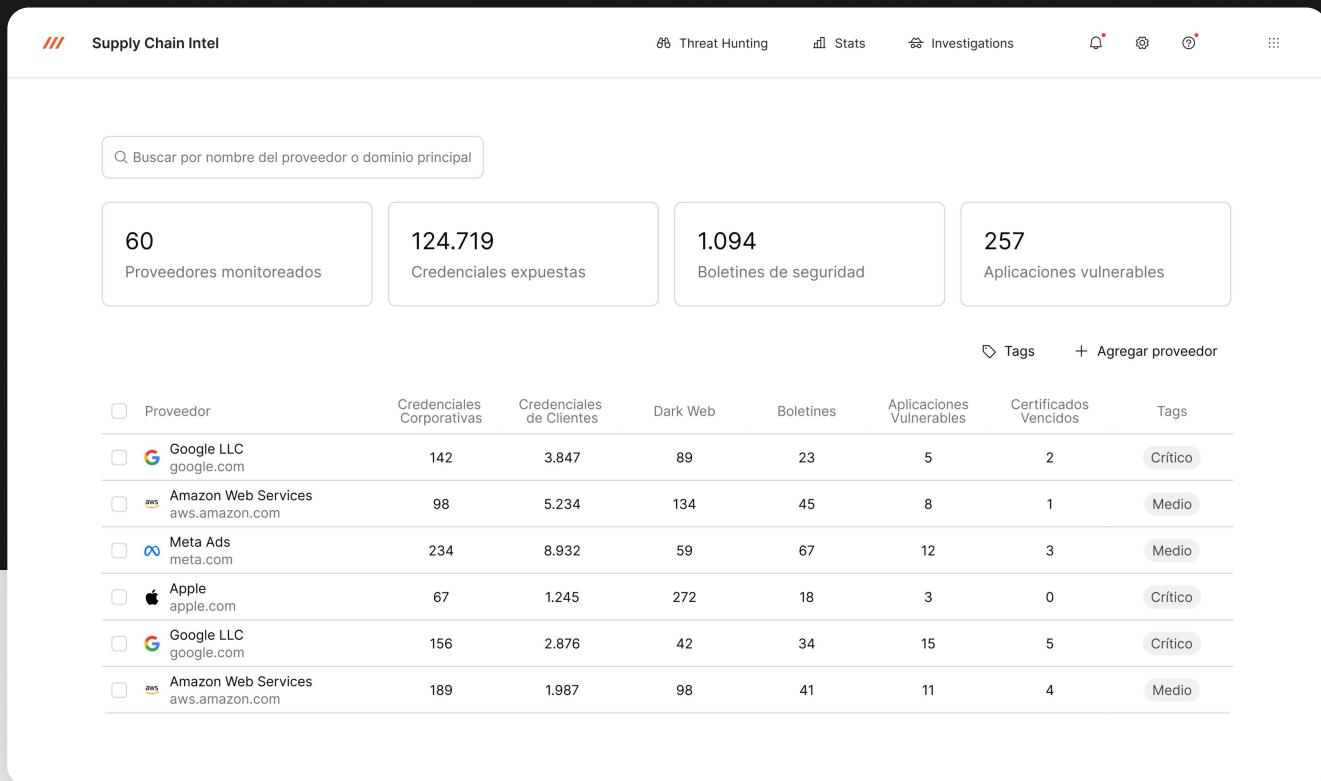


## Supply Chain Intel

Inteligencia de exposición de terceros para equipos de seguridad

# Investigue y actúe sobre la exposición en la cadena de suministro con inteligencia externa unificada y correlacionada



The screenshot shows the Supply Chain Intel dashboard interface. At the top, there's a search bar labeled "Buscar por nombre del proveedor o dominio principal". Below it are four summary boxes: "60 Proveedores monitoreados", "124.719 Credenciales expuestas", "1.094 Boletines de seguridad", and "257 Aplicaciones vulnerables". A navigation bar includes "Threat Hunting", "Stats", "Investigations", and other icons. The main content area displays a table of vendor monitoring data:

Proveedor	Credenciales Corporativas	Credenciales de Clientes	Dark Web	Boletines	Aplicaciones Vulnerables	Certificados Vencidos	Tags
Google LLC google.com	142	3.847	89	23	5	2	Criticó
Amazon Web Services aws.amazon.com	98	5.234	134	45	8	1	Medio
Meta Ads meta.com	234	8.932	59	67	12	3	Medio
Apple apple.com	67	1.245	272	18	3	0	Criticó
Google LLC google.com	156	2.876	42	34	15	5	Criticó
Amazon Web Services aws.amazon.com	189	1.987	98	41	11	4	Medio

Las cadenas de suministro modernas están altamente interconectadas. Los proveedores y socios suelen contar con acceso privilegiado a sistemas críticos, lo que los convierte en objetivos prioritarios para los atacantes. Al mismo tiempo, los equipos de seguridad enfrentan dificultades debido a la fragmentación de la inteligencia externa, distribuida en herramientas desconectadas entre sí.

Supply Chain Intel de Axur aborda este desafío al correlacionar señales externas de amenazas en una visión unificada y cualitativa de la exposición de terceros. Esto permite a los equipos de seguridad identificar amenazas reales provenientes de proveedores, comprender patrones de exposición y actuar con mayor rapidez.



Detecte amenazas antes de que escalen a incidentes



Acelere la respuesta ante incidentes relacionados con proveedores



Detección temprana de ataques de movimiento lateral

# Amenazas reales en la cadena de suministro. Diseñado para equipos de seguridad.

## Dominios Relacionados

Mapee de forma proactiva los dominios asociados a proveedores externos para descubrir activos ocultos que puedan ampliar la exposición en la cadena de suministro.

## Panorama de Amenazas de Proveedores

Realice un seguimiento continuo de inteligencia de amenazas y avisos de seguridad relacionados con proveedores externos para anticipar riesgos en la cadena de suministro.

## Credenciales Expuestas

Detecte credenciales de proveedores expuestas y verifique accesos activos o de invitados en sus sistemas de identidad y sistemas internos.

# Amplíe sus investigaciones con Threat Hunting

Profundice en la exposición de terceros con inteligencia correlacionada, investigando credenciales filtradas y otras señales de amenazas para anticipar riesgos de proveedores.

### ➡ Datos Masivos de Amenazas

Investigue utilizando más de 17 mil millones de credenciales filtradas únicas y más de 40 millones de URL escaneadas diariamente.

### ➡ Inteligencia Correlacionada

Aproveche conjuntos de datos enriquecidos para correlacionar señales y respaldar investigaciones más profundas, basadas en evidencia.

La mayoría de las herramientas de terceros se enfocan en la postura de seguridad. Nuestra inteligencia de cadena de suministro amplía esa visión al revelar exposiciones activas y amenazas emergentes, permitiendo a los equipos de seguridad actuar antes, con mayor evidencia y contexto.

## Productos & Servicios

Obtenga visibilidad sobre productos y servicios de terceros para comprender mejor cómo las amenazas externas pueden afectar su cadena de suministro.

## Superficie de Ataque Externa

Identifique activos expuestos externamente, operados por proveedores, que puedan ser aprovechados en ataques a la cadena de suministro.

## Menciones en la Dark Web

Monitoree la deep y dark web para detectar de forma temprana abusos en la cadena de suministro o filtraciones de datos vinculadas a proveedores.

### AI Query Builder

Hola, soy el AI Query Builder!  
Dime qué necesitas, y generaré consultas para ti

Generando consultas para URL y Dominios

Quiero sugerencias para la investigación...

➔ Generar

¿No sabes por dónde empezar? Pruebe uno de estos ejemplos:

Credenciales para el dominio de correo electrónico ejemplo.com en los últimos 3 meses ➔

Credenciales de usuario@ejemplo.com filtradas ➔

Credenciales filtradas donde el usuario inició sesión en example.com con una contraseña de más de 12 caracteres ➔

Credenciales con dominio de correo electrónico ejemplo.com donde la computadora fue infectada en los últimos 3 meses ➔

Manténgase un paso adelante de los riesgos de terceros con Axur.

## INICIAR CON UNA DEMOSTRACIÓN

Descubra todas nuestras soluciones en [axur.com](http://axur.com)



AXUR