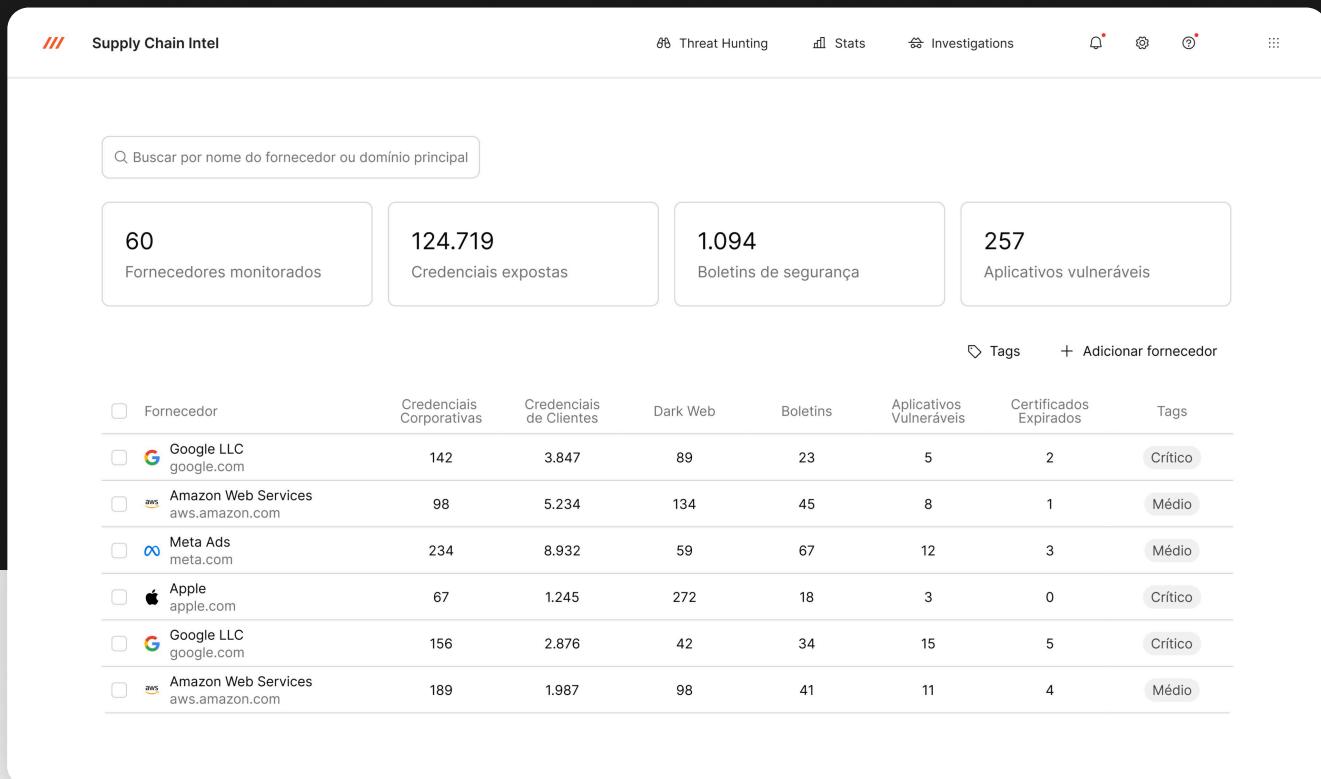


Supply Chain Intel

Inteligência supply chain para times de segurança

Investigue e responda à exposição da cadeia de suprimentos com inteligência externa unificada e correlacionada



The screenshot shows the Supply Chain Intel dashboard. At the top, there's a search bar labeled "Q. Buscar por nome do fornecedor ou domínio principal". Below it are four summary boxes: "60 Fornecedores monitorados", "124.719 Credenciais expostas", "1.094 Boletins de segurança", and "257 Aplicativos vulneráveis". A navigation bar at the top right includes "Threat Hunting", "Stats", "Investigations", and other icons. The main content area displays a table of monitored suppliers with columns for Fornecedor, Credenciais Corporativas, Credenciais de Clientes, Dark Web, Boletins, Aplicativos Vulneráveis, Certificados Expirados, and Tags. The table lists several well-known companies like Google, Amazon, and Apple.

