

MAGNET AXIOM CYBER™

Simplifique sus Investigaciones

Una potente solución forense digital diseñada especialmente para satisfacer las necesidades de organizaciones y proveedores de servicios que necesitan recopilar, analizar y reportar evidencia obtenida de computadoras, servicios en la nube, IoT y dispositivos móviles.

```
146 </li>
147 </ul>
148 </div>
149 );
150 }
151 }
152
153 renderWhatNewLink() {
154   return {
155     <div className={style
156     <h4 className={style
157     <ul className={Clas
158       {this.renderWha
159       {this.renderWha
160       {this.renderWha
161       {this.renderWha
162       {this.renderWha
163       {this.renderWha
164       {this.renderWha
165     </ul>
166   </div>
167
168   renderWhatNewItem(title, url
169   return {
170     <li className={style.foo
171     <h4
172     <li className={style.foo
173     <h4
174     href={trackUrl(url)}
175     target="_blank"
176     rel="noopener noreferrer"
177   >
178     {title}
179   </li>
180 }
181 }
```

La Nube

Los servicios de almacenamiento y comunicación en la nube han cambiado la forma en que los equipos se comunican, comparten y almacenan información.

Aproveche las credenciales de administrador o usuario para acceder a los registros de auditoría y examinar las cuentas en la nube de los trabajadores sin avisarles sobre una investigación en curso.

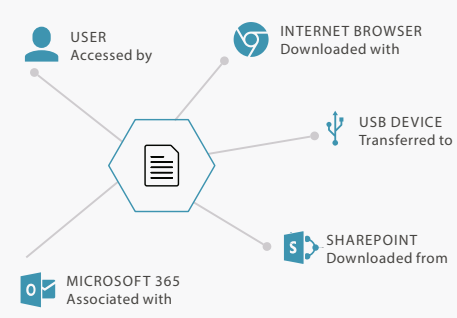
AXIOM Cyber adquiere y analiza información de los servicios corporativos de almacenamiento en la nube como AWS S3, EC2 y Azure, además a otras fuentes en la nube, incluidas Microsoft 365, Google Workspace, Box, Dropbox, Slack y iCloud.



Computadora

AXIOM Cyber proporciona las más completas y potentes herramientas de recuperación, búsqueda, análisis y de reportes para Mac, PC y Linux.

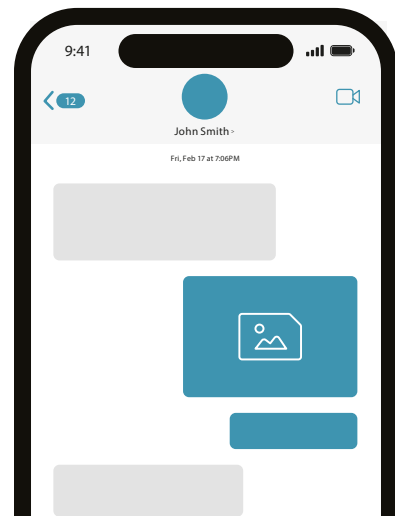
Obtenga información procesable sobre la actividad y los ejecutables en la memoria física de un end point, así como los procesos que se ejecutan solo en la memoria, como las amenazas persistentes avanzadas (APT) que aprovechan las técnicas sin archivos.



Móvil

Ya sea que el dispositivo móvil laboral sea propiedad del trabajador o proporcionado por la empresa, convierta a AXIOM Cyber en una parte esencial de su kit de herramientas para investigaciones en iOS y Android.

Técnicas de análisis y tallado integral que permiten encontrar más artefactos forenses como el historial de navegación, chats, correos electrónicos y documentos. Visualice y presente evidencias fácilmente mostrando correos electrónicos y chats en su formato original, a menudo necesarios para las investigaciones de RR.HH., como mala conducta de los empleados o situaciones de acoso.



MAGNET AXIOM CYBER™

Todas las organizaciones, independientemente de su tamaño, caen víctimas de amenazas y ataques de ciberseguridad a diario. Con un enfoque en artefactos forenses y la incorporación de adquisición remota, Magnet AXIOM Cyber le permite comprender rápidamente los incidentes de seguridad, a fin de que pueda salvaguardar a su empresa de futuras amenazas.

Podrá usar AXIOM Cyber para investigación de RR.HH. o de amenazas internas, así como analizar las causas raíz para una adecuada respuesta a incidentes.

RECOPIACIÓN REMOTA

AXIOM Cyber le permite realizar de manera rápida y discreta, recopilaciones remotas de dispositivos Mac y Windows a un contenedor AFF4-L con solidez forense. Se conectará automáticamente al objetivo en caso de desconexión y continuará con la recopilación desde donde lo dejó.

Mediante el uso de agentes compartidos, varias instancias de AXIOM Cyber pueden recopilar desde un end point sin necesidad de implementar un agente diferente cada vez.

UTILICE AXIOM CYBER EN LA NUBE

Ejecute AXIOM Cyber en Azure o AWS para aprovechar los beneficios del procesamiento en la nube más la capacidad de realizar recopilaciones remotas aun estando fuera de la red.

REDUCE LA COMPLEJIDAD

El enfoque en artefactos forenses de AXIOM Cyber permite la presentación inmediata de los datos necesarios para avanzar con facilidad y eficacia en el caso. Obtenga datos de una variedad de fuentes, incluyendo computadoras, dispositivos móviles y cuentas corporativas en la nube.

Luego, podrá hacer uso de potentes funciones de análisis como Timeline, Connections, reglas YARA y Magnet.AI, que le ahorrarán tiempo y molestias.

ADQUISICIÓN AVANZADA EN LA NUBE

Use credenciales de administrador para adquirir datos de Microsoft 365, Google Workspace, y Box, de manera que no alerte a los trabajadores que son parte de una investigación en curso.

Miles de organizaciones de todo el mundo confían en los productos de Magnet Forensics para su protección, mediante una gran variedad de investigaciones cibernéticas:

MALA CONDUCTA DEL EMPLEADO

Junta todas las piezas del rompecabezas examinando artefactos forenses del sistema de archivos, cuentas en la nube, memoria y dispositivos móviles, cuando se trate de reclamos de acoso en el lugar de trabajo o mal uso de los activos corporativos.

SOPORTE PARA eDISCOVERY

Acelere y simplifique la evaluación temprana de casos, proporcionando a los socios de eDiscovery los datos que necesitan. Genere un archivo de carga que contenga datos seleccionados, analizados y etiquetados para su posterior revisión.

ROBO DE I.P.

Cuando se trata de casos de filtración de datos, es fundamental ver todo el historial de un archivo. Podrá comprender el historial de un archivo a través de todas las fuentes probatorias, incluyendo Microsoft 365, Google Workspace y almacenamiento en la nube AWS.

RESPUESTA A INCIDENTES

Las intrusiones en la red, correo corporativo comprometido, el malware y los ataques de ransomware, tienen consecuencias catastróficas en una empresa. El potente conjunto de herramientas de AXIOM Cyber le permitirá comprender cómo ocurrió un incidente para que pueda ser prevenido en el futuro..

CANALES DE CONTACTO:

✉ info@hansgross.com.pe
☎ (+51) 971 596 045
☎ (044) 467335

Facebook Hans Gross
Instagram hansgrossperu
LinkedIn Hans Gross

