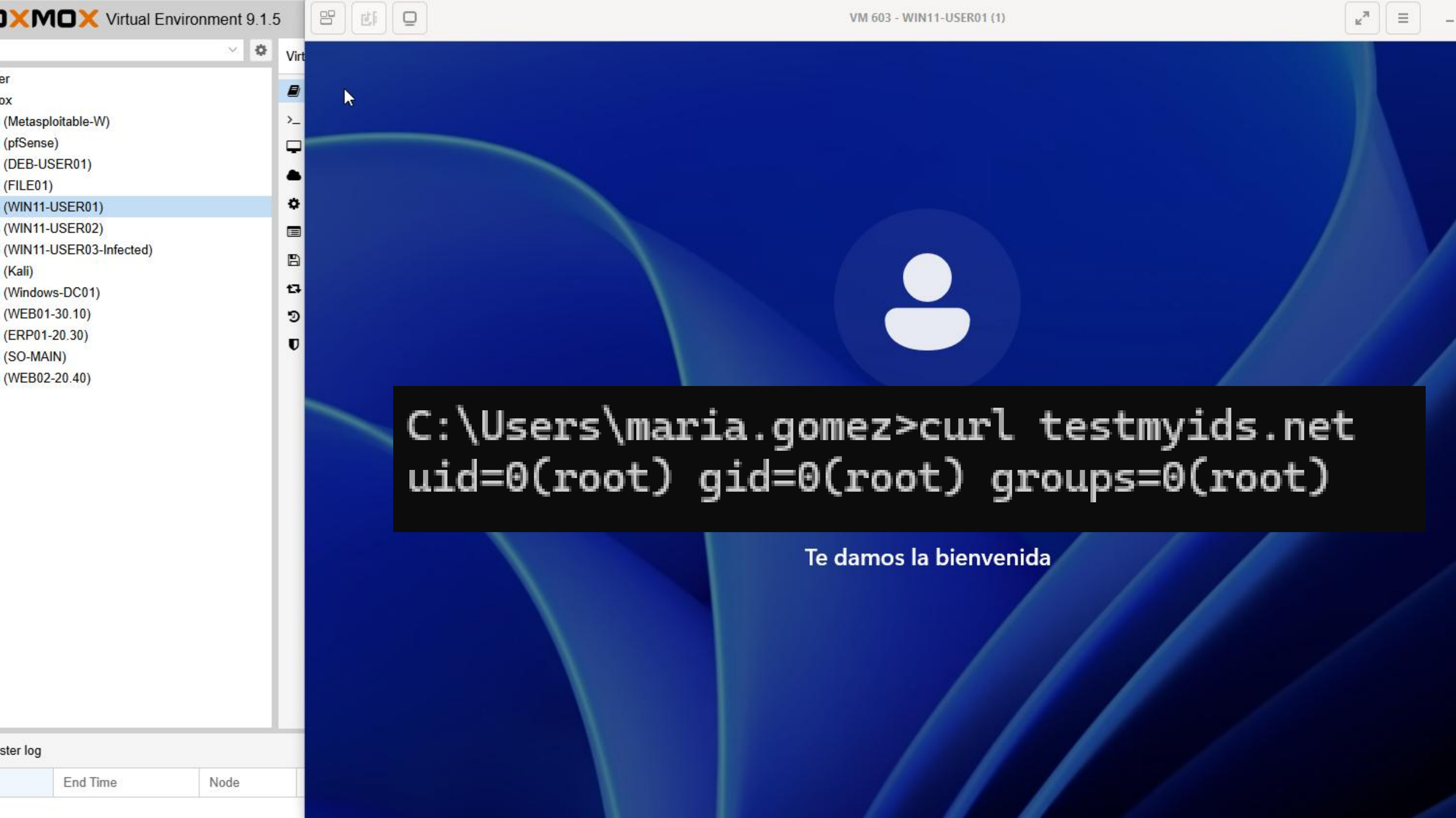
Aplicaciones Web & WAF

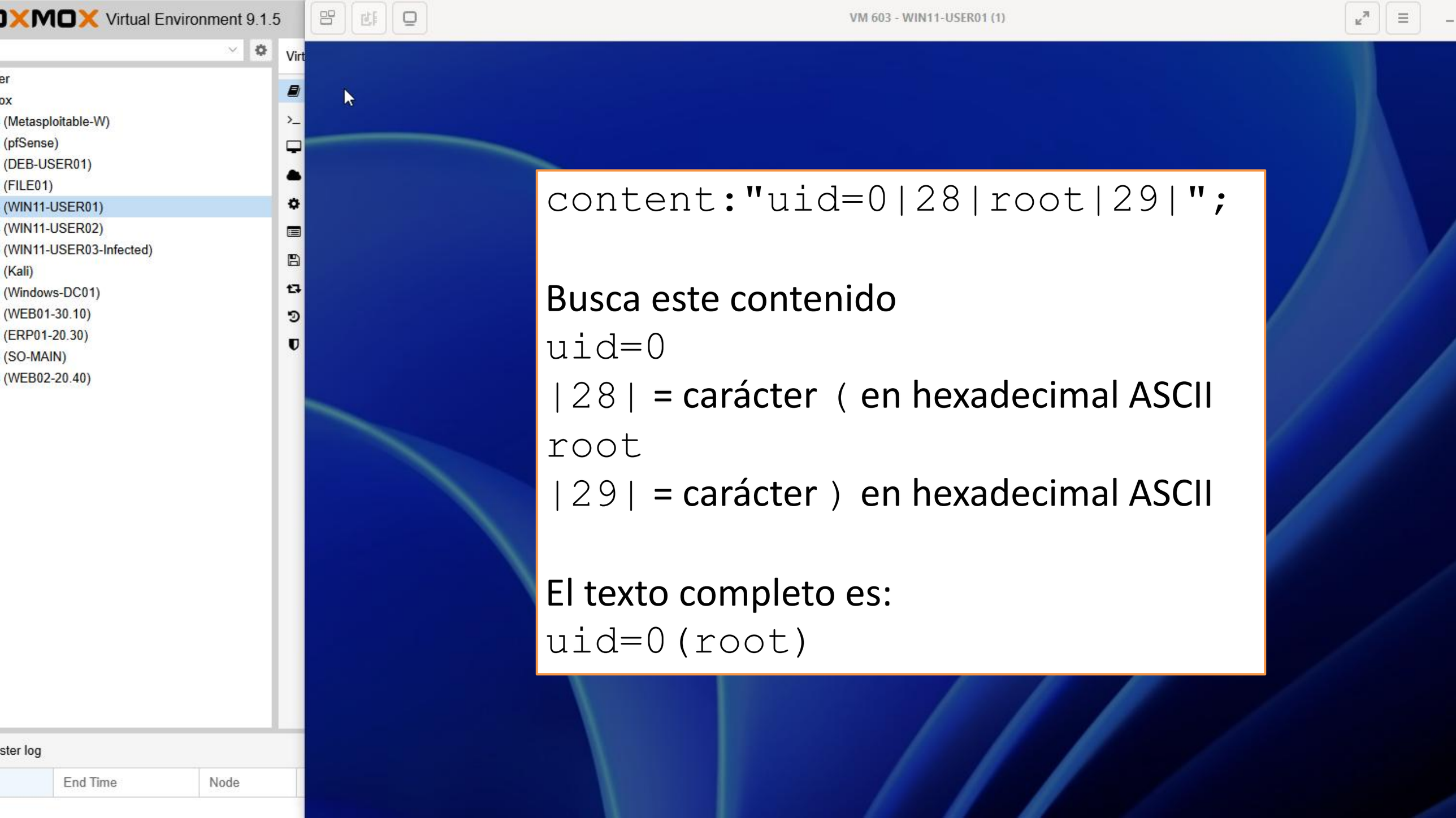
Routers / Switches
(NetFlow)

SIEM REPORT

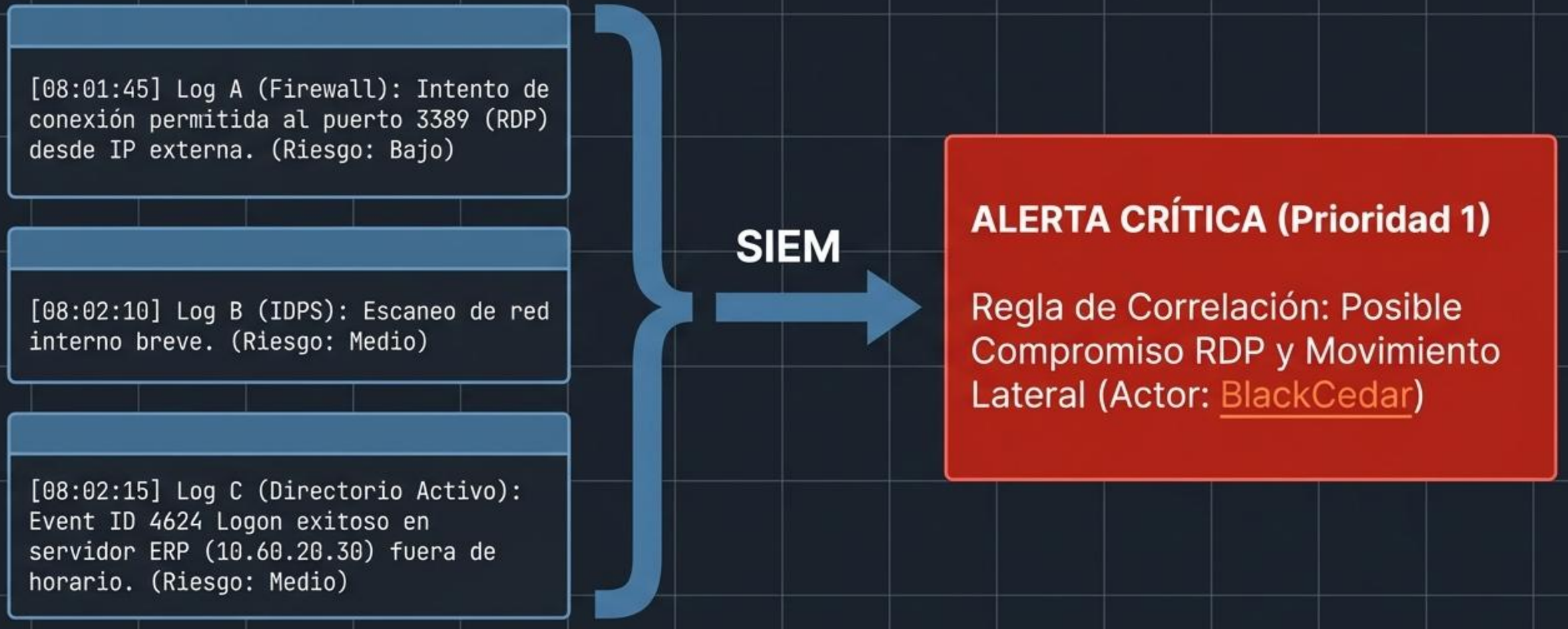
Incluso cuando existen herramientas de seguridad, los atacantes pueden encontrar formas de eludir dichos mecanismos de seguridad para ingresar a la red



