OpenText™ - ArcSight™ SIEM & SecOps

Gestión Integral de Información, Eventos de Seguridad y Operaciones de Seguridad (SecOps)

RESUMEN EJECUTIVO

Solución integral de SIEM y SecOps diseñada para proporcionar detección de amenazas en tiempo real, análisis masivo de registros y respuesta automatizada ante ciberataques avanzados. Procesa más de 100,000 EPS y reduce hasta un 90% el volumen de alertas mediante inteligencia de correlación, optimizando la capacidad operativa del Centro de Operaciones de Seguridad (SOC).

ESPECIFICACIONES CLAVE

Atributo	Detalle
Capacidad de Procesamiento	> 100,000 EPS (Eventos por segundo) en tiempo real.
Inversión y Escalabilidad	Reducción del 90% en volumen de alertas mediante correlación e IA.
Integración de Fuentes	> 480 Conectores nativos (SODP SmartConnectors) y FlexConnector.
Automatización SOAR	Playbooks visuales con > 120 plugins e integraciones externas
Almacenamiento y Búsqueda	Base de datos columnar optimizada para consultas en lenguaje natural.
Análisis de Comportamiento	Motor UEBA basado en Machine Learning (ArcSight Intelligence)
Cifrado y Privacidad	Voltage SecureData (Format Preserving Encryption - FPE)
Modelos de Despliegue	SaaS (Amazon S3), On-Premises Containerized, Nube Privada/Soberana.

BENEFICIOS CLAVE Y RETORNO DE INVERSIÓN (ROI)

- **Reducción de Costos Operativos y TCO.** Cierra hasta un 33% de los incidentes de forma 100% automatizada mediante su motor SOAR nativo, disminuyendo la carga manual sobre el equipo de analistas.
- **Mitigación de la Fatiga de Alertas.** Elimina duplicados y filtra ruido en un 90%, permitiendo que el personal del SOC se concentre únicamente en eventos de alto impacto estratégico.
- **Cumplimiento Normativo Acelerado.** Incluye más de 100 reportes y tableros preconfigurados (CIPs) para normativas como GDPR, PCI-DSS, FIPS 140-2, IT-GOV y OWASP.
- **Visibilidad Mitre ATT&CK® y D3FEND.** Mapeo interactivo en tiempo real integrado con feeds de inteligencia GTAP Plus para aplicar contramedidas proactivas.
- **Continuidad del Negocio Garantizada.** Arquitectura de Alta Disponibilidad (HA) multiobjetivo con failover automático entre sistemas ESM.

NOTAS DE USO Y APLICACIONES RECOMENDADAS

Centros de Operaciones de Seguridad (SOC) de Alta Madurez

Procesamiento masivo de eventos en tiempo real con priorización dinámica de riesgo bajo estándares NIST.

Entornos Híbridos y Multicloud

Monitoreo y centralización de logs en infraestructura local (On-Premises), AWS, Azure y Google Cloud.

Sector Financiero y Gobierno

Proyectos con altos requisitos de privacidad de datos sensibles donde se requiere cifrado FPE y soberanía estricta de la información.

Confidencial — Uso comercial autorizado. Propiedad intelectual de Grupo CONSISA. Prohibida su reproducción sin autorización.