OpenSearch Dashboards Reports

Search

May 1, 2025 @ 00:00:00.000 → Jun 1, 2025 @ 00:00:00.000

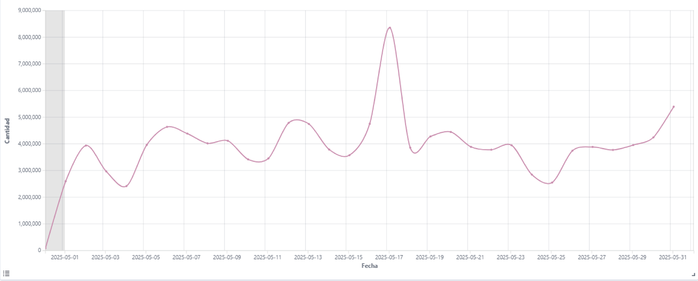
Informe Mensual | VIERCI

Resumen de detecciones de nivel 10 (diez) a 16 (Dieciséis)

Esta sección proporciona un resumen global de las detecciones correspondientes a los niveles 10 (diez) a 16 (dieciséis). Está diseñada para monitorear tendencias y cantidades, con el objetivo de establecer un plan de mejora continua.

A continuación, se presentan los datos correspondientes al total de detecciones relevantes, su evolución temporal y un ranking de los agentes con mayor actividad.

Evolución de Detecciones



Detecciones Registradas | Top 10 Equipos

Equipos	Detecciones Registradas	Equipos Registrados
RETSVRDC01	49,917,468	1
OLVSVRDC02	18,232,047	1
retsvrcas01	16,831,470	1
olvsvrcas01	12,912,777	1
olvsvrcas02	12,138,112	1
retsvrradius01	5,051,903	1
olvsvrdb17	2,278,715	1
olvaudisd01	1,113,867	1
OLVSVRGWSAP	784,352	1
SVRVISUALFACT	610,748	1
Otros	4,701,394	65
	124,572,853	**75**

Errores de Autenticación Múltiples

En los siguientes gráficos se listan los errores de **autenticación múltiples** del mes, esto ocurre cuando la operación de autenticación de una misma **[cuenta de usuario]** falla 8 (ocho) veces en un período consecutivo de 4 (cuatro) minutos.

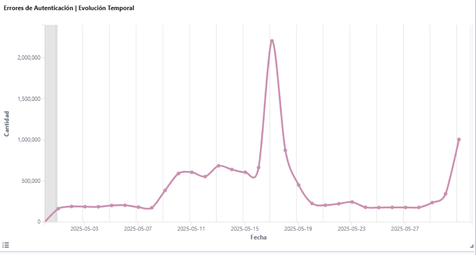
Estos pueden, potencialmente, indicar cuanto sigue:

- Intentos de fuerza bruta en la red
- Errores de configuración

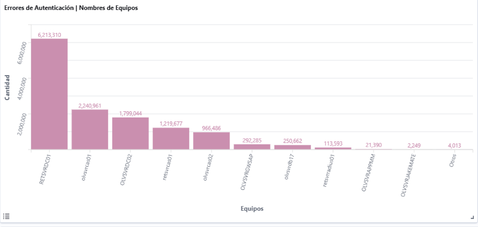
Errores de Autenticación

filters	Nivel	Descripción	Cantidad	Equipos Afectados
Severidad Alta	10	Multiple Windows Logon Failures	1,356,678	8
Severidad Alta	10	syslog: User missed the password more than one time	1	1
Severidad Moderada	9	User account locked out (multiple login errors)	17,139	2
Severidad Moderada	8	Maximum authentication attempts exceeded.	1	1
Severidad Moderada	5	Logon Failure - Unknown user or bad password	7,920,382	31
Severidad Moderada	5	Windows DC Logon Failure	3,577,544	2
Severidad Moderada	5	MS SQL server logon failure.	251,833	4
Severidad Moderada	5	sshd: authentication failed.	45	5
Severidad Moderada	5	PAM: User login failed.	25	9

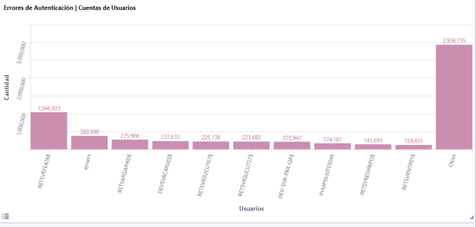
Errores de Autenticación | Evolución Temporal



Errores de Autenticación | Nombres de Equipos



Errores de Autenticación | Cuentas de Usuarios



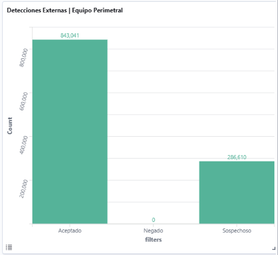
Actividad Remota

Esta sección explora la actividad correspondiente al tráfico de red que proviene de locaciones geográficamente externas a Paraguay cuyo destino es su Infraestructura Tecnológica. Le posibilita comprender diversos tipos de tráficos de red que son procesados por su solución de **Perímetro de Red (Firewall);** con lo cual puede implementar medidas para evitar o prevenir tráfico de orígenes geográficos no deseados.

