

EXTERNAL ATTACK SURFACE MANAGEMENT

Protect assets you didn't know you had

Untracked domains, misconfigured APIs, and exposed cloud services create risk you can't fix if you don't know it exists. Styx Intelligence gives you continuous monitoring across your full external footprint.

The threat landscape

Shadow IT spins up unapproved tools under your name. Expired certificates and misconfigured DNS records sit unnoticed until they cause an outage or an email spoofing incident. It doesn't take a sophisticated attacker, just something on your perimeter nobody's watching.

The existing tools gap

Internal vulnerability scanners weren't built to discover a sprawling, changing external footprint, and most ASM tools stop at an unprioritized list. Styx builds the inventory automatically, monitors it continuously, and tells you what to fix first.

CAPABILITIES

Your full external footprint, monitored in one place



Complete asset inventory

Automatically identifies and categorizes every domain, IP, cloud app, and piece of infrastructure linked to your organization.

- Unknown and shadow assets included, in one centralized dashboard
- Inventory kept current as your footprint changes, not on the next audit cycle



Guidance & prioritized remediation

Every issue comes with a clear, actionable recommendation, prioritized by business impact rather than handed over as a raw list.

- Digital Risk Score tracks posture over time
- Scoring based on exposure, misconfigurations, and IP reputation



Misconfiguration & vulnerability detection

Spots open ports, expired certificates, weak HTTP headers, and TLS/SSL issues across your perimeter.

- DNS and email-record errors that can lead to spoofing
- Alerts on exposed systems tied to known CVEs



Shadow IT detection

Discovers unapproved websites, tools, and cloud apps using your brand name without your knowledge.

- Unsanctioned assets flagged so you can shut them down
- Stops shadow IT before it exposes data or confuses customers

01

Stop learning the hard way

An outage or spoofing incident shouldn't be how your team learns an asset existed.

02

Know what to fix first

Every finding comes with a remediation recommendation, so your team closes gaps instead of triaging.

03

Track posture over time

The Digital Risk Score gives one number to show whether your external exposure is improving.

CONNECTED IN STYX INTELLIGENCE

Iris AI Assistant · New

Ask plain-language questions about your assets, findings, and external exposure.

Threat Intelligence

See which newly published CVEs and active threats touch the assets in your inventory.

Risk Scorecard

Score your external risk posture, track progress over time, and show leadership measurable improvement.

Attack Surface Management

Digital Risk Score **730**

ATTACK SURFACE FINDINGS — ACROSS YOUR EXTERNAL FOOTPRINT

ASM Findings Across all assets

11,882

Vulnerabilities CVE-linked exposures

6,390

Website Header Issues Weak or missing headers

808

TLS/SSL Certificate Issues Expired or invalid

248

MONITORED ASSETS — DOMAINS, DNS, HOSTS, AND INFRASTRUCTURE

Active Domains Owned and discovered

13

Hosts (Sub-Domain) Including shadow assets

508

DNS Health Issues Spoofing-enabling records

59

Potentially Insecure Ports Exposed services

72

Illustrative sample data

Less risk, less manual work.

Styx keeps your external inventory current and ranked by what actually matters, so your team fixes exposure instead of assembling spreadsheets.

Talk to Us

styxintel.com