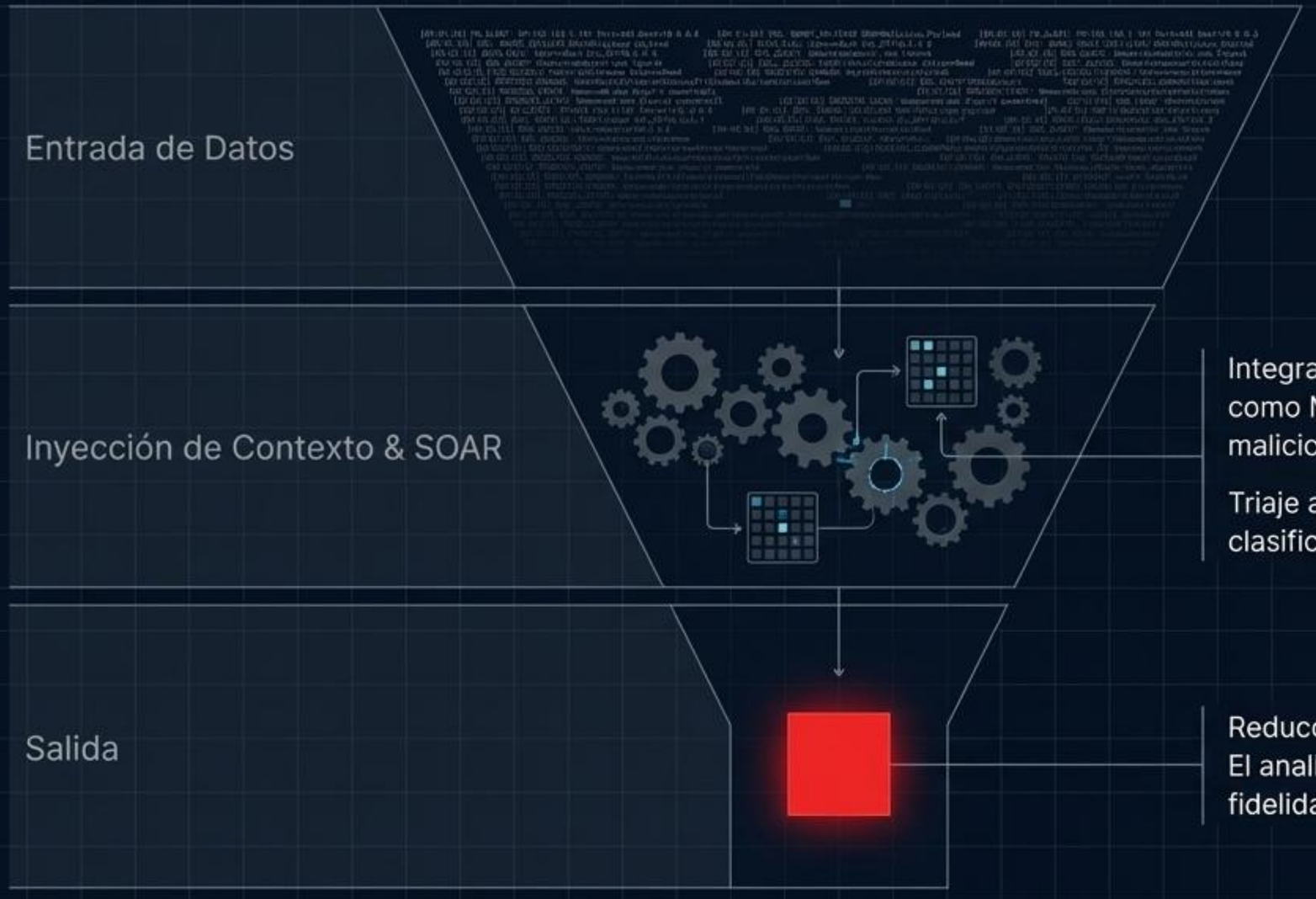

Virtual Environment 9.1.5
VM 603 - WIN11-USER01 (1)
(Metasploitable-W)
(pfSense)
(DEB-USER01)
(FILE01)
(WIN11-USER01)
(WIN11-USER02)
(WIN11-USER03-Infected)
(Kali)
(Windows-DC01)
(WEB01-30.10)
(ERP01-20.30)
(SO-MAIN)
(WEB02-20.40)
C:\Users\maria.gomez>curl testmyids.net
uid=0(root) gid=0(root) groups=0(root)
Te damos la bienvenida
End Time
Node


XMOX Virtual Environment 9.1.5
VM 603 - WIN11-USER01 (1)
(Metasploitable-W)
(pfSense)
(DEB-USER01)
(FILE01)
(WIN11-USER01)
(WIN11-USER02)
(WIN11-USER03-Infected)
(Kali)
(Windows-DC01)
(WEB01-30.10)
(ERP01-20.30)
(SO-MAIN)
(WEB02-20.40)
End Time
Node
content:"uid=0|28|root|29|";
Busca este contenido
uid=0
|28| = carácter (en hexadecimal ASCII
root
|29| = carácter) en hexadecimal ASCII
El texto completo es:
uid=0(root)

La Magia Operativa: Correlación de Eventos



Enriqueciendo la Visión: Inteligencia de Amenazas (CTI)



Integración de CTI (Bases de datos como MITRE, Secunia) con IOCs e IPs maliciosas.

