# 8

# MÉTRICAS E **INDICADORES**

**CONTENIDO**

- *Indicadores de actividad*
- *Indicadores de calidad del servicio*
- *Indicadores de riesgo*
- *HERA*
- *Wazuh*

Es necesario que las organizaciones sean **capaces de medir su capacidad ge gestión de incidentes de seguridad** para así poder mejorarlas. Es por esto que las organizaciones necesitan definir sus propios métricas e indicadores para poder determinar el nivel de calidad de la gestión de incidentes.

# ¿QUÉ INDICADORES HAY?

# INDICADORES DE **ACTIVIDAD**

Proporcionan información de los niveles de actividad del proceso de gestión de incidentes.

**14**

Incidentes gestionados al mes

**23** Números de incidentes gestionados dependiendo su **taxonomía**

**5**

Eventos de seguridad detectados al mes

**8**

Análisis forenses realizados al mes

**0**

Número de veces al año que se ha activado el GIR

* GIR (Grupo de Intervención Rápida)

# INDICADORES DE
# CALIDAD DEL SERVICIO

Proporcionan información relativa a la disponibilidad o capacidad de la que dispone la organización en el proceso de gestión de incidentes, así como la calidad de este.

**2**

Número de simulacros realizados en un año

**%**

Porcentaje de incidentes detectados automáticamente al trimestre.


Disponibilidad del servicio de gestión de incidentes

**4**

Número de incidentes críticos

# INDICADORES DE **RIESGO**

Proporcionan información del riesgo asociado a la gestión correcta o incorrecta de incidentes.

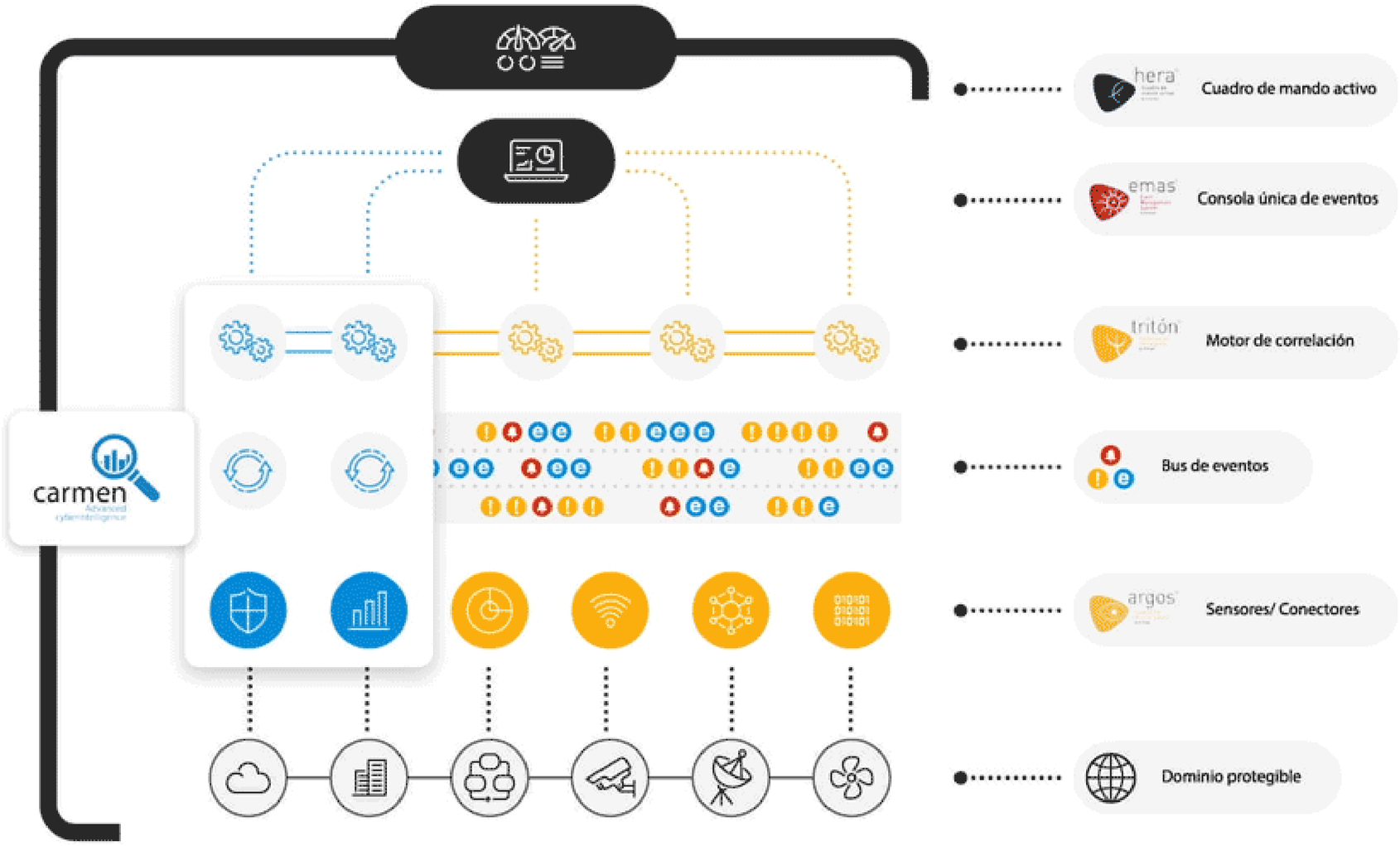
Porcentajes de incidentes MUY CRÍTICOS cuyo plazo es inferior a X horas

