

# Cómo funciona un SIEM: Una guía práctica



Entendiendo el poder de Cortex SIEM, Gurucul y Splunk en la Ciberseguridad



SEGURIDAD DE LA INFORMACIÓN

# Introducción: ¿Qué es un SIEM?

Un SIEM (Security Information and Event Management) permite centralizar, analizar y correlacionar eventos en tiempo real para detectar amenazas y responder a incidentes.

Ejemplos destacados:

Cortex SIEM: Inteligencia artificial integrada.

Gurucul: Análisis basado en comportamientos.

Splunk: Análisis avanzado y visualización.

# Arquitectura básica de un SIEM



- Componentes principales:
  - Recolectores de datos: Logs y eventos de sistemas.
  - Motor de correlación: Identificación de patrones sospechosos.
  - Almacenamiento de datos: Logs históricos para análisis.
  - Interfaz de usuario: Dashboards y reportes intuitivos.
- Ejemplos:
  - Cortex SIEM: Integración con Palo Alto.
  - Gurucul: Enfoque en patrones de comportamiento.
  - Splunk: Dashboards personalizables.



SEGURIDAD DE LA INFORMACIÓN

# ¿Cómo recolecta datos un SIEM?

- Fuentes de datos:
  - Firewalls (Palo Alto, Fortinet).
  - Soluciones de endpoint (CrowdStrike).
  - Aplicaciones empresariales (Microsoft 365, SAP).
- Métodos:
  - Cortex SIEM: API y Syslog para múltiples dispositivos.
  - Gurucul: Análisis de actividades empresariales.
  - Splunk: Agentes para sistemas locales y nube.



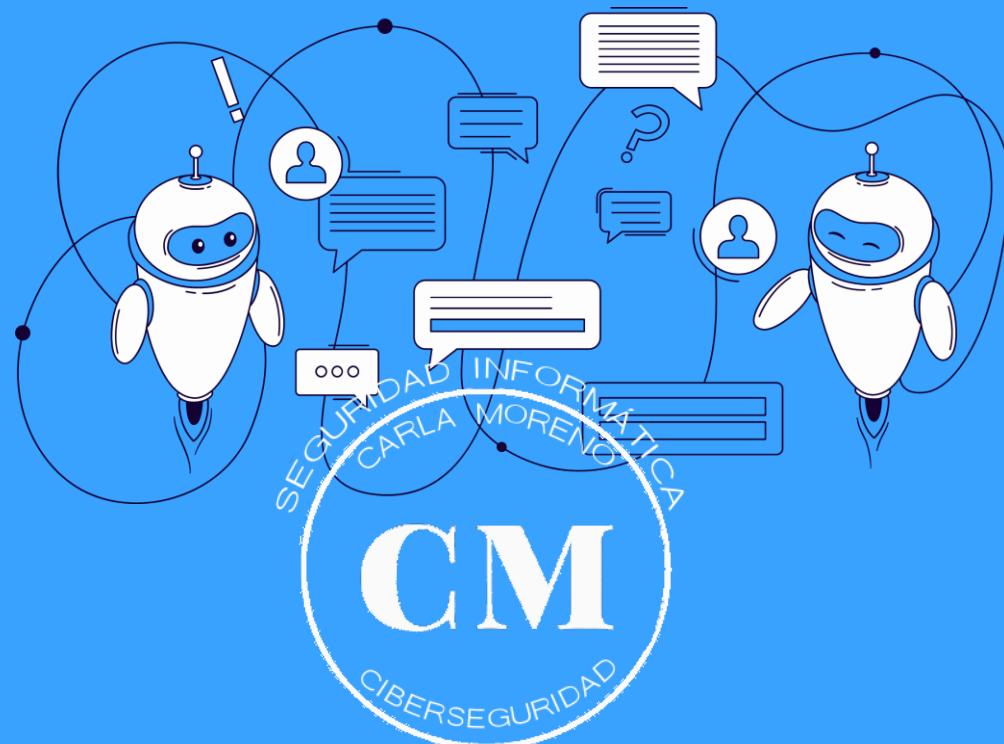
# Proceso de detección y respuesta

## PASOS PRINCIPALES

1. Recolección: Captura de datos en tiempo real.
2. Normalización: Formato estandarizado para análisis.
3. Correlación: Identificación de patrones sospechosos.
4. Generación de alertas: Notificación de amenazas.
5. Análisis y respuesta: Acciones para mitigar riesgos.