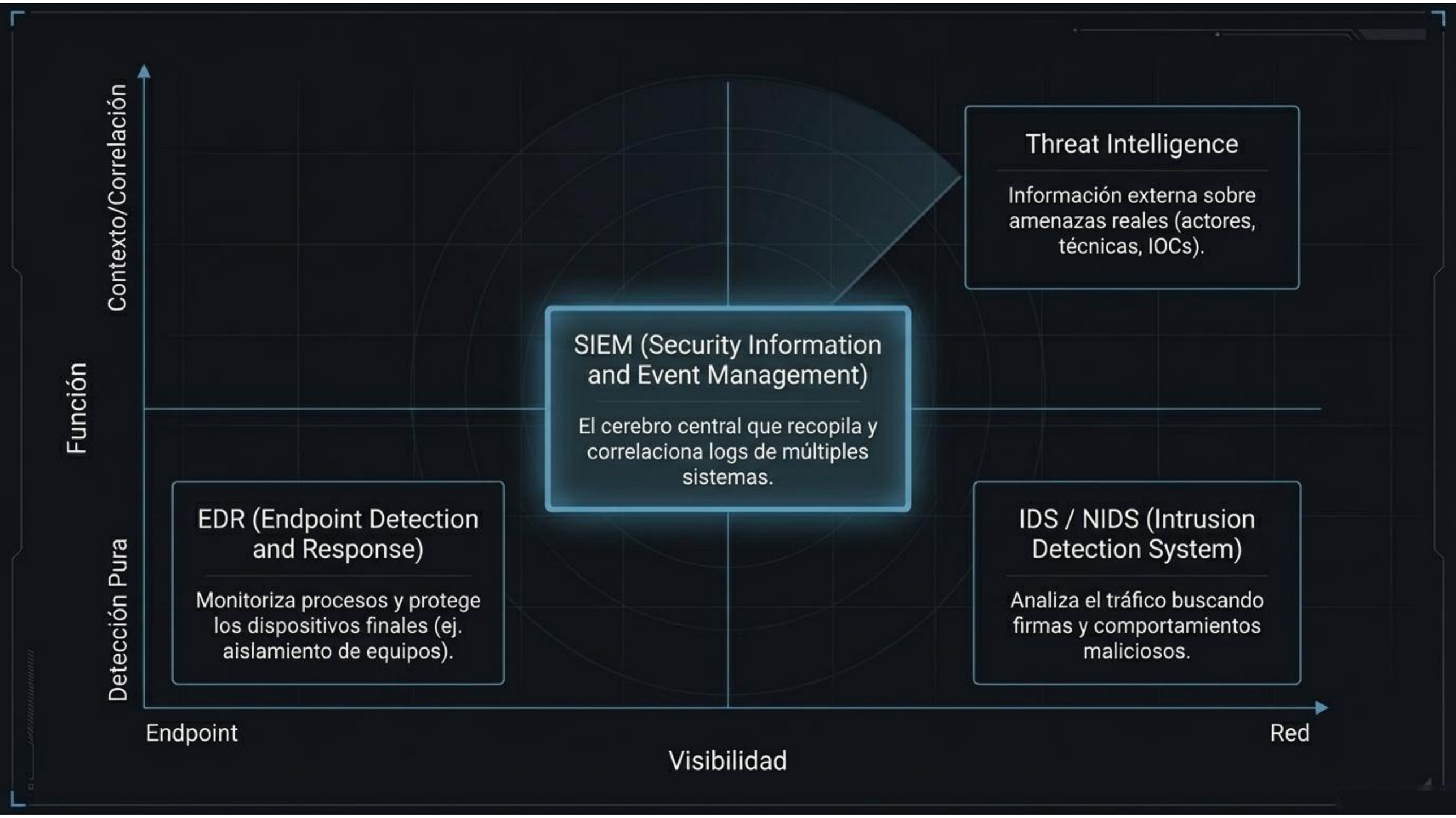
Triaje automático mediante SOAR para clasificar sin intervención manual.

Reducción drástica de falsos positivos. El analista T1 solo recibe alertas de alta fidelidad.

Cambiando las Reglas: Engaño Activo

Honeypots (El Señuelo Individual)	Honeynets (La Red Trampa)
Un sistema simulado (ej. falso servidor de facturación). Atrae ataques específicos para capturar IPs y payloads.	Colecciones de sistemas simulados (Windows, Linux, Mac) altamente monitorizados.

La Regla de Oro: 0% Falsos Positivos.
A diferencia de un firewall, ninguna actividad legítima debería tocar un honeypot. Si alguien entra, es una alerta roja confirmada. Sirve para estudiar tácticas en un entorno seguro.


Función
Contexto/Correlación
Detección Pura
Visibilidad
Endpoint
Red
Threat Intelligence
Información externa sobre amenazas reales (actores, técnicas, IOCs).
SIEM (Security Information and Event Management)
El cerebro central que recopila y correlaciona logs de múltiples sistemas.
EDR (Endpoint Detection and Response)
Monitoriza procesos y protege los dispositivos finales (ej. aislamiento de equipos).
IDS / NIDS (Intrusion Detection System)
Analiza el tráfico buscando firmas y comportamientos maliciosos.

Security Onion: Nuestro Entorno de Operaciones

La plataforma desde la que el analista monitoriza, investiga y responde.
Un conjunto integrado de sensores, SIEM y análisis forense de red.

