Plataforma de visualización y monitoreo de Seguridad

Sumario

Introducción general:

La plataforma de visualización y monitoreo se implementa utilizando Grafana, la cual permite consolidar y presentar información técnica compleja de forma clara y estructurada mediante paneles y visualizaciones.

En este contexto, la plataforma cumple un rol de visualización y centralización de datos, sin generar información propia, integrando fuentes internas y externas gestionadas por el Área de Ciberseguridad.

La información mostrada en los paneles proviene de

- Reportes internos de monitoreo
- Reportes externos de terceros
- Información de inteligencia de amenazas (listas negras, reputación, abusos)
- Resultados de evaluaciones técnicas periódicas

Todos los datos presentados pasan por procesos de normalización, validación y correlación, con el objetivo de reducir falsos positivos y facilitar la toma de decisiones.

Esta integración permite contar con una visión centralizada, coherente y verificable del estado de seguridad de la infraestructura institucional.

Estructura general de los paneles:

La plataforma se organiza en cuatro paneles principales, cada uno con un objetivo específico.

En la parte superior de los paneles se encuentra el filtro de red o IP (ip_filter), que permite definir el conjunto de activos que se desean visualizar, pudiendo seleccionarse un host individual o la red completa.

Asimismo, la plataforma dispone de un selector de rango temporal, que permite establecer el período de tiempo sobre el cual se desea consultar la información.

Ambos elementos —el filtro de red/IP y el rango temporal— actúan de forma conjunta y determinan qué datos se muestran en cada Panel, recalculándose todas las métricas y visualizaciones en función de los valores seleccionados.

Los paneles disponibles son los siguientes:

Detección de Seguridad: orientado a la identificación de eventos, alertas y comportamientos anómalos en la red.

Estado de Servicios: permite visualizar la disponibilidad y el estado operativo de servicios considerados críticos.

Reportes Externos: consolida notificaciones y observaciones provenientes de fuentes externas y organismos de referencia.

Vulnerabilidades: presenta información sobre debilidades técnicas detectadas en los activos, diferenciando entre el estado actual y su evolución histórica.

Reputación y Bloqueos Preventivos: centraliza la gestión de direcciones IP y dominios con comportamiento sospechoso, permitiendo visualizar bloqueos activos, analizar incidentes históricos y validar reputación en fuentes externas.

Cada Panel está diseñado para **facilitar la interpretación de la información y la priorización de tareas de seguridad**, evitando conclusiones erróneas o interpretaciones fuera de contexto.

La plataforma está concebida como una **herramienta de apoyo a la gestión técnica y a la toma de decisiones**, y no como un sistema de control disciplinario.

A continuación, se detalla cada Panel, indicando qué información se puede visualizar y cómo debe interpretarse para apoyar la toma de decisiones técnicas.

1.Detección de Seguridad

El Panel Detecciones de Seguridad presenta información relacionada con eventos y alertas observadas en la red, con el objetivo de identificar actividad potencialmente maliciosa, patrones de ataque y servicios expuestos con mayor nivel de interacción hostil.

La información mostrada corresponde a eventos detectados a partir del análisis del tráfico de red y se encuentra orientada a la detección temprana, no a la confirmación de incidentes.

1.1 Visualización: Incidentes detectados

La visualización **Incidentes detectados** muestra la cantidad de eventos de seguridad observados dentro del período seleccionado y para el conjunto de activos definidos por el filtro de red.

Cada evento representa una **detección técnica** asociada a un patrón conocido de ataque o comportamiento sospechoso. La presencia de eventos no implica necesariamente una intrusión exitosa, pero sí indica **intentos de interacción potencialmente maliciosos** que deben ser analizados en contexto.

