Clavis consolida su alianza con Axur, reduciendo en un 50% el tiempo de respuesta a incidentes

Sobre la empresa

Industria: Seguridad de la Información
Expertise: Más de 20 años en el mercado
Tamaño: Más de 130 especialistas en ciberseguridad con un amplio conjunto de soluciones

Desafío

Clavis buscaba mejorar sus capacidades de inteligencia de amenazas para ofrecer respuestas más rápidas y precisas a sus clientes. Aunque ya contaba con múltiples fuentes de monitoreo, algunos clientes comenzaron a notar que Axur detectaba amenazas críticas que no eran identificadas por otras soluciones—especialmente en casos de credenciales expuestas y filtraciones de datos. Estos desafíos impulsaron la búsqueda de un nuevo socio.

Solución

Con Axur, Clavis amplió su portafolio de inteligencia de amenazas, incorporando soluciones como Threat Hunting, monitoreo avanzado en la Deep & Dark Web y respuestas más ágiles frente a incidentes críticos, como exposición de credenciales e información sensible. Además de aumentar la precisión en las detecciones, la empresa fortaleció su posición como referente en seguridad de la información, ofreciendo un servicio aún más estratégico para sus clientes.

Threat Hunting: Investigando más allá de los activos monitoreados

Con la solución de Threat Hunting de Axur, el equipo de Clavis adquirió mayor capacidad estratégica para investigar incidentes en profundidad, correlacionando credenciales expuestas con otros indicadores de compromiso. Esto permitió obtener un contexto mucho más claro para cada incidente.

En un caso crítico, un cliente fue acusado de haber sufrido una filtración de datos. Mediante el uso del Threat Hunting de Axur, el equipo de Clavis rastreó el origen de la exposición y determinó que las credenciales comprometidas estaban relacionadas con un malware del tipo infostealer.

La investigación reveló que los datos fueron capturados desde dispositivos infectados incluso antes de que hubiera interacción con los sistemas de la empresa, descartando la hipótesis de una filtración interna. Este análisis técnico permitió que Clavis brindara pruebas contundentes para respaldar a su cliente, mitigando significativamente el impacto reputacional del incidente.

Gracias a una inteligencia de amenazas más robusta y respuestas más precisas ante incidentes, Clavis se consolidó como un socio estratégico para sus clientes, yendo más allá de la detección para entregar insights accionables y soporte especializado.

Su capacidad para anticiparse a riesgos, correlacionar amenazas y ofrecer respuestas basadas en evidencia fortaleció la confianza del mercado, posicionando a la empresa como referente en respuesta a incidentes.

"El mayor beneficio que hemos obtenido es la solidez en la respuesta ante incidentes que proporciona el Threat Hunting."

Darlin Fernandes,
Diretor de Serviços na Clavis.

La inteligencia obtenida en la Deep & Dark Web también aportó acceso a fuentes exclusivas. Para Clavis, esta visibilidad profunda diferenció a Axur de competidores globales, facilitando un análisis más preciso de amenazas emergentes.

Reducción del 50% en el tiempo de respuesta ante incidentes

Con la alianza con Axur, Clavis multiplicó por cinco su capacidad de detección de información sensible filtrada, ampliando considerablemente su visibilidad ante amenazas críticas.

El tiempo de respuesta a incidentes se redujo hasta en un 50%, permitiendo acciones más rápidas y precisas. “Esta velocidad es fundamental en momentos de crisis”, destaca Darlin Fernandes, Director de Servicios.

Logramos reducir drásticamente el tiempo de respuesta ante incidentes. En casos de filtración de información, la reducción fue de al menos la mitad. La integración de las alertas de Ciberinteligencia (CTI) con nuestro SOC, a través de la plataforma Clavis, potencia significativamente el análisis y respuesta ante filtraciones de información. Esta sinergia genera información valiosa, permitiendo al equipo de seguridad tomar decisiones más informadas y proactivas frente a amenazas emergentes», añade Fernandes.

Integración completa y automatización inteligente

Axur fue integrada con facilidad al ecosistema de Clavis, permitiendo una automatización eficiente en el flujo de inteligencia de amenazas. A través de APIs y webhooks, las detecciones se incorporan directamente a su plataforma, garantizando una ingestión estructurada de datos.

“Axur se adapta perfectamente a nuestra plataforma. Todo el proceso, desde la detección hasta la comunicación y generación de tickets, se realiza de forma integrada y sin fricciones.”

Darlin Fernandes,
Director de Servicios en Clavis

Además de mejorar la seguridad, Clavis utiliza los datos proporcionados por Axur para fortalecer su oferta de servicios. El modelo de alianza MSSP, desarrollado conjuntamente, permitió que Clavis ampliara aún más su portafolio.

Los eventos patrocinados con el Fondo de Desarrollo de Marketing (MDF) de Axur también impulsan la visibilidad de marca y fortalecen la relación con prospectos y clientes.

Conozca más sobre cómo Axur ayuda a MSSPs y equipos de ciberseguridad a detectar y responder ante amenazas externas en una demostración personalizada.

Descubra cómo obtener mayor visibilidad, respuestas más ágiles e inteligencia accionable

DESCUBRA LA PLATAFORMA

Gartner Peer Insights 5/5

Conozca todas nuestras soluciones en axur.com

///AXUR