El Mapa de Red Corporativo

Mapa Maestro

USERS - 10.60.10.0/24 (vmbr10)

WIN11 Endpoints

SERVERS - 10.60.20.0/24 (vmbr20)

AD corp.local

DMZ - 10.60.30.0/24 (vmbr30)

Servidor Web Público

pfSense Firewall
(The Gateway)

SOC - 10.60.40.0/24 (vmbr40)

Security Onion
IDS/IPS, Log Management, Threat Hunting

Capa Invisible: vmbr50 (SPAN Backbone)

El Cerebro: Infraestructura SOC (Security Onion)

Tier 1
Ingesta (Los Ojos)

Fleet Server
(Logs de Endpoints)

Interfaces SPAN
(enp6s19, enp6s20, enp6s21)

Tier 2
Análisis (El Motor)

Zeek
(Network metadata)

Suricata
(Alertas/Firmas)

Elasticsearch / Logstash
(Almacenamiento)

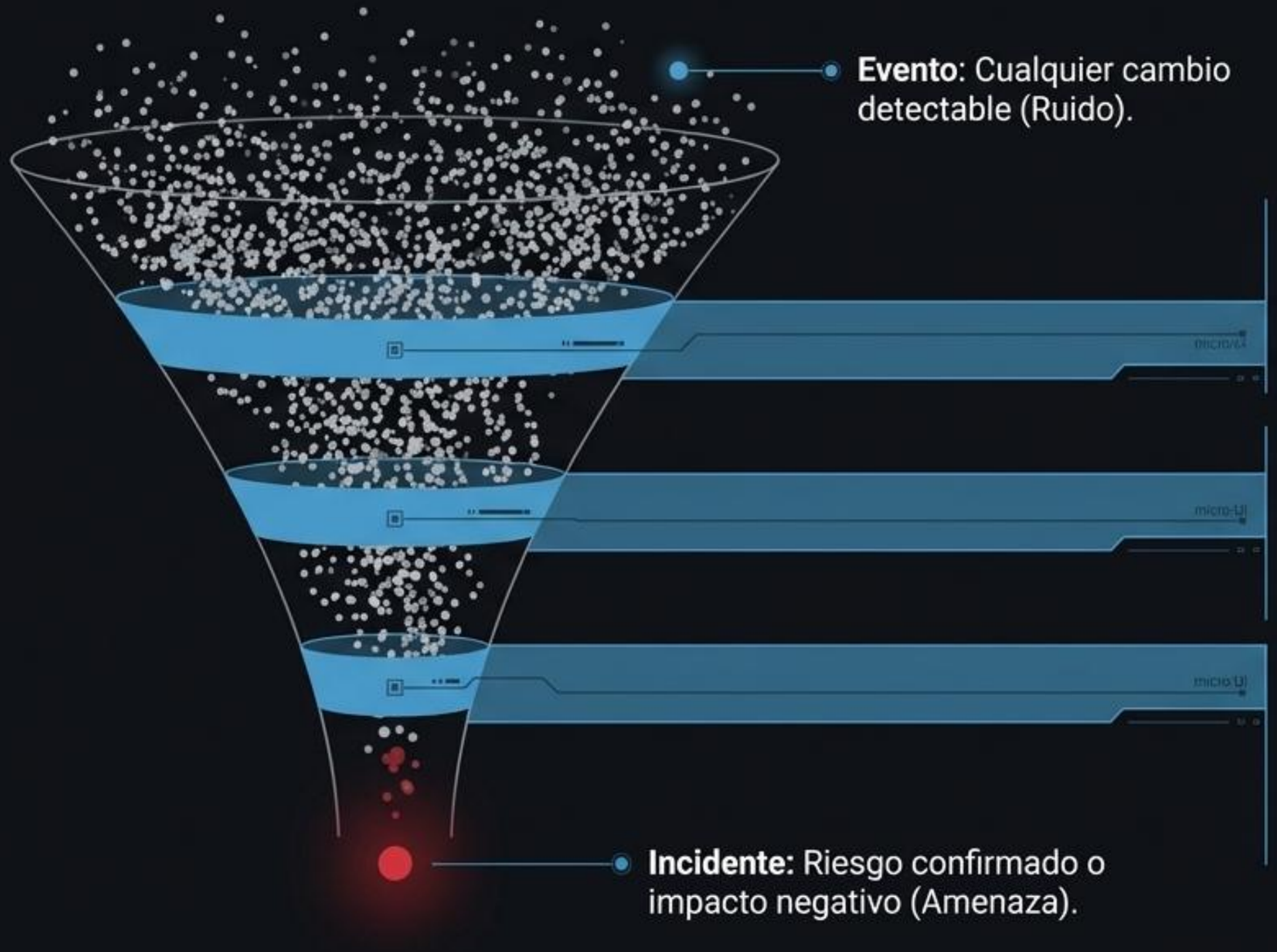
Tier 3
Visualización (Nuestra Pantalla)

Kibana
(Threat hunting)

SOC UI
(Gestión de alertas)

IP de Gestión: 10.60.40.10. Este es vuestro puesto de mando.
Un pipeline SIEM/NDR de nivel enterprise condensado en una sola plataforma.

La Misión del Centro de Operaciones de Seguridad



Evento: Cualquier cambio detectable (Ruido).

Incidente: Riesgo confirmado o impacto negativo (Amenaza).

1. Monitorizar (24/7):
Observación continua de redes, servidores y endpoints.

2. Detectar & Analizar:
Separar anomalías reales del tráfico legítimo.

3. Responder:
Intervenir antes de que la amenaza cause un impacto en el negocio.

El Ciclo de Vida del Incidente

Guía de Manejo de Incidentes de Seguridad Informática

Basado en el estándar **NIST SP 800-61 Rev. 2**

Existe la revisión 3 desde abril de 2025

NIST

NIST (National Institute of Standards and Technology) es una agencia del gobierno de EE.UU. que desarrolla estándares, directrices y mejores prácticas para la tecnología y, fundamentalmente, para la ciberseguridad. Su herramienta más conocida es el Marco de Ciberseguridad NIST (CSF), diseñado para ayudar a las organizaciones a gestionar y reducir los riesgos cibernéticos mediante un enfoque estructurado de cinco funciones principales

Para una empresa en Europa, el NIST es importante porque sirve como base técnica sólida para cumplir con las normativas europeas estrictas, principalmente la Directiva NIS2.