Incidentes Detectados

Fecha	IP destino ↑	Puerto destino	Proto	IP atacante	Amenaza	Severidad
2026-03-02 06:02:04	170.210.	111	UDP	64.62.197.43	GPL RPC portmap listing UDP 111	2
2026-03-02 06:00:21	170.210.	22	TCP	192.241.134.135	ET INFO SSH-2.0-Go version string Observed in	3
2026-03-02 06:02:01	170.210.	111	UDP	64.62.197.34	GPL RPC portmap listing UDP 111	2
2026-03-01 06:58:21	170.210.	22	TCP	185.194.217.71	ET INFO SSH-2.0-Go version string Observed in	3
2026-03-01 06:58:37	170.210.	22	TCP	46.101.75.32	ET INFO SSH-2.0-Go version string Observed in	3

1.2 Visualización: Servicios más atacados

La visualización **Servicios más atacados** identifica los servicios o puertos que concentran la mayor cantidad de eventos de seguridad dentro del período analizado.

Esta visualización permite detectar **superficies de ataque expuestas**, servicios innecesarios o configuraciones que atraen actividad maliciosa de forma recurrente.

La información es especialmente útil para priorizar acciones de endurecimiento, restricción de accesos o revisión de configuraciones. Esta visualización indica **interés externo** sobre los servicios expuestos.

Servicios mas Atacados

IP Destino	Puerto	Cantidad de Ataques
170.210.81	22	2
170.210.81	22	2
170.210.81	111	1
170.210.81	22	1
170.210.81	22	1
170.210.81	83	1
170.210.81	443	1
170.210.81	111	1
170.210.81	30807	1

1.3 Visualización: Top IPs origen de eventos

Esta visualización identifica las direcciones IP de origen que generan la mayor cantidad de eventos de seguridad dentro del período seleccionado y para el conjunto de activos definido por el filtro de red.

Su objetivo es visibilizar orígenes externos con actividad reiterada, lo que puede corresponder a escaneos automáticos, intentos de acceso no autorizado o campañas genéricas de ataque dirigidas a servicios expuestos.

La información presentada permite detectar comportamientos persistentes y constituye un insumo para la priorización de análisis, el cruce con fuentes de inteligencia de amenazas o la aplicación de medidas preventivas a nivel perimetral, cuando corresponda.

Un alto volumen de eventos asociado a una IP no implica necesariamente una intrusión exitosa, sino interés o actividad reiterada sobre la infraestructura analizada.

Top IPs origen de eventos

ip_origen	total_eventos
167.172.229.197	1
167.94.138.185	1
167.94.138.98	1
170.64.142.78	1
185.194.217.71	1
192.241.134.135	1
209.38.23.28	1
209.38.24.107	1
209.38.86.31	1

1.4 Visualización: Eventos por categoría / tipo

Esta visualización agrupa los eventos de seguridad detectados según su tipo o categoría técnica, permitiendo identificar qué clases de actividad predominan en el tráfico observado durante el período seleccionado.

Su finalidad es brindar contexto sobre el perfil general de amenazas, diferenciando entre actividades automatizadas (por ejemplo, escaneos masivos) y comportamientos más específicos que podrían requerir un análisis más detallado.

La información presentada es de carácter descriptivo y debe utilizarse como complemento de otros indicadores, contribuyendo a la comprensión del escenario de detección sin constituir, por sí sola, confirmación de un incidente de seguridad

2. Estado de Servicios

El Panel Estado de Servicios presenta información sobre la disponibilidad y el estado operativo de los servicios y hosts monitoreados.

Su objetivo es brindar visibilidad sobre interrupciones, degradaciones y recuperaciones de servicios críticos, permitiendo una detección temprana de fallas y un seguimiento de eventos recientes.

Los servicios y hosts incluidos en este Panel se incorporan al monitoreo a solicitud del técnico responsable, en función de la criticidad del servicio, su exposición y las necesidades operativas definidas por cada área.

2.1 Visualización: Estado actual del servicio

Esta visualización muestra el estado actual de los servicios y hosts monitoreados al momento de la consulta.

Los estados reflejan la condición operativa informada por el sistema de monitoreo y permiten identificar rápidamente servicios caídos, con fallas intermitentes o funcionando con normalidad.

Se utiliza para el seguimiento operativo y validación posterior a tareas de mantenimiento, detección de caídas activas y validación posterior a tareas de mantenimiento.

