Security Information and Event Management

Ciberseguridad Avanzada

¿Qué es SIEM?

SIEM es una solución centralizada que recoge, analiza y correlaciona eventos y registros (logs) generados por infraestructuras TI, con el objetivo de detectar, monitorear y responder a incidentes de seguridad.

- **Funciones clave:**
  - Agregación y normalización de logs.
  - Correlación y análisis de eventos en tiempo real.
  - Alerta automática ante incidentes o patrones sospechosos.
  - Visualización mediante dashboards y reportes auditables.
- **Componentes principales:**
  - Colección de datos, análisis, correlación, gestión de alertas, generación de reportes y respuesta ante incidentes.

Beneficios principales

- **Visibilidad completa:** Integración de logs de múltiples fuentes para una visión holística del entorno TI.
- **Detección proactiva:** Descubrimiento temprano de amenazas avanzadas y patrones de ataque mediante inteligencia artificial y reglas personalizadas.
- **Respuesta acelerada:** Automatización en la generación de alertas y mecanismos de respuesta ante incidentes.
- **Cumplimiento normativo:** Apoyo a auditorías y regulaciones al centralizar información crítica y reportes.
- **Investigación eficiente:** Facilita análisis forense y determina el origen y alcance de amenazas o incidentes.

Desafíos y retos de implementar SIEM

- **Alto volumen de información**: Excesiva generación de logs puede dificultar su gestión y conducción eficiente.
- **Complejidad en la integración:** Consolidar fuentes heterogéneas requiere planificación y recursos técnicos especializados.
- **Reglas de correlación personalizadas:** El desarrollo y mantenimiento de reglas efectivas exige personal con gran experiencia.
- **Falsos positivos:** El SIEM puede inundar a los equipos con alertas irrelevantes si no existe una calibración adecuada.
- **Costo y recursos**: Requiere inversión en infraestructura, licencias y personal cualificado.

Como se despliega un SIEM?

1. Identificar Fuentes/Origenes de los datos.
2. Consolidacion de datos e informacion.
3. Analisis, filtrado, visualizacion de los datos y la informacion.

Funciones Destacadas

1. Gestión de los datos de los logs.
2. Visibilidad de lo que sucede en la red.
3. Para la correlación y análisis de eventos.
4. Proporciona Inteligencia ante amenazas.
5. Ayuda para el cumplimiento de TI.
6. Alertas de seguridad en tiempo real.
7. Generar informes.

Objetivo Principal

Reducir el MTTD y MTTR

Mean Time To Detect

Parámetro que muestra de tiempo medio de detección

Mean Time To Respond

Parámetro que muestra de tiempo medio de respuesta.

SIEM’s destacados

Plataforma	Características Clave	Ventajas	Desafíos / Limitaciones
Splunk	Analítica avanzada, dashboards interactivos, flexibilidad	Intuitivo, gran comunidad, amplia integración	Licenciamiento alto, complejidad en grandes entornos
IBM QRadar	Correlación automática, integración IA, flujo de trabajo	Precisión en detección, fácil gestión de incidentes	Costo inicial, curva de aprendizaje
ArcSight	Alto rendimiento, gestión extensiva de eventos	Escalable, enfoque en grandes organizaciones	Configuración compleja, coste elevado