¿Qué es la Guía NIST 800-61?

Publicada por el *National Institute of Standards and Technology*, la revisión 2 de la publicación especial 800-61 establece el estándar global para la respuesta a incidentes.

Proporciona una metodología estructurada y repetible para mitigar ciberamenazas de manera eficiente.

Ayuda a las organizaciones a prepararse, detectar, analizar y recuperarse de brechas de seguridad.

Enfatiza la importancia de la mejora continua y la comunicación transversal en toda la empresa.

Es el marco de referencia utilizado por los equipos CSIRT (Computer Security Incident Response Team) de élite.

Fase 1: Preparación

El fundamento de la respuesta

Esta es la fase más crítica. Consiste en establecer una capacidad robusta de respuesta a incidentes que garantice una acción rápida cuando ocurra un evento de seguridad real.

Incluye la creación de políticas claras, el aprovisionamiento de herramientas de hardware y software especializadas, y lo más importante: la formación continua de los analistas para prevenir que los incidentes ocurran en primer lugar.

- Creación de políticas claras.
- Aprovisionamiento de herramientas de hardware y software especializadas.
- Formación continua de los analistas para prevenir que los incidentes ocurran en primer lugar.

Fase 2: Detección y Análisis

En esta fase, los analistas deben discernir rápidamente entre la actividad normal del sistema y una verdadera amenaza a la seguridad (triaje).

Fuentes de alertas:
Monitoreo activo de registros de sistemas, plataformas SIEM, alertas de IDS/IPS y reportes de usuarios finales.

Análisis de indicadores:
Búsqueda de precursores (signos de que un incidente puede ocurrir) e indicadores de compromiso (IoCs).

Documentación:
Registro seguro de toda la información técnica descubierta para **preservar la cadena de custodia** y facilitar el **análisis de causa raíz.**

Fase 3: Contención, Erradicación y Recuperación

Contención y Erradicación

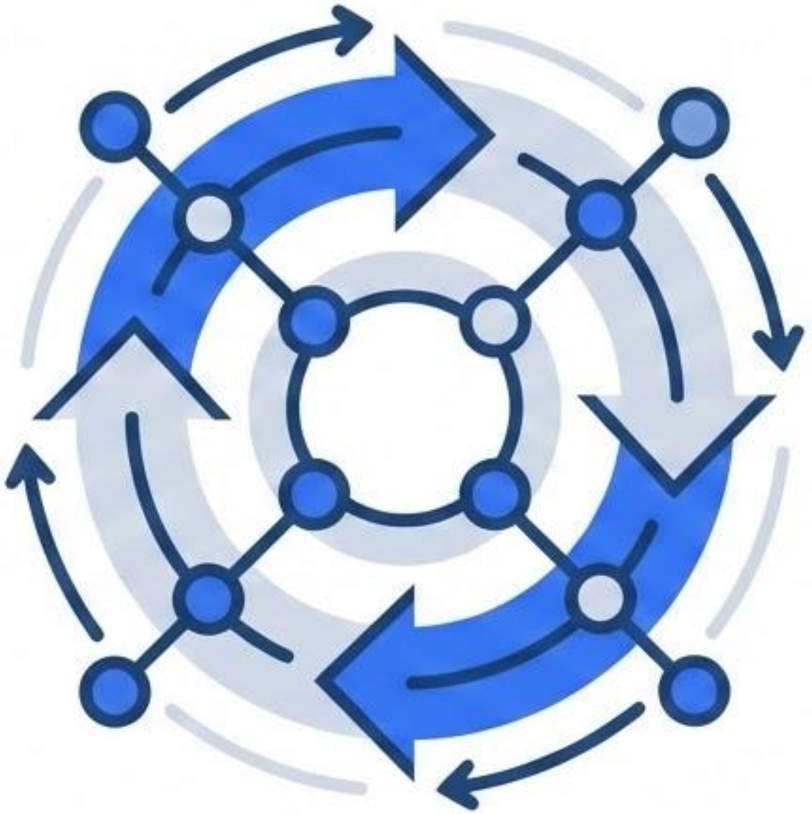
Esta etapa devuelve los sistemas impactados a su funcionamiento habitual. Se prioriza la **mitigando aislamiento rápido** e **eliminar de forma segura** e inmutables generadas antes de la infección. Implica realizar pruebas exhaustivas para validar que la amenaza ha sido erradicada por completo y aplicar una **monitorización intensificada** a corto plazo para evitar reinfecciones.

Fase 3: Contención, Erradicación y Recuperación

Restauración y Recuperación

Esta etapa devuelve los sistemas impactados a su funcionamiento habitual. Se prioriza la **restauración desde copias de seguridad limpias e inmutables** generadas antes de la infección. Implica realizar pruebas exhaustivas para validar que la amenaza ha sido erradicada por completo y aplicar una **monitorización intensificada** a corto plazo para evitar reinfecciones.

Fase 4: Actividad Post-Incidente



Reunión de Lecciones Aprendidas

A menudo omitida, esta fase es vital para cerrar el ciclo de NIST. Consiste en reunir a todos los actores involucrados para discutir constructivamente qué ocurrió, qué se hizo bien y qué falló en el proceso de respuesta.
El resultado debe ser una **mejora medible** en las políticas y herramientas de seguridad. Además, en esta fase se define el período de retención de las evidencias recolectadas, asegurando el cumplimiento legal y regulatorio a largo plazo.