Estado Actual

ip	host	estado	detalle	fecha
170.210.8	.i.uncoma.edu.ar	UP	PING OK - Packet loss = 0%, R	2026-03-01 19:30:59.000
170.210.8	a.uncoma.edu.ar	UP	TCP OK - 1,017 second respons	2026-03-01 19:30:41.000

2.2 Visualización: Eventos recientes del servicio

La visualización Eventos recientes del servicio presenta un historial cercano de cambios de estado, incluyendo caídas y recuperaciones de servicios monitoreados.

Su objetivo es brindar contexto temporal sobre incidentes recientes, permitiendo identificar interrupciones breves, fallas recurrentes o recuperaciones automáticas.

Esta visualización es especialmente útil para analizar comportamientos intermitentes y para validar acciones correctivas realizadas por los equipos técnicos.

Eventos Recientes

Fecha	Host	Servicio	IP	Estado	Detalle
2026-03-01 19:30:59	i.uncoma.edu.ar	_	170.210.8	UP	PING OK - Packet loss = 0%, RTA = 1.25 ms
2026-03-01 19:30:41	a.uncoma.edu.ar	_	170.210.8	UP	TCP OK - 1,017 second response time on 170.210.80
2026-03-01 18:40:55	i.uncoma.edu.ar	_	170.210.8	DOWN	CRITICAL - Host Unreachable (170.210.8
2026-03-01 18:15:40	.uncoma.edu.ar	_	170.210.8	UNREACHABLE	connect to address 170.210.8
2026-03-01 18:09:45	a.uncoma.edu.ar	_	170.210.8	DOWN	connect to address 170.210.8 port 8110: No existe ninguna ruta hasta el host

2.3 Visualización: Servicios con mayor cantidad de eventos.

Esta visualización presenta un ranking de los servicios que registraron la mayor cantidad de eventos dentro del período y alcance seleccionados.

Cada evento corresponde a un cambio de estado o notificación generada por el sistema de monitoreo, incluyendo caídas, recuperaciones o estados de advertencia.

El objetivo de esta visualización es identificar **servicios inestables o con comportamientos recurrentes**, que pueden requerir una revisión técnica más profunda, ajustes de configuración o acciones correctivas preventivas.

La información presentada permite diferenciar incidentes puntuales de problemas persistentes, contribuyendo a la priorización de tareas de mantenimiento y mejora de la disponibilidad

Servicios con Mayor Cantidad de Eventos

host_servicio	total_eventos
a.uncoma.edu.ar : _	3
uncoma.edu.a	2

3.Reportes Externos

En este Panel se consolida información proveniente de **fuentes externas de referencia**, con el objetivo de identificar incidentes observados desde fuera de la organización y detectar activos que puedan encontrarse listados en mecanismos públicos de reputación o bloqueo.

Este Panel permite incorporar **contexto externo** al análisis interno, complementando la información obtenida a partir de los sistemas de monitoreo y detección locales.

3.1 Visualización: Detalles de incidentes reportados

Esta visualización presenta el detalle de incidentes reportados por fuentes externas, asociados a direcciones IP pertenecientes a la infraestructura analizada.

Los reportes reflejan observaciones realizadas desde el exterior y pueden incluir actividades como abuso de servicios, configuraciones inseguras o comportamientos anómalos detectados por terceros.

La información presentada debe interpretarse como una **notificación externa**, que requiere validación técnica interna para confirmar su alcance y causa.