El SIEM Wazuh procesa la actividad mencionada y la clasifica según su tipo de actividad; que se presenta en el siguiente mapa mundial mediante objetos de color.

- - **[Tráfico Sospechoso]:** Cualquier actividad clasificado como **[ataque]** o **[error de autenticación]** que **no fue detenido por el Equipo Perimetral**.
- - **[Tráfico Aceptado]:** Cualquier actividad correspondiente a tráfico **aceptado por el Equipo Perimetral**.
- - **[Tráfico Negado]:** Cualquier actividad correspondiente a tráfico **detenido por el Equipo Perimetral**.

Detecciones Externas | Equipo Perimetral



Detecciones de Paraguay | Equipo Perimetral

filters	Cantidad
Aceptado	0
Negado	0
Sospechoso	0

Análisis de Vulnerabilidades

Este apartado presenta un resumen de las **Vulnerabilidades** detectadas por el SIEM Wazuh, el cual utiliza el sistema de puntuación **[CVSS 3]** que a su vez las clasifica en categorías de severidad. El objetivo del presente resumen es mejorar la **postura de seguridad** de su Organización, mediante la ejecución del **Plan de Acción para mitigar o erradicar Vulnerabilidades Presentes**.

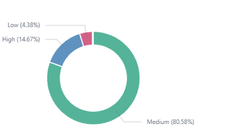
Primeramente se muestran la diversidad de **Vulnerabilidades Presentes.** Adicionalmente, se enfoca en mostrar aquellas de mayor severidad (críticas y altas), correspondiente a:

- Sistemas Operativos y Paquetes con mayor vulnerabilidad.
- Vulnerabilidades más comunes.
- Cantidad de vulnerabilidades.

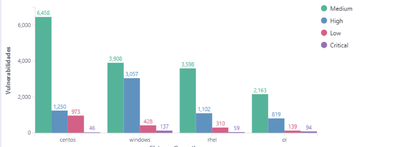
Total Vulnerabilidades

Severidad	Cantidad	Equipos Afectados
Critical	266	67
High	5,146	73
Low	1,569	73
Medium	12,064	73
	19,045	**286**

Total Vulnerabilidades



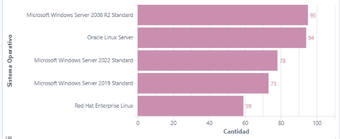
Total Vulnerabilidades | Sistema Operativo



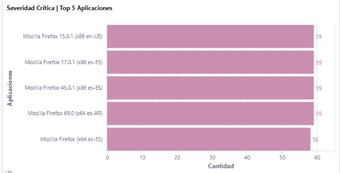
Vulnerabilidades Críticas | Top 15

CVE	Equipos
CVE-2025-21298	26
CVE-2025-21307	26
CVE-2022-22822	22
CVE-2022-22823	22
CVE-2022-22824	22
CVE-2024-38063	22
CVE-2024-38140	22
CVE-2024-38199	22
CVE-2024-49112	21
CVE-2022-23852	20
CVE-2022-2526	20
CVE-2023-37920	20
CVE-2020-14343	19
CVE-2022-25235	19
CVE-2022-25236	19

Severidad Crítica | Top 5 Sistemas Operativos



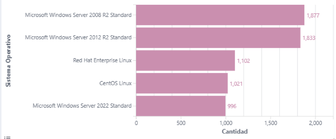
Severidad Crítica | Top 5 Aplicaciones



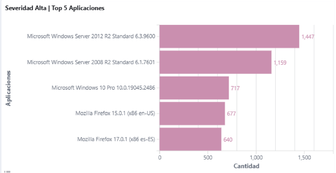
Vulnerabilidades Altas | Top 15

CVE	Equipos
CVE-2022-31676	43
CVE-2023-34058	42
CVE-2023-20900	41
CVE-2022-22943	39
CVE-2023-6040	30
CVE-2024-49851	30
CVE-2024-49860	30
CVE-2024-50278	30
CVE-2024-50301	30
CVE-2024-53156	30
CVE-2024-56600	30
CVE-2024-56601	30
CVE-2024-56603	30
CVE-2024-56606	30
CVE-2024-36960	29

Severidad Alta | Top 5 Sistemas Operativos



Severidad Alta | Top 5 Aplicaciones



----- Fin del Reporte -----