Tiempo de respuesta a incidentes MUY CRÍTICOS

**1**

Número de simulacros con un resultado global NEGATIVO

La organización debe definir las **fuentes de datos** y la **metodología de cálculo** y **representación** concretos en cada caso, así como el responsable del indicador, para cada uno de los indicadores definidos.


carmen
hera
Cuadro de mando activo
emas
Consola única de eventos
tritón
Motor de correlación
Bus de eventos
argos
Sensores/ Conectores
Dominio protegible

hera 2.2.0

Sesion | Disponibilidad | Actividad | Calidad | Riesgo | Administración | Ayuda

hera

OK

En curso | Mes anterior | Eventos gestionados

## Eventos totales y muy altos o criticos

**46**

totales de los cuales

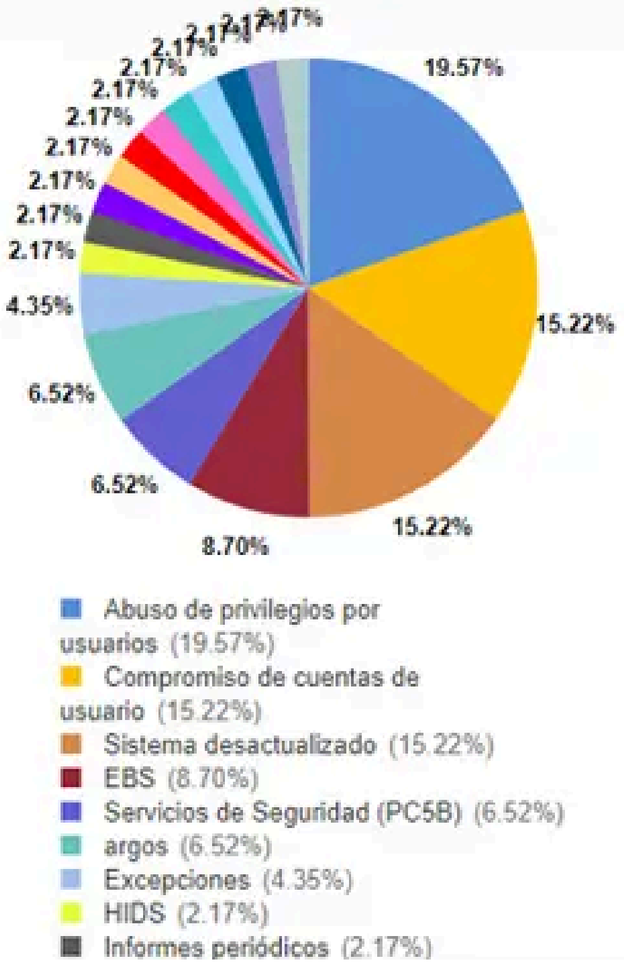
**0**

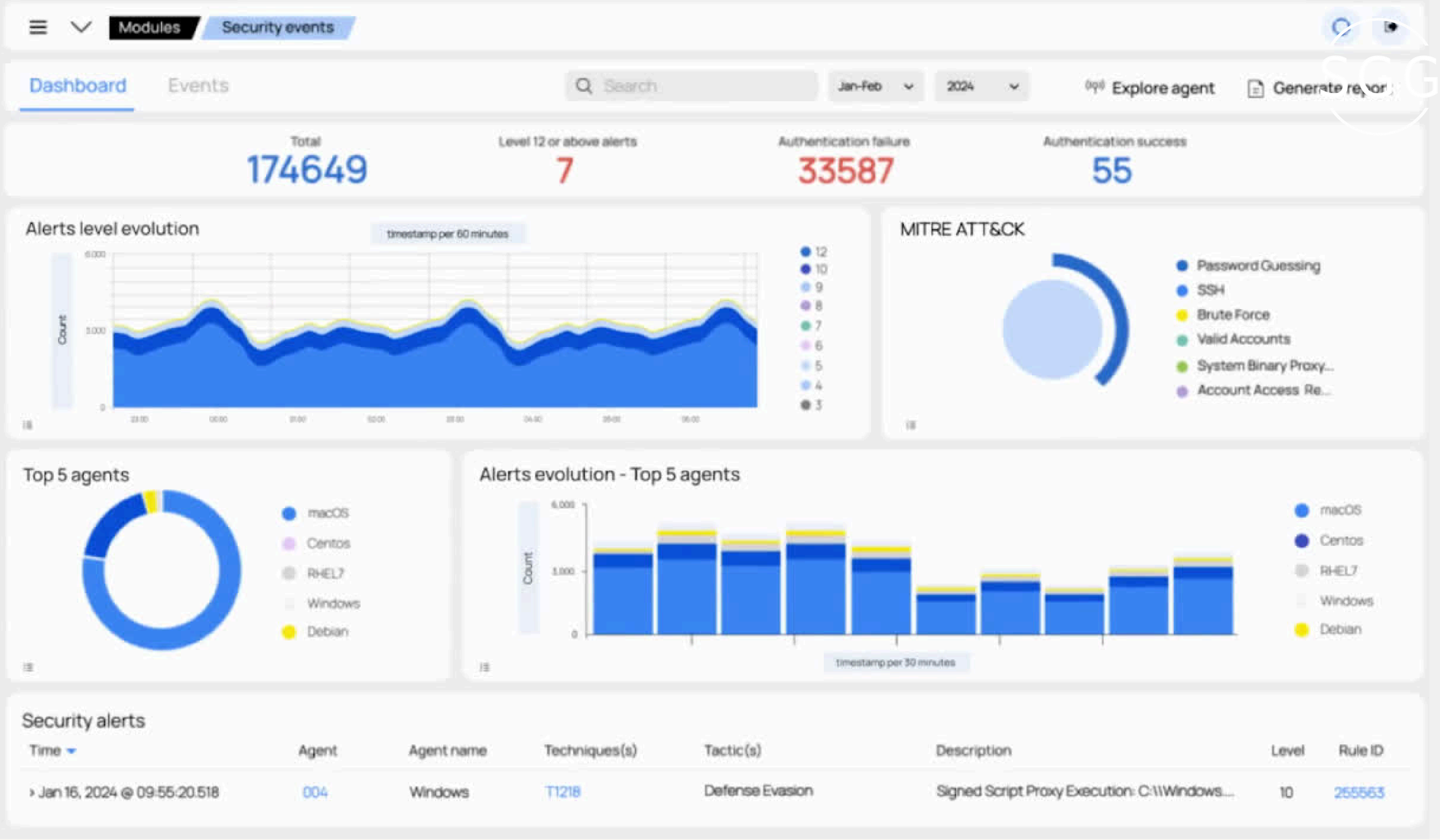
muy altos o críticos

## Tipologia

| Tipos | Totales |
|---|---|
| Abuso de privilegios por usuarios | 9 |
| Compromiso de cuentas de usuario | 7 |
| Sistema desactualizado | 7 |
| EBS | 4 |
| Servicios de Seguridad (PC5B) | 3 |
| argos | 3 |
| Excepciones | 2 |