Uso recomendado:

- Identificar incidentes que no fueron detectados internamente
- Correlacionar con otras Visualizaciones (detecciones, servicios, vulnerabilidades)
- Priorizar análisis sobre activos reportados por terceros

Detalles de Incidentes Reportados

time	fecha	IP destino	Puerto	Protocolo	Severidad	Descripción
2026-02-28 11:33:54	2026-02-28 14:33:54	170.210.8	22	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "hassh": "077e440c58
2026-02-28 11:01:59	2026-02-28 14:01:59	170.210.	22	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "hassh": "425d29fe50
2026-02-28 10:37:31	2026-02-28 13:37:31	170.210.8	22	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "hassh": "779664e661
2026-02-28 09:43:30	2026-02-28 12:43:30	170.210.	22	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "hassh": "779664e661
2026-02-28 09:10:52	2026-02-28 12:10:52	170.210.	22	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "hassh": "779664e661
2026-02-28 09:09:50	2026-02-28 12:09:50	170.210.	5672	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "class": "10", "naics": "
2026-02-28 09:09:14	2026-02-28 12:09:14	170.210.8	22	tcp	medium	{"geo": "AR", "city": "BUENOS AIRES", "hassh": "779664e661
2026-02-28 07:58:22	2026-02-28 10:58:22	170.210.	8006	tcp	low	{"geo": "AR", "city": "BUENOS AIRES", "jarm": "", "naics": "", "

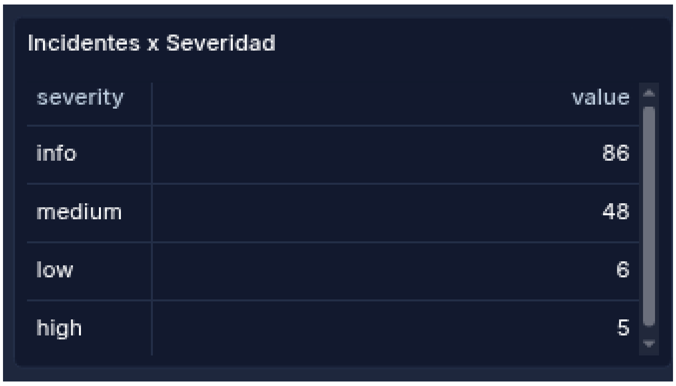
3.2 Visualización: Incidentes por severidad

Esta visualización agrupa los incidentes reportados por fuentes externas según su nivel de severidad, permitiendo dimensionar el **impacto potencial** de las observaciones recibidas.

Su objetivo es facilitar la priorización del análisis y la atención de incidentes, enfocando los esfuerzos en aquellos reportes que representan un mayor riesgo o una mayor exposición.

La severidad asignada corresponde a la clasificación realizada por la fuente externa y debe considerarse como un **indicador orientativo**, no como una evaluación definitiva.

La visualización de Reportes Externos permite incorporar una **visión desde el exterior** de la infraestructura, complementando el monitoreo interno y contribuyendo a una gestión más integral de la exposición y la reputación institucional.


Incidentes x Severidad

severity	value
info	86
medium	48
low	6
high	5

4.Vulnerabilidades

El Panel de Vulnerabilidades tiene como objetivo:

- Mostrar el estado actual de exposición de conjunto de activos o una red.
- Facilitar la priorización de remediaciones.
- Permitir un seguimiento histórico sin inducir interpretaciones erróneas.

Importante: el Panel no mide esfuerzo, no mide rendimiento del equipo ni compara escaneos entre sí de forma directa. Mide exposición técnica.

4.1 Visualización: Fecha último reporte

Indica cuándo se realizó el último escaneo de vulnerabilidades.
Los reportes se realizan principalmente con una periodicidad trimestral.
No obstante, dicha frecuencia puede ajustarse cuando se incorporan nuevos servicios, se producen cambios relevantes en la infraestructura, el técnico responsable del servicio solicita una evaluación específica o el Área de Ciberseguridad lo considera necesario.

Esta flexibilidad es fundamental, ya que pueden surgir nuevas vulnerabilidades de alto impacto entre evaluaciones programadas, ya sea por la aparición de fallas críticas, cambios en el contexto de amenazas o alertas provenientes de fuentes externas.

4.2 Visualización: Contadores por severidad

Se muestran tres indicadores:

Altas / Críticas (rojo)

Medias (amarillo)

Bajas (verde)

Estos valores representan:

Cantidad de vulnerabilidades actualmente presentes según el último escaneo.