Recolección de datos

Activo

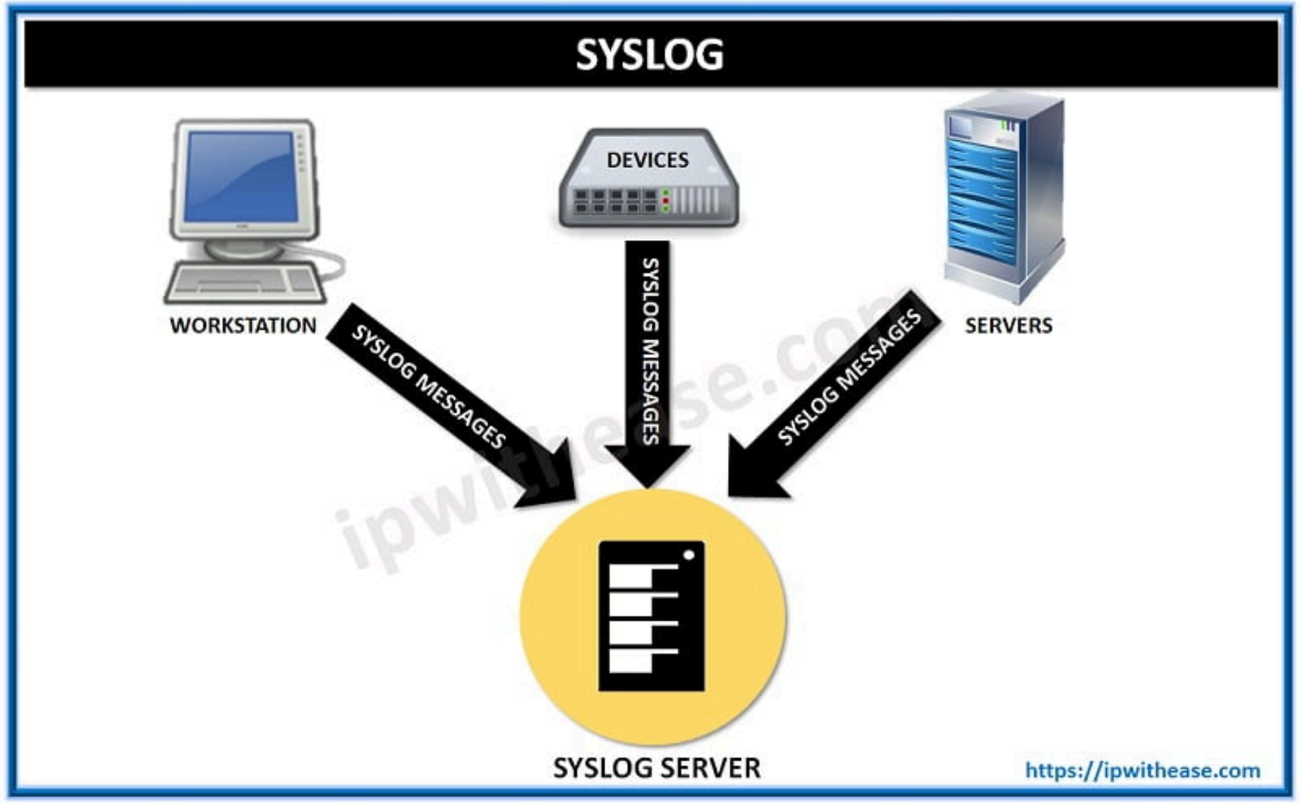
- Consultas BD
- WMI (RPC)
- SCP
- CIFS

Pasivo

- SYSLOG
- Agente

Capas Lógicas - Recolección

SYSLOG



Agentes (conector)

- Parseo
  - Análisis sintáctico del Log, interpretar datos, REGEX
- Normalización
  - Estandarizar campos
- Categorización
  - Agregar etiqueta a los logs, agrupar por eventos similares
- Agregación
  - Agrupa por eventos iguales, dependen del SIEM
- Filtrado
  - Descartar eventos no relevantes

Correlación

- **Funciones**
  - Recepción de Datos.
  - Almacenamiento Temporal
  - Generación de eventos de correlación
  - Notificaciones
  - Análisis/Búsquedas

Almacenamiento

- **Almacenamiento de logs a largo plazo**
  - Tiempo determinado.
  - Rotado
  - Accesibles
  - Centralizacion
  - Logs consultables
  - Integridad

Funcionalidades

- Análisis de fallos simulación de exploits.
- Priorización de vulnerabilidades.
- Análisis y Topologías de red.
- Detección de anomalías de Red.
- Gestión de incidentes.

Toma de Requisitos

- **Definir Alcance**
  - Actividad económica.
  - Para que necesitan el SIEM?
  - Conocimiento real del funcionamiento de la empresa.
- **Cumplimiento**
  - Que normativa cumplir?.
  - Solución SIEM mas adecuad?
    - Importante para simplificar el cumplimiento de la normativa.
  - Documentación.