## EJEMPLOS

- Cortex SIEM: Reglas basadas en IA.
- Gurucul: Detección por aprendizaje automático.
- Splunk: Alertas visuales y reportes.



SEGURIDAD DE LA INFORMACIÓN

# CASOS DE USO

# CASOS DE USO

# CASOS DE USO



SEGURIDAD DE LA INFORMACIÓN

# Caso de Uso: Cortex SIEM



SEGURIDAD DE LA INFORMACIÓN

Empresa: Proveedor global de telecomunicaciones.

Problema: Intentos de explotación de vulnerabilidades en la nube.

Solución:

- Integración con firewalls Palo Alto y Prisma Cloud.
- Cortex SIEM utiliza IA para correlacionar eventos sospechosos.
- Respuesta automatizada con Cortex XSOAR para bloquear tráfico malicioso.

Resultado:

- Mitigación inmediata de amenazas sin intervención manual.
- Reducción del tiempo de respuesta en un 80%.

# Caso de Uso: Gurucul



SEGURIDAD DE LA INFORMACIÓN

Empresa: Compañía de seguros con 10,000 empleados.

Problema: Posible fuga de información interna.

Solución:

- Modelos de ML analizan patrones de acceso a bases de datos.
- Identificación de accesos inusuales y descargas de documentos.
- Restricción de accesos con alertas de alto riesgo.

Resultado:

- Prevención de fuga de información confidencial.
- Reducción del 90% de falsos positivos en alertas.

# Caso de Uso: Splunk



SEGURIDAD DE LA INFORMACIÓN

Empresa: Banco multinacional con servicios on-premise y en la nube.

Problema: Detectar accesos sospechosos en su infraestructura híbrida.

Solución:

- Splunk Enterprise Security recolecta logs de servidores y firewalls.
- Correlación de eventos para detectar accesos anómalos.
- Automatización con Splunk SOAR para bloquear direcciones IP sospechosas.



Resultado:

- Reducción del tiempo de respuesta en un 65%.
- Prevención de fraude interno detectando credenciales comprometidas.



SEGURIDAD DE LA INFORMACIÓN

EJEMPLO DE CASOS DE USO  
EJEMPLO DE CASOS DE USO  
**EJEMPLO DE CASOS DE USO**

Para detectar fuga de información interna, Gurucul SIEM utiliza Machine Learning y reglas de correlación.

# Cómo configurar un Caso de Uso en Gurucul SIEM



SEGURIDAD DE LA INFORMACIÓN

- ◊ Ingesta de Datos:
  - Active Directory (registros de autenticación)
  - Logs de VPN, accesos a bases de datos
  - Eventos de archivos compartidos y endpoints
  
- ◊ Creación de Modelos de ML:
  - Perfil de usuario basado en historial de accesos
  - Detección de descargas inusuales o accesos fuera de horario
  - Generación de alertas con índice de riesgo

# Ejemplo de Regla de Detección en Gurucul SIEM



SEGURIDAD DE LA INFORMACIÓN

## ◊ Regla en JSON:

```
{  
  "ruleName": "Descargas Inusuales",  
  "conditions": {  
    "userBaselineDownloadCount": { "greaterThan": "3x" },  
    "timeOfDay": "fuera_horario",  
    "deviceType": "desconocido"  
  },  
  "actions": {  
    "alertSeverity": "High",  
    "notifySOC": true,  
    "autoBlockAccess": true  
  }  
}
```



## ◊ Resultado:

- Se genera una alerta si el usuario descarga archivos en horarios inusuales
- Se puede bloquear temporalmente el acceso a los datos críticos.

# Automatización de Respuesta con Gurucul SOAR



SEGURIDAD DE LA INFORMACIÓN

- ◊ Acción Automática con Python:  
Si un usuario descarga datos sospechosos:

- 1 Se envía alerta al SOC con índice de riesgo
- 2 Se bloquea temporalmente el acceso
- 3 Se requiere autenticación adicional

Ejemplo de código en Python para bloquear un usuario:

```
...  
import requests  
  
api_url = 'https://soar.gurucul.com/api/block_user'  
  
data = {'user_id': 'empleado123', 'action': 'disable_account'}  
  
response = requests.post(api_url, json=data)  
  
print(response.json())  
...
```

# Monitoreo y Ajuste del Modelo en Gurucul



SEGURIDAD DE LA INFORMACIÓN

- ◊ ¿Cómo mejorar la detección de amenazas internas?
    - Ajustar umbrales de riesgo para reducir falsos positivos
    - Reentrenar modelos de Machine Learning con nuevos datos
    - Integrar SOAR para automatizar más respuestas
-  Impacto esperado:
- 90% menos falsos positivos
  - Respuesta automática ante riesgos internos
  - Mayor control sobre accesos y filtraciones de datos