| HIDS | 1 |
| Informes periódicos | 1 |
| Ataque de fuerza bruta | 1 |
| Explotación de vulnerabilidad software | 1 |
| Otros Incidentes | 1 |
| AUD | 1 |
| Acceso a servicios no autorizados | 1 |
| Virus | 1 |
| Triton (Soporte) | 1 |
| ARGOS | 1 |
| Auditoría de vulnerabilidades | 1 |

## Tipologia según totales




Modules
Security events
Dashboard
Events
Search
Jan-Feb
2024
Explore agent
Generate report
Total
174649
Level 12 or above alerts
7
Authentication failure
33587
Authentication success
55
Alerts level evolution
timestamp per 60 minutes
Count
12
10
9
8
7
6
5
4
3
MITRE ATT&CK
Password Guessing
SSH
Brute Force
Valid Accounts
System Binary Proxy...
Account Access Re...
Top 5 agents
macOS
Centos
RHEL7
Windows
Debian
Alerts evolution - Top 5 agents
Count
timestamp per 30 minutes
macOS
Centos
RHEL7
Windows
Debian
Security alerts
Time
Agent
Agent name
Techniques(s)
Tactic(s)
Description
Level
Rule ID
› Jan 16, 2024 @ 09:55:20.518
004
Windows
T1218
Defense Evasion
Signed Script Proxy Execution: C:\\Windows....
10
255563