PPG protege su superficie de ataque con monitoreo continuo de amenazas externas

Sobre la empresa

PPG es una una multinacional estadounidense del sector de pinturas y recubrimientos, con una fuerte presencia en América Latina a través de la marca Comex. Con décadas de historia, la empresa opera una amplia red de tiendas físicas, plataformas digitales y concesionarios autorizados. PPG mantiene un compromiso constante con la innovación y la protección de sus marcas.

El problema

Antes de Axur, PPG necesitaba una solución capaz de controlar la exposición de datos sensibles, como repositorios de código, credenciales e nuevos dominios. Además, la empresa necesitaba una solución capaz de identificar perfiles falsos en redes sociales, diferenciar concesionarios legítimos de estafadores y monitorear el uso indebido de la marca en marketplaces y plataformas digitales.

Incluso utilizando otras herramientas de monitoreo, la cobertura era limitada y la velocidad de respuesta insuficiente frente a la escala de los riesgos que enfrentaba.

La solución

Axur proporcionó visibilidad sobre la superficie de ataque digital de PPG. La plataforma comenzó a monitorear de manera continua repositorios de código, credenciales expuestas, dominios no autorizados, perfiles en redes sociales y marketplaces.

Con la facilidad de solicitar takedowns e investigaciones directamente desde la plataforma, el equipo de seguridad de PPG ganó agilidad para responder ante incidentes críticos, desentrañar casos complejos y actuar proactivamente antes de que generaran un impacto mayor en el negocio.

Casos de uso que marcaron la diferencia

Exposición de código en GitHub

PPG descubrió que desarrolladores externos contratados para proyectos específicos habían publicado código propietario de la compañía en repositorios públicos de GitHub. Además, se identificaron desarrollos de malware y campañas de spam que utilizaban dominios de la empresa. Sin Axur, esta exposición habría permanecido invisible, poniendo en riesgo la propiedad intelectual y la seguridad operativa.

Credenciales comprometidas

El monitoreo continuo detectó credenciales robadas por infostealers que otorgaban acceso a sistemas sin autenticación multifactor. El equipo identificó dominios y portales creados por desarrolladores sin conocimiento del área de seguridad. Estas credenciales eran válidas y permitían acceso irrestricto, representando una puerta de entrada crítica para atacantes.

Uso indebido de la marca

La plataforma identificó a un individuo que publicaba fotos inapropiadas en redes sociales utilizando productos y logotipos de Comex. La capacidad de monitorear perfiles en plataformas como Facebook, Instagram y otras redes permitió al equipo identificar rápidamente al responsable, solicitar la eliminación del contenido y proteger la reputación de la marca antes de que el daño se amplificara.

Impacto en cifras

+ 1.447 takedowns solicitados en 6 meses

1.300 perfiles falsos identificados

450 casos de piratería o venta irregular detectados

Investigación de incidente con hacktivismo

Pantallas digitales instaladas en tiendas Comex, administradas por un socio externo, fueron comprometidas por hacktivistas que modificaron el contenido publicitario para mostrar mensajes relacionados con el conflicto en Gaza. PPG aprovechó las horas de investigación proporcionadas por Axur para rastrear el origen del ataque, entender el contexto completo de la amenaza y tomar medidas preventivas para mitigar riesgos y evitar recurrencias.

Exposición de datos en una POC

Durante la evaluación de una solución ofrecida por un proveedor, se usaron credenciales genéricas para realizar una prueba de concepto (POC). Tras decidir no adquirir la herramienta, el proveedor no eliminó la interfaz de prueba. Axur detectó que esta POC seguía activa con credenciales expuestas y contenía información real de PPG, incluyendo datos de un director. El incidente fue gestionado de inmediato, evitando la filtración de información corporativa sensible.

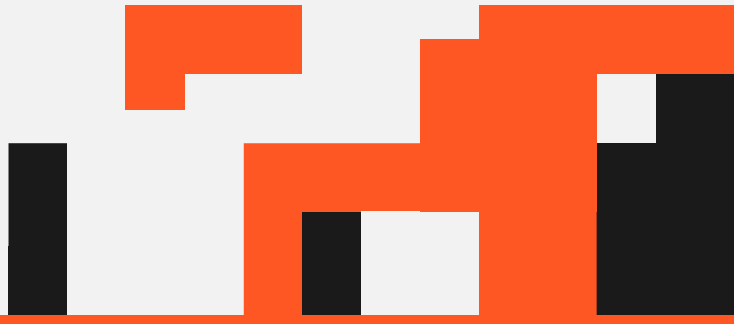
Mucho más que la cobertura tradicional

Axur se distingue por abarcar áreas que otras soluciones no alcanzan. Mientras que las herramientas tradicionales se enfocan únicamente en el monitoreo de la dark web y de dominios, la plataforma de Axur supervisa marketplaces digitales, redes sociales y repositorios de código, superficies de ataque cada vez más explotadas por los ciberdelincuentes.

La facilidad para solicitar takedowns e investigaciones directamente desde la plataforma hizo que la operación fuese mucho más ágil. En un mercado competitivo, Axur sobresale gracias a su tecnología avanzada, que ofrece cobertura amplia y automatización inteligente, acelerando la toma de decisiones y reduciendo significativamente el tiempo de exposición a riesgos.

> *"La facilidad y la rapidez son los puntos clave. Axur ve cosas que otras herramientas no ven. No existe ninguna solución en el mercado que ofrezca lo que Axur ofrece. Siempre que tenemos un problema o una duda, Axur lo resuelve todo rápidamente. Además, la relación costo-beneficio es muy competitiva."*
>
> **Ernesto Origel,**
> **IT Security at PPG**

PPG fortaleció su postura de seguridad digital con una solución que ofrece visibilidad completa, respuesta ágil y cobertura en áreas que otras herramientas suelen pasar por alto. Con Axur, la compañía protege no solo sus sistemas y datos, sino también su reputación y la confianza de millones de clientes en la marca Comex.



Protege su marca y sus operaciones frente a amenazas digitales

Conozca las soluciones de Axur y amplíe el monitoreo de su superficie de ataque externa.

AGENDE UNA DEMO

Gartner Peer Insights 4.9 ★★★★★

Conozca todas nuestras soluciones en: **axur.com**

///AXUR