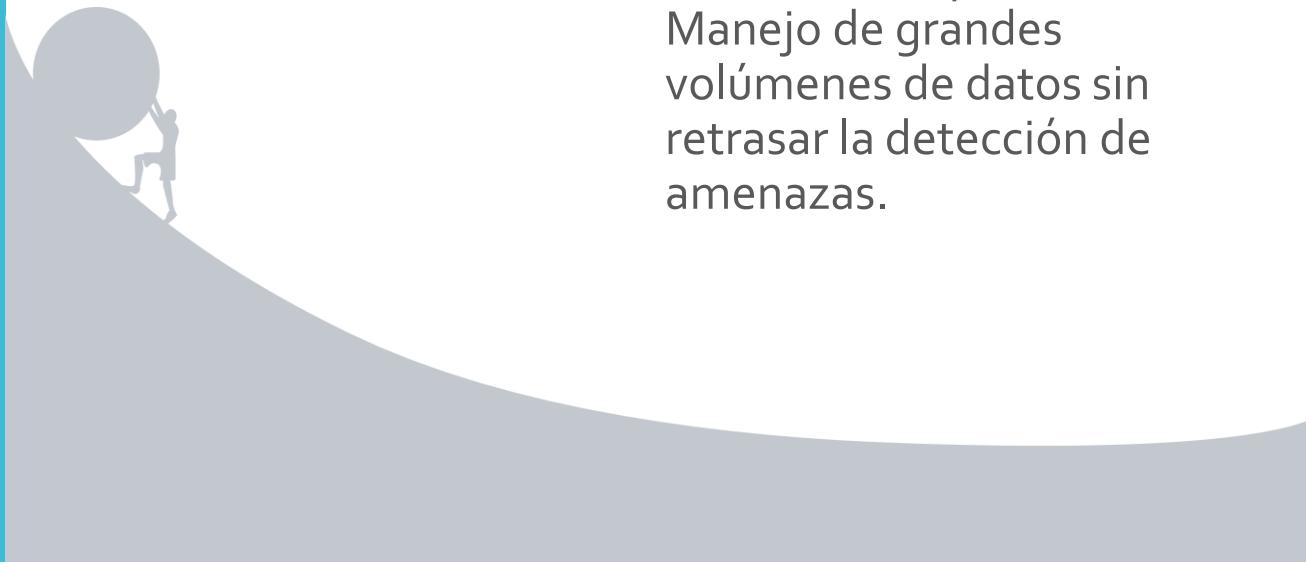
# Beneficios y desafíos



SEGURIDAD DE LA INFORMACIÓN

## Beneficios:

- Detección avanzada
- Cumplimiento normativo
- Visibilidad centralizada



## Desafíos:

- Falsos positivos: Ajustes iniciales necesarios.
- Requerimientos de almacenamiento: Gestión de logs históricos.
- Escalabilidad y rendimiento: Manejo de grandes volúmenes de datos sin retrasar la detección de amenazas.

Comparación de SIEM: Splunk vs. Cortex SIEM vs. Gurucul	Característica	Splunk	Cortex SIEM	Gurucul
	Enfoque	Análisis avanzado y visualización de datos	Integración con Palo Alto y análisis basado en IA	Análisis de comportamiento y detección de amenazas internas
	Casos de uso principal	Detección de amenazas en entornos híbridos	Análisis y correlación en tiempo real con seguridad en la nube	Predicción de ataques internos y análisis de riesgo basado en ML
	Ventajas	Alta personalización y dashboards intuitivos	Automatización y respuesta rápida con IA	Predicción avanzada con modelos de ML y análisis de identidad
	Ideal para	Empresas con grandes volúmenes de datos	Organizaciones con seguridad basada en Palo Alto	Entidades que requieren prevención de amenazas internas



SEGURIDAD DE LA INFORMACIÓN

# Conclusión

Los SIEM como Splunk, Cortex SIEM y Gurucul son herramientas indispensables para proteger los activos de las organizaciones. Cada uno tiene un enfoque único que se adapta a diferentes necesidades empresariales.

Sígueme en  
mis redes  
sociales



<https://www.linkedin.com/in/carlamorenogamboa1411/>



<https://www.youtube.com/@secumomdiaries>



<https://github.com/secumomdiaries>



SEGURIDAD DE LA INFORMACIÓN