Interpretación clave:

0 Altas/Críticas = situación aceptable

Medias y Bajas pueden gestionarse por ventana de mantenimiento

4.3 Visualización: Tabla de Vulnerabilidades Actuales

Lista detallada de todas las vulnerabilidades detectadas en el último escaneo.

Columnas principales: IP afectada, Nombre de la vulnerabilidad,CVSS, Severidad y Fecha del escaneo

Vulnerabilidades Actuales

ip	vulnerabilidad	cvss	threat	fecha_scan
170.210.8	Proxmox Virtual Environment (VE, PVE) End of	10	High	2025-12-15
170.210.8	Operating System (OS) End of Life (EOL) Detec	10	High	2025-12-15
170.210.8	WordPress WPForms Lite plugin <= 1.9.3.1 XSS	5.40	Medium	2025-12-15
170.210.8	WordPress Colibri Page Builder Plugin < 1.0.24	5.40	Medium	2025-12-15
170.210.8	WordPress WPForms Contact Form Plugin <=	5.30	Medium	2025-12-15
170.210.8	WordPress < 6.5 Private Information Exposure	5.30	Medium	2025-12-15
170.210.8	SSL/TLS: Renegotiation DoS Vulnerability (CVE	5	Medium	2025-12-15

Sección inferior: Información histórica

Esta sección permite identificar dónde hubo problemas recurrentes o críticos a lo largo del tiempo. No representa el estado actual, sino el comportamiento histórico.

4.4 Visualización: Hosts con más vulnerabilidades

Ranking de IPs según cantidad total de vulnerabilidades históricas.

Sirve para identificar activos estructuralmente débiles y priorizar revisiones profundas.

Un host frecuente en este ranking suele indicar: Mala configuración base, Software sin mantenimiento y exposición innecesaria

Hosts con mas Vulnerabilidades

ip	total_vulns	max_cvss
170.210.8	33	10
170.210.8	14	10
170.210.8	39	10
170.210.8	76	10
170.210.8	26	10
170.210.8	21	10
170.210.8	33	10
170.210.8	64	10

4.5 Visualización: Tabla de Vulnerabilidades

Muestra el listado de vulnerabilidades históricas

Tablas de vulnerabilidades

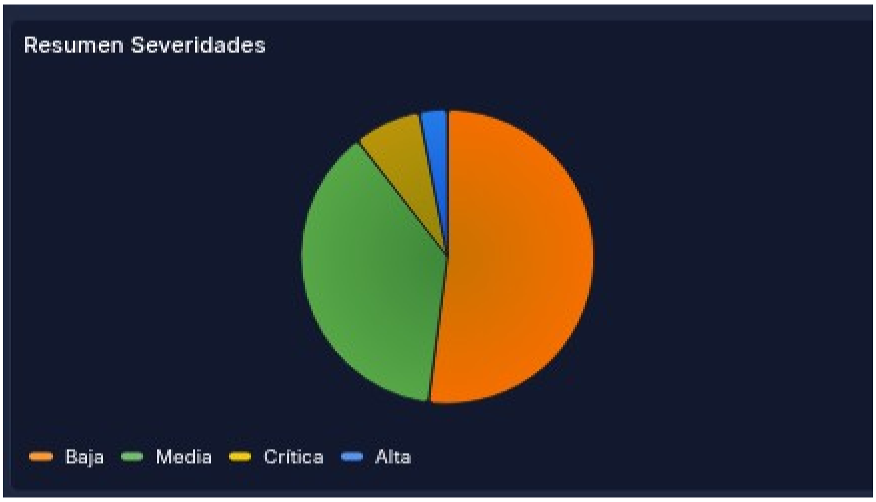
ip	vulnerabilidad	cvss	threat	fecha_scan
170.210.8	Proxmox Virtual Environment (	10	High	2025-12-15
170.210.8	Proxmox Virtual Environment (	10	High	2025-09-02
170.210.8	Proxmox Virtual Environment (	10	High	2024-03-01
170.210.8	Operating System (OS) End of	10	High	2025-09-02
170.210.8	Report outdated / end-of-life S	10	High	2024-06-03
170.210.8	Report outdated / end-of-life S	10	High	2024-06-03
170.210.8	Report outdated / end-of-life S	10	High	2024-06-03

4.6 Visualización: Resumen de severidades (gráfico)

Distribución porcentual de vulnerabilidades por severidad.

