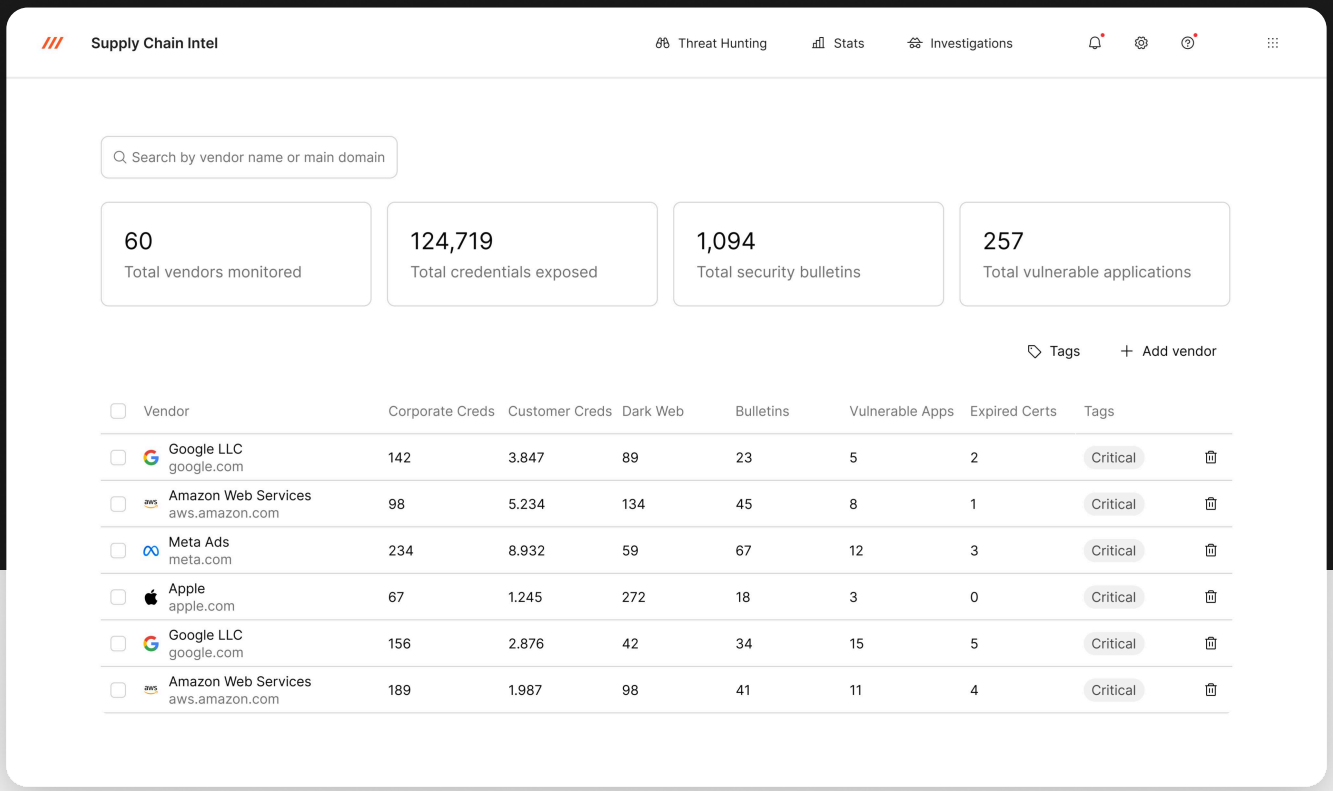
AXUR

Supply Chain Intel

Third-party exposure intelligence for security teams

Investigate and act on supply chain exposure with unified, correlated external intelligence



Modern supply chains are highly interconnected. Vendors and partners often have privileged access to critical systems, making them prime targets for attackers. At the same time, security teams struggle with fragmented external intelligence spread across disconnected tools.

Axur's Supply Chain Intel addresses this gap by correlating external threat signals into a unified, qualitative view of third-party exposure, enabling security teams to identify actual vendor threats, understand exposure patterns, and act faster.

- Detect threats before they escalate into incidents
- Accelerate response to vendor-related incidents
- Early detection of lateral movement attacks

Real supply chain threats. Built for security teams.

Most third-party tools focus on posture. Our supply chain intelligence adds visibility into active exposure and emerging threats. These use cases show how qualitative, real-time signals help security teams act earlier, with clearer evidence and deeper context.

Related Domains

Proactively map domains associated with third-party vendors to uncover hidden assets that may expand supply chain exposure.

Products & Services

Gain visibility into third-party products and services to better understand how external threats may affect your supply chain.

Vendor Threat Landscape

Continuously track threat intelligence and security advisories related to third-party vendors to anticipate supply chain threats.

External Attack Surface

Identify externally exposed assets operated by vendors that could be leveraged in supply chain attacks.

Exposed Credentials

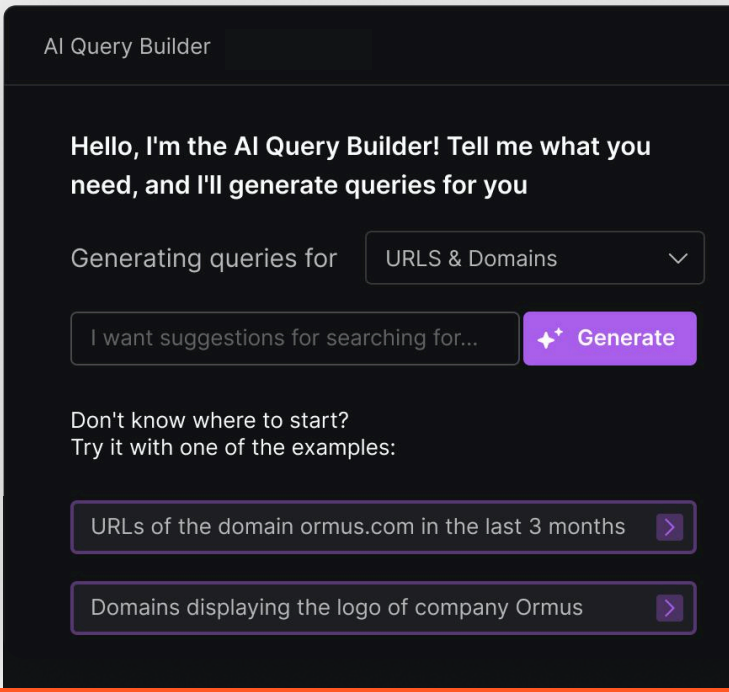
Detect exposed vendor credentials and verify active or guest access across your identity and internal systems.

Dark Web Mentions

Monitor deep and dark web activity related to vendors to identify early signals of supply chain abuse or data leaks.

Extend investigations with Threat Hunting

Go deeper into third-party exposure using correlated intelligence. Investigate leaked credentials, cards and additional threat signals to gain early context on vendor-related threats.



Massive Threat Data

Investigate using 17+ billion unique leaked credentials and more than 40 million URLs scanned daily.

Correlated Intelligence

Leverage enriched data sets to correlate signals and support deeper, evidence-based investigations.

Stay ahead of third-party risks with Axur

GET A DEMO

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Gartner Peer Insights 4.9

Discover all our solutions at **axur.com**

///AXUR