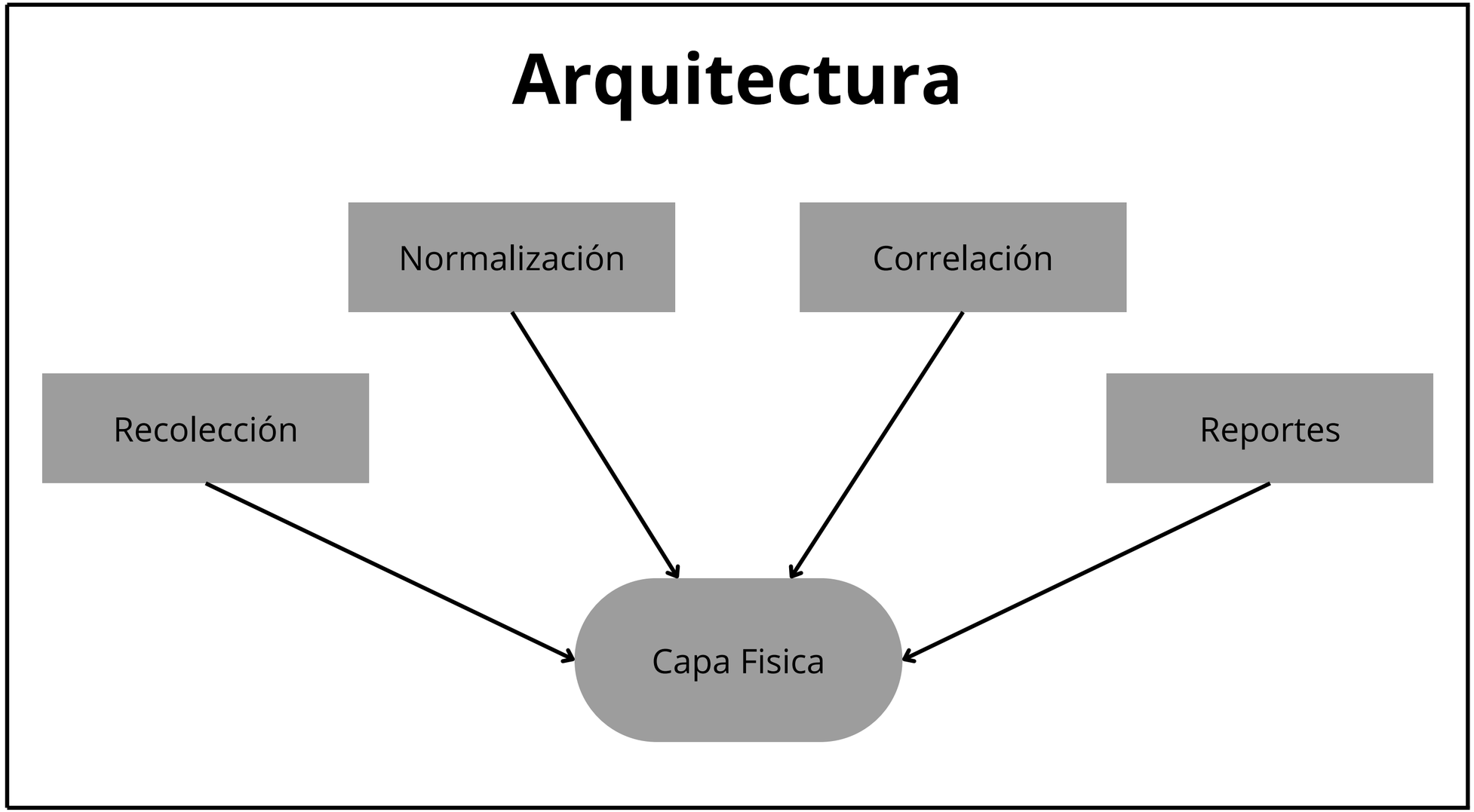
Toma de Requisitos

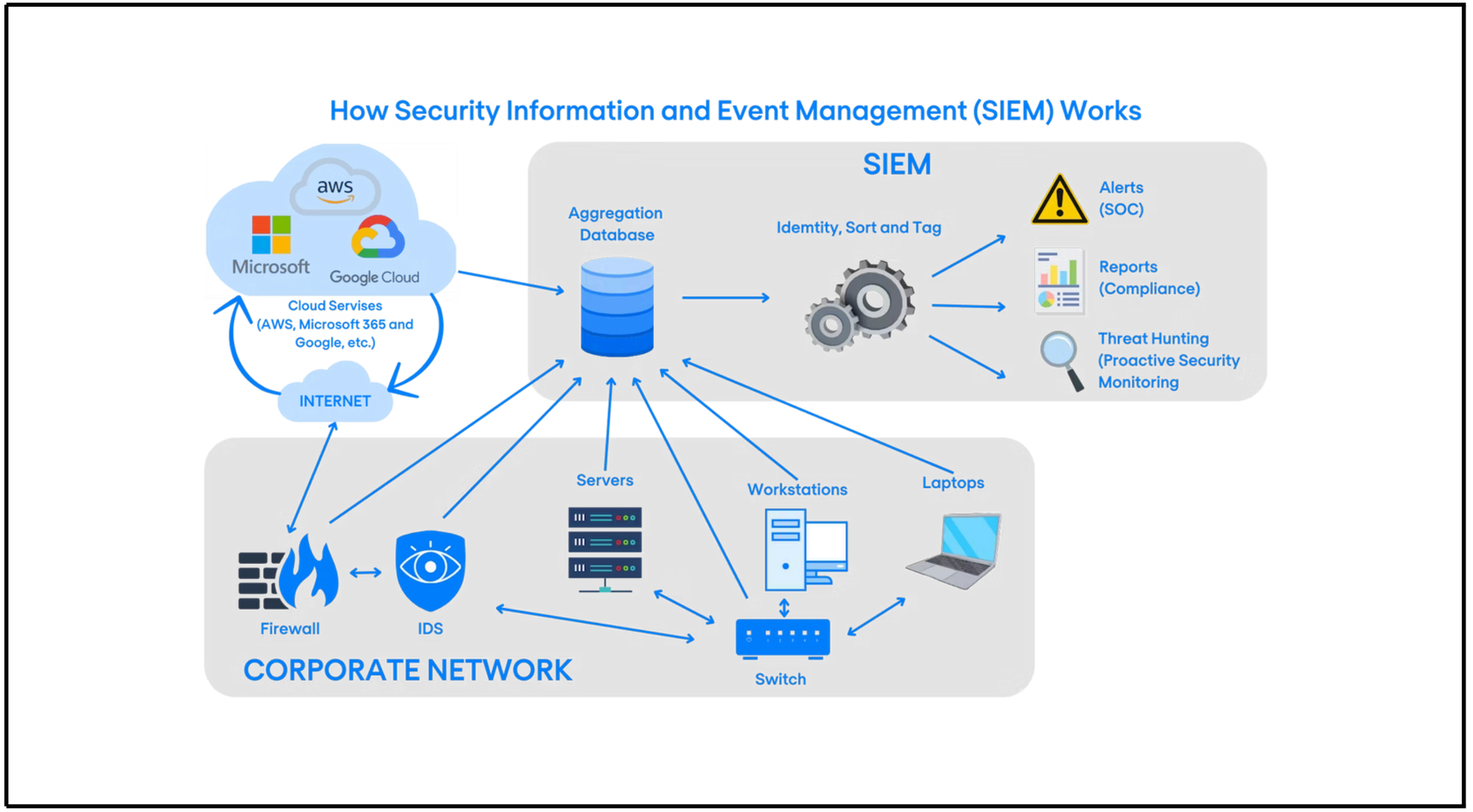
- **Fuentes de Datos**
  - Listado de activos.
  - Solución SIEM mas adecuada?
  - Valor a;adido
- **Recursos Criticos**
  - Necesidades de Protección estrictas.
  - Datos confidenciales
  - Ej: Legacy, sistemas SWIFT

