

OnLine Digital Forensic Suite™

.....la nueva generación de software para investigaciones de sistemas en vivo

Respuesta a Incidentes – E-discovery – Compliance

Rápida respuesta a incidentes de seguridad en cómputo

Examine sistemas en vivo de forma rápida sin impacto en las operaciones del negocio

OnLine Digital Forensic Suite™ de Cyber Security Technologies facilita las investigaciones de una forma sencilla y eficaz de sistemas de cómputo que no puedan o no deban ser apagados.

Online DFS está diseñado para ser usado por profesionales que se desempeñan en el área de seguridad de tecnologías de información; ya sea en la iniciativa privada, agencias gubernamentales o incluso en agencias de procuración de justicia. Es una valiosa herramienta para la respuesta a incidentes en tiempo real, para el descubrimiento en línea y las auditorías de cumplimiento de forma no intrusiva.

OnLineDFS se despliega y opera fácilmente, se apega a las mejores prácticas de análisis forense digital y provee un amplio conjunto de herramientas para la adquisición, búsqueda y análisis de los datos. Para asegurar la exactitud de toda la información colectada y analizada, OnLineDFS automatiza el registro y reporte de todas las acciones de investigación.

Análisis de Sistemas de Cómputo en operación Investigación on-line desde cualquier ubicación

- Examine una computadora en operación
 - Realice investigaciones de forma discreta y sin afectar las operaciones.
 - Examine sistemas de misión crítica sin tiempos muertos.
- Capture y registre información volátil del sistema objetivo
 - Recolecte información vital de programas en ejecución, conexiones de red, transmisiones de datos e información de la memoria y el registro.
 - Rescate información que se perdería si el sistema fuera apagado.
 - Reúna información de contexto.
 - Examine automáticamente sistemas seleccionados periódicamente.
- Obtenga datos estáticos de forma selectiva, desde un archivo hasta unidades enteras, enfocando la investigación únicamente en la información relevante para el mismo

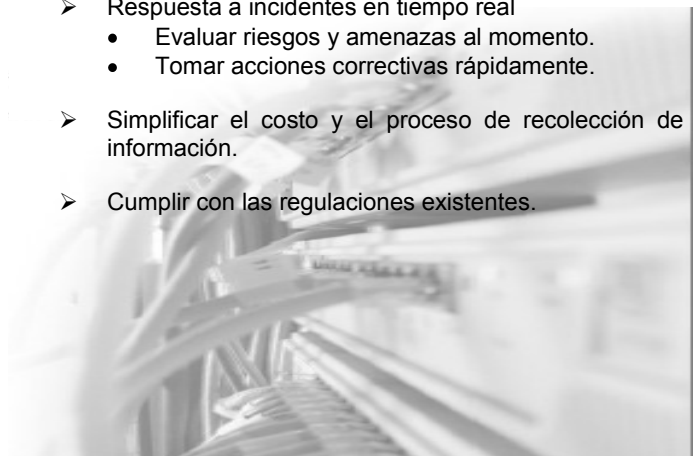
Rápida Respuesta: Al enfrentarse a una violación de las políticas de seguridad, ya sea proveniente desde el exterior o dentro de la organización, OnLineDFS permite realizar una investigación en tiempo real.

Investigaciones No-Intrusivas: OnLineDFS permite investigar de forma rápida, capturando datos relevantes, tal como el estado en ejecución, mientras el sistema que se está investigando continúa con sus operaciones

Investigaciones en Sitio o Remotas: Con OnLineDFS se tiene la capacidad de trabajar en sitio y de forma remota, ahorrando tiempos de traslado y gastos adicionales .

Beneficios

- Dirigir investigaciones de forma inmediata.
- Reducir los costos de las investigaciones.
- Trabajar discretamente sin afectar el equipo objetivo.
- Respuesta a incidentes en tiempo real
 - Evaluar riesgos y amenazas al momento.
 - Tomar acciones correctivas rápidamente.
- Simplificar el costo y el proceso de recolección de información.
- Cumplir con las regulaciones existentes.



Especificaciones y Características

Instalación y Operación Sencilla

- Sólo una instalación de OnlineDFS es necesaria para investigar todas las computadoras detrás de un firewall.
- No se requiere pre-instalar ningún software en la computadora objetivo.
- Una investigación con OnLineDFS puede ser realizada de forma local o vía remota a través de conexiones seguras.

Almacenamiento de Información y Conectividad

- Los datos recolectados pueden ser almacenados en el disco duro interno del sistema OnLineDFS o en dispositivos de almacenamiento externo; ya sea para movilidad o aislamiento de la evidencia digital.
- Los investigadores pueden acceder a OnLineDFS a través de un navegador de Internet capaz de realizar conexiones seguras (SSL) vía el protocolo HTTPS, tales como Internet Explorer 4.0 (o superior), Mozilla Firefox, Mozilla Suite y Netscape Navigator 4.0 (o superior).

Plataformas Soportadas para Analizar

Microsoft Vista (Disponible a mediados del 2008)
Microsoft Windows XP Professional
Microsoft Windows 2000
Microsoft Windows NT 4.0 o superior
Microsoft Windows Server 2003
Versiones populares de Unix y Linux

Principales Características

- Investigación de sistemas en operación en tiempo real.
- Recolección de información del sistema objetivo en estado de ejecución.
- Captura de información en memoria y del registro.
- Aplicación que trabaja por comunicación en red no intrusiva.
- Aplicación a control remoto que se usa a través de un navegador de Internet y un enlace de comunicaciones.
- Herramientas para el ordenamiento y análisis de los datos.
- Extensas capacidades de búsqueda.
- Recolecciones de información programadas.
- Visor de múltiples tipos de archivos.
- Captura de archivos individuales o de la unidad entera.
- Generación de reportes en formatos ordenados y estructurados.
- Procesos documentados, estructurados y apegados a las buenas prácticas del análisis forense digital.
- Autenticidad verificada a través de firmas digitales.
- Generación de bitácoras automáticamente para un buen seguimiento.
- Marco de trabajo consistente para las investigaciones.



an affiliate of Architecture Technology Corporation

9977 Valley View Road * Suite 200 * Eden Prairie, MN 55344
Telephone: 952-937-6258 * Fax: 952-937-1998 * info@cyberstc.com *
www.cyberstc.com

Distribuidor para Latinoamérica:
Mattica

Bosque de Radiatas # 22 – 104. Col. Bosques de las Lomas, México, D.F., 05120, México
+52 (55) 13 27 8050 * contacto@mattica.com * www.mattica.com