Este gráfico es descriptivo, no operativo.

Uso recomendado: Presentaciones de contexto e informes ejecutivos



5 “Reputación y Bloqueos Preventivos”

El Panel Reputación y Bloqueos Preventivos permite: Visualizar IPs y dominios actualmente bloqueados, consultar el historial de bloqueos, Verificar reputación en listas negras externas.

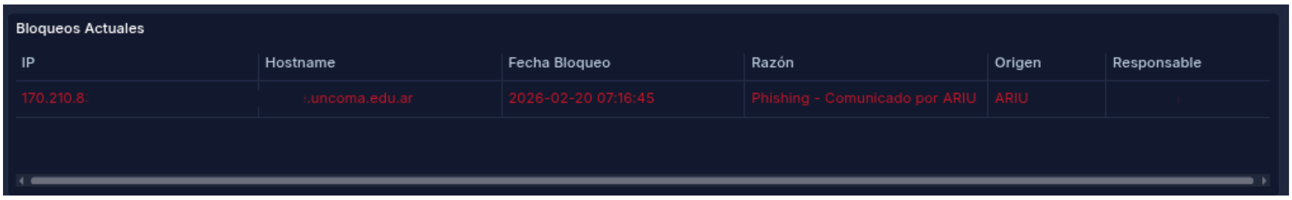
5.1 Bloqueos Preventivos

Esta sección muestra los bloqueos activos aplicados sobre direcciones IP o dominios que presentan comportamientos anómalos o han sido reportados como sospechosos.

Los bloqueos pueden originarse por:

- Detección automática de anomalías.
- Reportes internos.
- Alertas de organismos externos.
- Identificación de campañas de phishing.
- Actividad relacionada con malware o abuso de red.

El objetivo principal es reducir el impacto de incidentes y preservar la reputación institucional ante proveedores, organismos y redes externas.



Bloqueos Actuales

IP	Hostname	Fecha Bloqueo	Razón	Origen	Responsable
170.210.8[redacted]	[redacted].uncoma.edu.ar	2026-02-20 07:16:45	Phishing - Comunicado por ARIU	ARIU	[redacted]

5.2 Bloqueos por IP

Este Panel presenta un resumen estadístico de los bloqueos asociados a cada dirección IP.

Su función principal es llevar un registro acumulativo de incidentes por IP, permitiendo identificar aquellas que presentan mayor nivel de riesgo.

5.3. Históricos

Esta sección almacena el registro histórico completo de todos los bloqueos realizados en el sistema.

Incluye información sobre:

- IP y dominio involucrados.
- Estado del bloqueo.
- Fecha de inicio y finalización.
- Motivo.
- Observaciones asociadas.

5.4 Visualización: Listas negras por IP

Esta visualización muestra si una dirección IP se encuentra listada en uno o más mecanismos públicos de reputación o bloqueo externos, junto con la fecha de la última detección informada.

La presencia de una IP en estas listas puede afectar la **reputación de los servicios**, la entrega de correo electrónico o el acceso desde redes externas, aun cuando no exista un incidente activo en curso.

Cuando una IP aparece listada, corresponde al **administrador del servicio** verificar la causa, aplicar las correcciones necesarias y gestionar la solicitud de remoción directamente ante el organismo o servicio correspondiente.

Listas Negras por IP

IP	Spamhaus	AbuseIPDB	Blocklist.de	OTX	Última detección
170.210.8	No Listada	No Listada	No Listada	No Listada	
170.210.8	No Listada	No Listada	No Listada	No Listada	

La información presentada en la plataforma debe ser utilizada como insumo técnico para la mejora continua de los servicios.

La interpretación y las acciones derivadas corresponden a los equipos responsables de cada sistema.