Toma de Requisitos

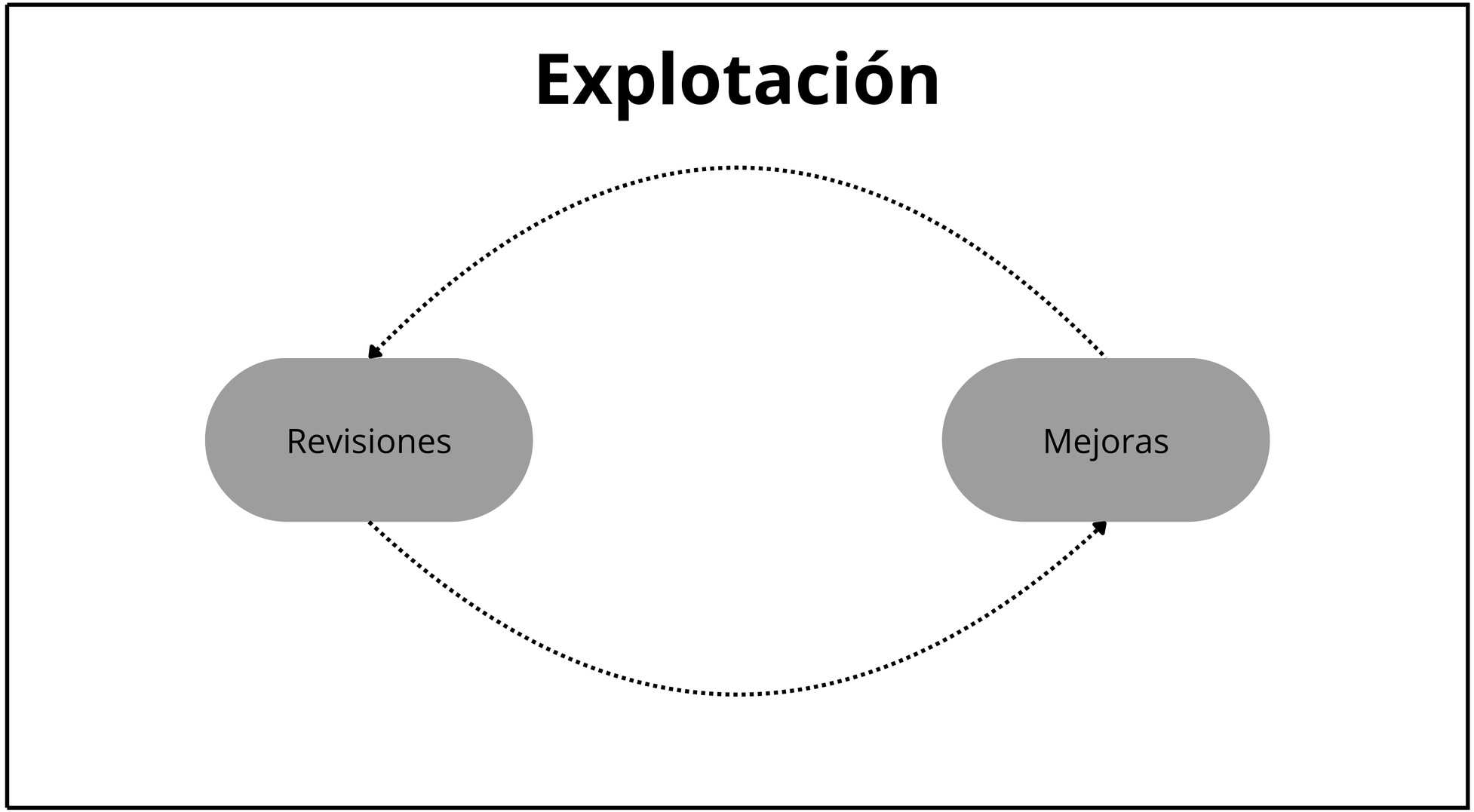
- **Viabilidad Financiera**
  - Costos del Software.
  - Costos del Hardware.
  - Costos de la banda ancha

Implementación




How Security Information and Event Management (SIEM) Works
aws
Microsoft
Google Cloud
Cloud Servises
(AWS, Microsoft 365 and
Google, etc.)
INTERNET
SIEM
Aggregation
Database
Idemtity, Sort and Tag
Alerts
(SOC)
Reports
(Compliance)
Threat Hunting
(Proactive Security
Monitoring
Servers
Workstations
Laptops
Firewall
IDS
CORPORATE NETWORK
Switch