As cadeias de suprimentos modernas são altamente interconectadas. Fornecedores e terceiros frequentemente possuem acesso privilegiado a sistemas críticos, tornando-se alvos prioritários para atacantes. Ao mesmo tempo, equipes de segurança enfrentam dificuldades com inteligência externa fragmentada, distribuída entre ferramentas desconectadas.

O Supply Chain Intel da Axur resolve essa lacuna ao correlacionar sinais externos de ameaça em uma visão unificada e qualitativa da exposição de terceiros, permitindo que times de segurança identifiquem ameaças reais de fornecedores, compreendam padrões de exposição e ajam com mais rapidez.



Detecte ameaças antes que se tornem incidentes



Acelere a resposta a incidentes relacionados a fornecedores



Identifique precocemente ataques de movimento lateral

Ameaças reais à fornecedores e terceiros. Desenvolvido para times de segurança.

Domínios relacionados

Mapeie proativamente domínios associados a fornecedores terceiros para descobrir ativos ocultos que podem ampliar a exposição da cadeia de suprimentos.

Panorama de ameaças

Acompanhe continuamente inteligência de ameaças e alertas de segurança relacionados a fornecedores para antecipar riscos na cadeia de suprimentos.

Credenciais expostas

Detecte credenciais de fornecedores expostas e verifique acessos ativos ou de convidados em seus sistemas de identidade e ambientes internos.

A maioria das soluções de supply chain foca apenas em postura. Nossa supply chain intel adiciona visibilidade sobre exposição ativa e ameaças emergentes. Esses casos de uso mostram como sinais qualitativos, em tempo real, ajudam equipes de segurança a agir mais cedo, com evidências mais claras e contexto aprofundado.

Produtos & serviços

Obtenha visibilidade sobre produtos e serviços de terceiros para entender melhor como ameaças externas podem impactar sua cadeia de suprimentos.

Superfície de ataque externa

Identifique ativos expostos externamente, operados por fornecedores, que podem ser explorados em ataques à cadeia de suprimentos.

Menções na dark web

Monitore atividades na deep e dark web relacionadas a fornecedores para identificar sinais precoces de abuso da cadeia de suprimentos ou vazamentos de dados.

Amplie investigações com Threat Hunting

Aprofunde-se na exposição de terceiros usando inteligência correlacionada. Investigue credenciais vazadas, cartões e outros sinais de ameaça para obter contexto antecipado sobre riscos relacionados a fornecedores.

→ Grande volume de dados de ameaças

Investigue com base em mais de 17 bilhões de credenciais vazadas únicas e mais de 40 milhões de URLs analisadas diariamente.

→ Inteligência correlacionada

Utilize conjuntos de dados enriquecidos para correlacionar sinais e conduzir investigações mais profundas, baseadas em evidências.

AI Query Builder

Olá, sou a AI Query Builder!
Diga o que precisa, e eu gero queries para você

Gerando consultas para

URLs & Domínios

Quero sugestões para pesquisar...

Gerar

Não sabe por onde começar? Experimente um destes exemplos:

Credenciais do domínio de e-mail example.com nos últimos 3 meses

Credenciais vazadas de user@example.com

Credenciais vazadas em que o usuário fez login em example.com com uma senha com mais de 12 caracteres

Credenciais vazadas com o domínio de e-mail example.com onde o computador foi infectado nos últimos 3 meses

Antecipe os riscos de terceiros com a Axur

SOLICITE UMA DEMONSTRAÇÃO

Descubra todas as nossas soluções em axur.com



AXUR