Factores Críticos de Éxito en la Respuesta

Apoyo Ejecutivo y Patrocinio: Un equipo de respuesta a incidentes efectivo requiere un mandato claro, presupuesto adecuado y el respaldo continuo de la alta dirección empresarial.

Ejercicios de Simulación (Tabletops): La teoría no es suficiente. Realizar simulaciones periódicas del plan de respuesta asegura que cada miembro del equipo conozca exactamente su rol bajo la presión de un ataque real.

Automatización de Primer Nivel: Utilizar tecnologías de Orquestación y Respuesta (SOAR) para automatizar el triaje inicial reduce significativamente el volumen de alertas, previniendo el agotamiento del analista (alert fatigue).

Protocolos de Comunicación Claros: Definir previamente canales de comunicación seguros fuera de banda (out-of-band) y estrategias de relaciones públicas para gestionar correctamente la divulgación del incidente interna y externamente.

ACTUALIZACIÓN 2024/2025

NIST SP 800-61 Revisión 3

De la Respuesta Técnica a la Gestión Estratégica del Riesgo de Ciberseguridad.

Integración Profunda con el Marco CSF 2.0.

The NIST Cybersecurity Framework (CSF) 2.0

Marco voluntario para la gestión y reducción del riesgo de ciberseguridad.

Principales Novedades de la Versión 2.0:

- Nueva Función Central 'GOVERN': Enfatiza la gobernanza, la estrategia y la gestión de riesgos a nivel directivo.
- Alcance Universal: Diseñado para todas las organizaciones, independientemente de su sector o tamaño, no solo infraestructura crítica.
- Enfoque en la Cadena de Suministro: Mayor atención a la gestión de riesgos de terceros y proveedores.
- Integración de Privacidad: Mejor alineación con los principios de privacidad.

El Eslabón Crítico: Terceros

Ataques a la Cadena de Suministro

A diferencia de la Rev 2, la Revisión 3 asume que los incidentes más severos pueden no comenzar en su propia red. El documento pone un énfasis masivo en la gestión de riesgos de terceros.

Exige integrar explícitamente a **Proveedores de Servicios en la Nube (CSP), MSPs y contratistas** dentro de los "playbooks" de respuesta. Requiere definir Acuerdos de Nivel de Servicio (SLA) para la notificación de brechas y coordinar simulacros conjuntos antes de que ocurra un desastre.

El Factor Diferenciador de la Rev 3

GOVERN

La Nueva Función Central

Elevando la Ciberseguridad a la Junta

El cambio más drástico de la Revisión 3 es la adopción de la función "Govern" (Gobernanza) del CSF 2.0.

La respuesta a incidentes ya no puede existir en el vacío. Requiere supervisión ejecutiva, políticas corporativas formales, presupuesto garantizado y una comprensión clara del **apetito de riesgo** de la organización. El liderazgo empresarial es ahora responsable último de la eficacia de la respuesta.

Comparativa: Rev 2 vs Rev 3

SP 800-61 Rev 2 (2012)	SP 800-61 Rev 3 (Actualización)
Enfoque Principal: Táctico / Manejo Técnico de Incidentes	Estratégico / Gestión de Riesgos de Ciberseguridad
Alineación Normativa: Modelo de ciclo de vida independiente	Mapeo directo a funciones de NIST CSF 2.0
Entorno Operativo: Redes on-premise, perímetros definidos	Nube híbrida, OT, IoT, Zero Trust, Cadena de suministro
Actores Involucrados: Equipo de TI y SOC local	Toda la Organización, Asesoría Legal, Proveedores (MSPs/CSPs)
Mejora Continua: Reportes estáticos post-incidente	Alimentación directa al "Risk Register" corporativo

Actividad Post-Incidente Evolucionada

Integración con el Registro de Riesgos (Risk Register) Las "Lecciones Aprendidas" ya no son un PDF que se archiva. La Rev 3 exige que las brechas descubiertas durante un incidente modifiquen directamente el perfil de riesgo corporativo y fuercen la reasignación de presupuestos.

Obligación de Compartir Inteligencia Pasa de ser opcional a ser un mandato táctico. Compartir Indicadores de Compromiso (IoCs) y TTPs con agencias gubernamentales (CISA) y grupos de la industria (ISACs) para fortalecer la defensa colectiva.

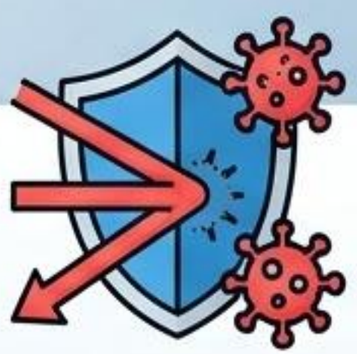
Recalibración de Modelos de Amenazas (Threat Modeling) Obligación de actualizar las defensas asumiendo que el atacante evolucionará. Si falló el MFA perimetral, el modelo post-incidente debe asumir identidades comprometidas por defecto.

FLUJO DE RESPUESTA A INCIDENTES DE UN SOC

DETECCIÓN

Identificación de amenazas y anomalías.

Monitorización de logs y alertas de seguridad.



CONTENCIÓN

Aislamiento inmediato de sistemas afectados.

Bloqueo de tráfico malicioso.

ERRADICACIÓN

Eliminación de la causa raíz de la amenaza.

Limpieza de malware y parcheo de vulnerabilidades.

RECUPERACIÓN

Restauración de sistemas y datos desde copias de seguridad.

Retorno a la operación normal.

LECCIONES APRENDIDAS

Análisis post-incidente.

Documentación y mejora continua de procesos y controles.