Implementación



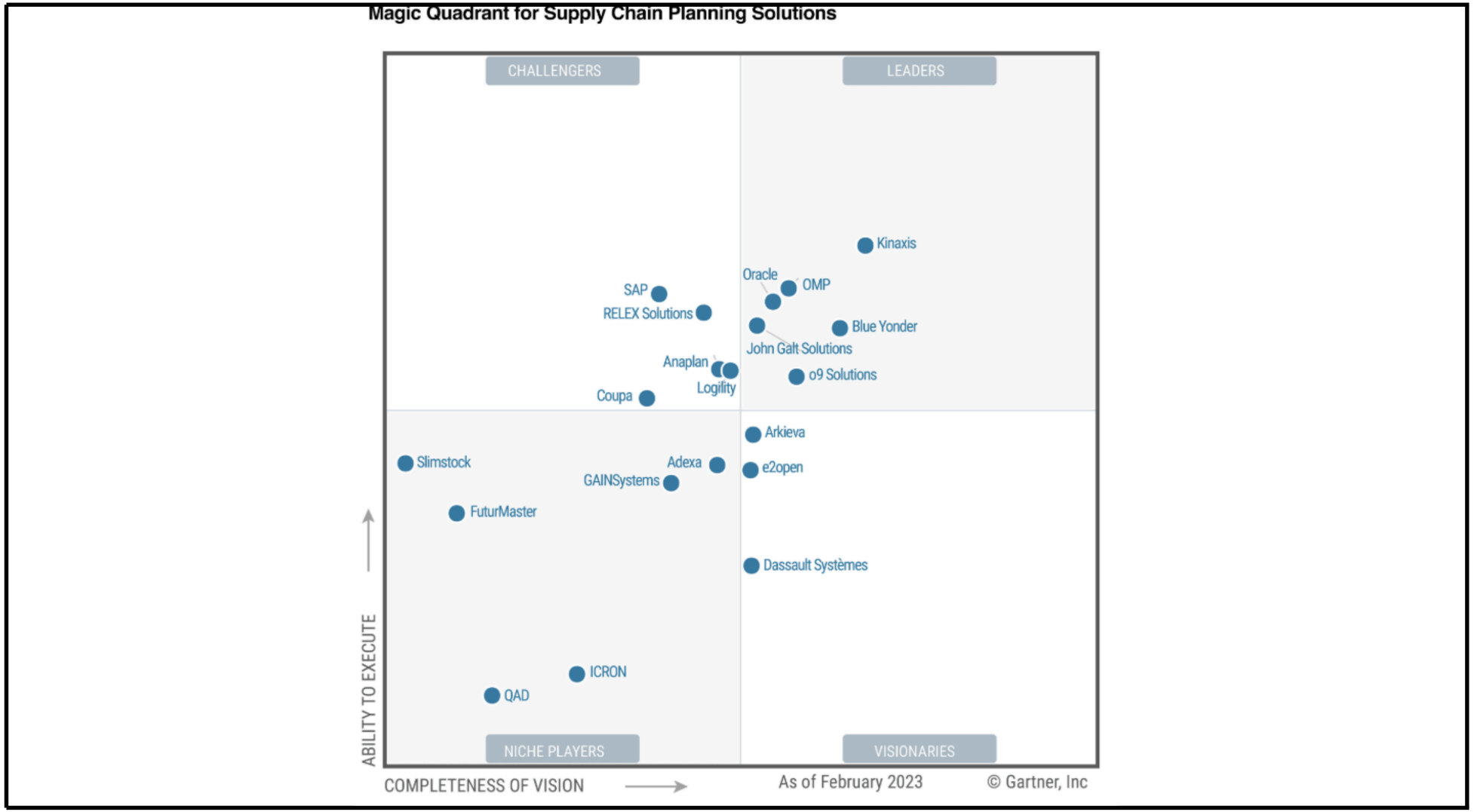
Fabricantes

Gartner Magic Quadrant

Informe que evalúa y posiciona a los principales fabricantes de soluciones.

- **Líderes:** empresas fuertes tanto en visión como en ejecución (ej: Splunk, Microsoft Sentinel, IBM QRadar en ciertos años).
- **Visionarios**: ideas innovadoras pero aún con retos en ejecución.
- **Retadores (Challengers):** gran capacidad operativa pero poca innovación.
- **Nicho:** soluciones especializadas o con mercado limitado.

