OpenText™ EnCase™ DFIR

Forensia Digital, Adquisición Remota y Respuesta a Incidentes (DFIR)

RESUMEN EJECUTIVO

Estándar de la industria en investigación forense digital, análisis de evidencia admisible en juzgados y respuesta a incidentes a escala empresarial. Permite auditar, recolectar y preservar datos en más de 36,000 perfiles de dispositivos y escalar investigaciones a más de 1,000,000 de endpoints de forma remota bajo arquitectura Zero Trust.

ESPECIFICACIONES CLAVE

Atributo	Detalle
Análisis Forense Profundo	EnCase Forensic: Adquisición de disco/memoria, Artifacts Explorer y categorización por IA.
Investigación Remota	EnCase Endpoint Investigator: Escaneo discreto y adquisición fuera de VPN en modelo Zero
Forensia Móvil e IoT	EnCase Mobile Investigator: Soporte para > 35,000 perfiles, bypass, OCR y extracción en nube.
Gobierno de ESI	EnCase Information Assurance: Identificación, recolección y preservación remota de ESI.
Hardware Forense	EnCase Forensic Equipment: Bloqueadores de escritura (write-blockers) y duplicadores portátiles.
Sistemas Operativos	Soporte multiplataforma mediante agentes ligeros para Windows, macOS, Linux y UNIX.
Modelos de Despliegue	Servidor centralizado On-Premises, Nube Privada y Entornos Híbridos multi-sede.

BENEFICIOS CLAVE Y RETORNO DE INVERSIÓN (ROI)

- **Admisibilidad Jurídica Garantizada.** Genera evidencia científicamente respaldada y jurídicamente válida bajo estándares globales (.E01/.Ex01), reduciendo riesgos en litigios y procesos penales.
- **Reducción de Costos de Desplazamiento y Operación.** La adquisición remota fuera de VPN permite investigar incidentes sin necesidad de enviar personal técnico en sitio ni interrumpir al usuario final.
- **Aceleración del Triaje con IA.** Módulo Artifacts Explorer y categorización inteligente de imágenes que automatizan la priorización de artefactos críticos del sistema operativo.
- **Capacidad de Respuesta Masiva ante Brechas.** Permite contener y auditar hasta 1,000,000 de endpoints simultáneamente durante incidentes de ciberseguridad a gran escala.
- **Investigación Unificada Móvil y Nube.** Unifica la recolección de evidencia física, dispositivos móviles y servicios en la nube (Google Drive, redes sociales) en un solo flujo de trabajo.

NOTAS DE USO Y APLICACIONES RECOMENDADAS

Unidades de Respuesta a Incidentes (CSIRT/SOC) y Forensia

Análisis profundo de amenazas persistentes avanzadas (APT) y respuesta rápida ante intrusiones corporativas.

Departamentos Legales, Cumplimiento y eDiscovery

Identificación y preservación de Información Almacenada Electrónicamente (ESI) para procesos judiciales o auditorías.

Organismos Policiales y Agencias Gubernamentales.

Investigaciones judiciales de delitos informáticos con inspección física y extracción en dispositivos móviles o de campo.

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