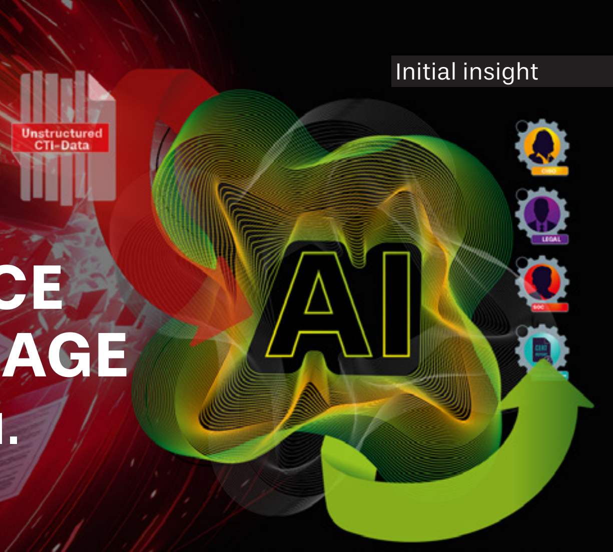
asvin

Initial insight



CYBER THREAT INTELLIGENCE THAT SPEAKS YOUR LANGUAGE

Structured. Contextual. Operational.

asvin's CTI layer transforms your unstructured threat data into structured, role-specific reports—automatically, AI-augmented, and at scale. This empowers your teams across business units with targeted insights to detect and respond to threats more effectively. Integrated within the Risk by Context™ platform, it also helps ensure compliance with UN R155, NIS2, and the Cyber Resilience Act, strengthening your overall security posture.

The Challenge

Why CTI often fails to deliver impact.

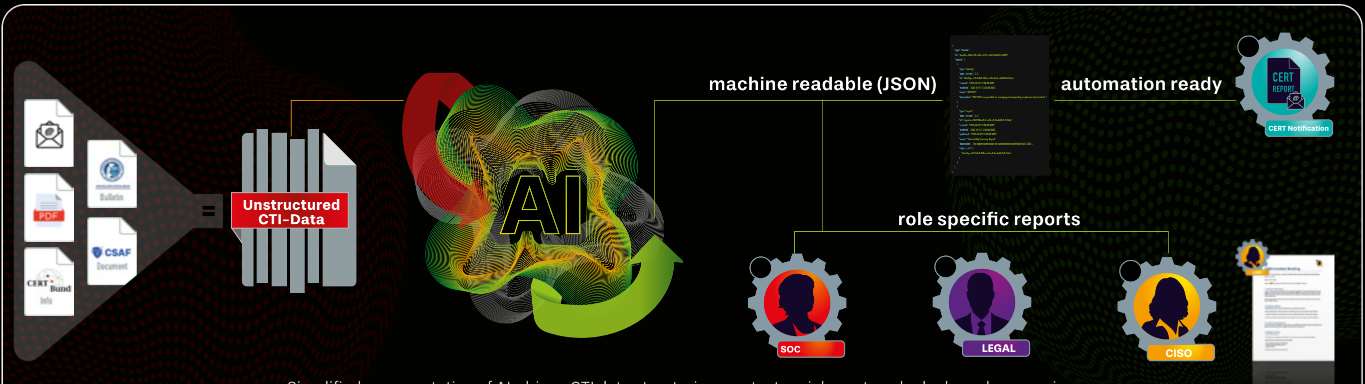
- Business units work with different technologies and have fragmented views of threats.
- Threat reports from vendors lack product-specific context and are hard to align.
- There is no consistent, organization-wide threat landscape.
- CTI is often delivered manually as a central service — time-consuming, siloed, and unscalable
- As a result, threat understanding remains isolated, and response efforts lack coordination.

The Solution

How AI-powered CTI unlocks clarity, speed, and strategic alignment.

- Establish a consistent, organization-wide threat landscape
- Bridge the gap between business units through role-specific CTI insights
- Map cyber threats directly to products, services, and technologies
- Replace manual CTI reports with scalable, AI-powered automation.

CTI redefined: From reactive reports to automated, role-specific intelligence



Simplified representation of AI-driven CTI data structuring, context enrichment, and role-based processing

By turning fragmented data into structured, actionable outputs, and by tailoring intelligence to each role, asvin shifts CTI from reactive reporting to an integrated, automated capability. The result: greater clarity, higher consistency, and full readiness — at scale.