Fabricantes



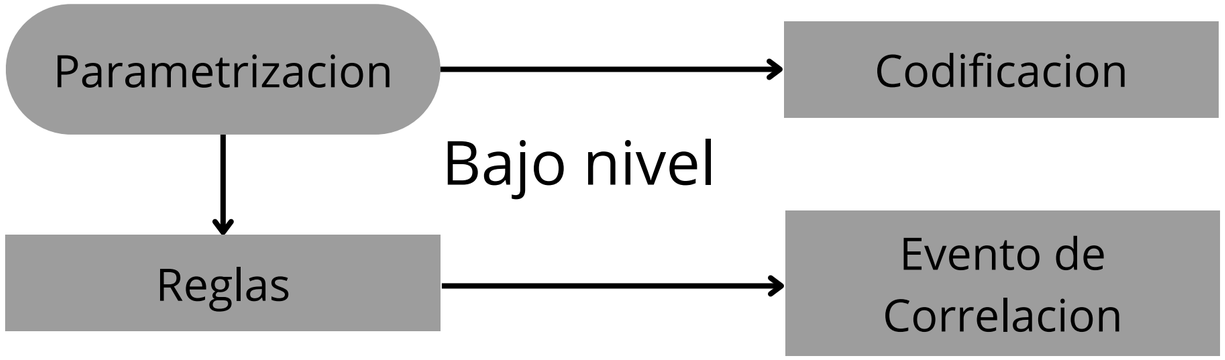
Inteligencia

Tareas de un Analista

- **Análisis de eventos y alertas**
  - Correlacionar logs y actividades sospechosas.
  - Priorizar incidentes según criticidad y contexto.
- **Gestión de reglas**
  - Ajustar y optimizar reglas de correlación para reducir falsos positivos.
  - Crear nuevas reglas basadas en amenazas emergentes.

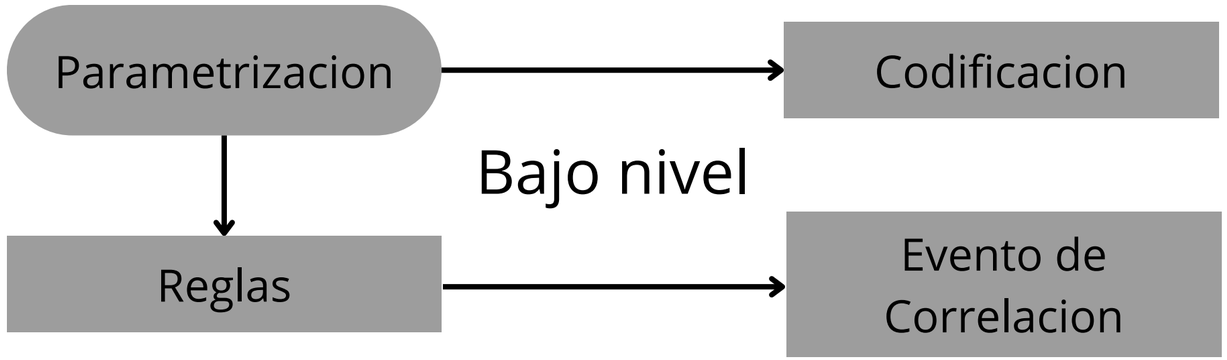
Casos de uso

- Definir escenarios de detección (ej: exfiltración de datos, acceso no autorizado).
- Validar la efectividad de los casos con pruebas y simulaciones.
- Abstracto - Alto nivel



Casos de uso

- **Evento de correlación**
  - Envió emails
  - Informes
  - Actualizar listas
  - Investigación.



Casos de uso

- **Reglas**
  - Dos tipos:
    - Simples
    - Complejas

Simples	**Complejas**
Escaneo a la Nz con acceso denegado	Escaneo a la Nz con acceso concedido

Casos de uso

- **Seguimiento de Usuarios**
  - Ataques de fuerza bruta.
  - Cuentas bloqueadas/Comprometidas.
  - Acceso a recursos no autorizados.
  - Movimientos Laterales - Verticales (AUC).
- **Equipos comprometidos**
  - Detecciones de Malware.
  - Trafico saliente.

Casos de uso

- **Cambios en sistema**
  - Cambios no planeados en sistemas críticos.
  - Control de Cambios
  - Modificación en DLL’s.
  - SYSMON
    - Permite identificar inyecciones de memoria, librerias maliciosas, etc.

Casos de uso

- **IPS - IDS**
  - Firmas - Patrones Coincidentes
  - Detección de políticas (FW dinamico)
  - Anomalías (aprendizaje automático)
- **Anomalías de Red**
  - Escaneos.
  - Exceso de FW deny.
  - Trafico saliente sospechoso.