Nuestra Consola: Security Onion

Alerts

(El Punto de Entrada)

"Algo puede estar mal". Amenazas detectadas automáticamente listas para ser priorizadas.

Dashboard

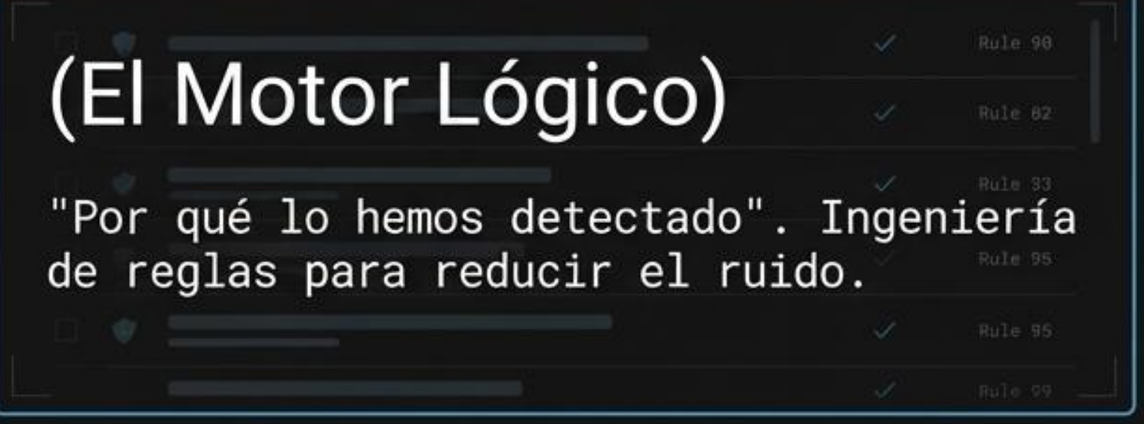
(La Vista Estratégica)

"Qué está pasando en general". Tendencias, anomalías globales y conciencia situacional.

Detections

(El Motor Lógico)

"Por qué lo hemos detectado". Ingeniería de reglas para reducir el ruido.



PCAP

(La Verdad Técnica)

"Qué ocurrió realmente". Capturas completas de paquetes para análisis forense profundo.

Las 4 Áreas Clave del Analista

Alerts

- **Función:** Detecciones automáticas por sistemas (Suricata/Sigma).
- **Uso SOC:** Punto de entrada operativo. Triage inicial.

Dashboard

- **Función:** Actividad global del entorno y tendencias.
- **Uso SOC:** Conciencia situacional y vista estratégica.

Detections

- **Función:** Gestión de lógicas, reglas y mecanismos de alertado.
- **Uso SOC:** Ingeniería de detección y ajuste de ruido.

PCAP

- **Función:** Capturas completas de paquetes de red.
- **Uso SOC:** Verdad forense profunda y validación.

Módulos de Security Onion y qué monitorizan

La Red

- **Función:**
- Suricata (IDS/IPS)
- Zeek (Análisis de Red)

Los Logs

- **Función:**
- Sigma (Reglas de Logs)

La Correlación

- **Función:**
- ElastAlert (Correlación y Alertas)

Endpoints y Ficheros

- **Función:**
- Fleet (Gestión de Endpoints)
- Strelka (Análisis de Ficheros)

El Modelo Mental del Analista

ALERTS

*Algo puede estar mal.

DASHBOARD

¿Qué está pasando en general?

DETECTIONS

¿Por qué lo hemos detectado?

PCAP

¿Qué ocurrió realmente en el cable?

Laboratorio: La Primera Alerta

Acceded al Dashboard. Encontrad la alerta.
Averiguad de qué nos avisa y decidid si es peligrosa.

ALERTA ENTRANTE

Real, dinámico y relativamente imprevisible

Preguntas del Analista Tier-1

- [ ] ¿Qué equipos internos de la empresa están involucrados?
- [ ] ¿Qué dominios externos están involucrados?
- [ ] ¿Cuándo comenzó la actividad? ¿Sigue activa?
- [ ] ¿Cuántas consultas se han hecho en las últimas 24h?

Security Onion: Nuestro Entorno de Operaciones

La plataforma desde la que el analista monitoriza, investiga y responde.
Un conjunto integrado de sensores, SIEM y análisis forense de red.

“Si mañana vuelve a aparecer esta alerta...
¿qué debería hacer un analista?”

Análisis de Riesgo: DynDNS

¿Por qué existe esta regla? ¿Cómo distinguir un uso legítimo de un ataque C2?

Malicioso	Legítimo
C2 malware	Teletrabajo
Botnets	Laboratorios internios
RATs	IoT
Exfiltración	VPN domésticas
Accesos remotos persistentes	

Toma de Decisiones en el SOC

¿Qué haría un analista en producción frente a esta alerta?

Toma de Decisiones en el SOC

¿Qué haría un analista en producción frente a esta alerta?

“Si mañana vuelve a aparecer esta alerta...
¿qué debería hacer un analista?”

Toma de Decisiones en el SOC

¿Qué haría un analista en producción frente a esta alerta?

1. Validar legitimidad del dominio
2. Identificar host origen
3. Ver frecuencia consultas
4. Correlacionar tráfico posterior
5. Evaluar riesgo negocio
6. Decidir acción

PLAYBOOK

Fin de la Sesión 01

La alerta ha sido documentada y la red permanece monitorizada.

Pero el adversario acaba de empezar a observar.

Próxima misión: Sesión 02 - Compromiso Inicial y Command & Control.

Fin de la Sesión 01

El reconocimiento ha terminado. En la próxima sesión: Phishing, robo de identidades y el inicio de la intrusión real en MedData.