

THREAT INTELLIGENCE

Know what's coming before it hits

Malware campaigns, targeted attacks, and cybercriminal chatter move fast. Styx Intelligence tracks them as they happen and maps them to your own digital footprint, so your team gets actionable context instead of a generic feed.

The threat landscape

Criminal forums discuss targets before they're breached, vulnerabilities are exploited before patch cycles catch up, and leaked credentials circulate long before anyone knows. The intelligence exists, but it's scattered across sources most teams can't watch.

The existing tools gap

Scanners flag what's technically exploitable but not what attackers are targeting now, and most intel tools never connect back to your assets, vendors, or exposure. Styx ties threat intelligence directly to your digital footprint.

CAPABILITIES

Intelligence tied to your footprint, not generic feeds



Real-time cyber threat monitoring

Visibility into malware campaigns, targeted attacks, and cybercriminal tactics as they emerge.

- Alerts arrive with actionable context, so threats are neutralized before they escalate
- Insight into global incidents, threat actor trends, and TTPs



Vulnerability identification & prioritization

Tracks new CVEs across your brand assets, vendor systems, and exposed infrastructure.

- Prioritized by exploitability, business impact, and threat actor chatter
- Remediation focused on what actually puts your brand at risk



Data breach detection & analysis

Monitors for leaked credentials, stolen customer records, and internal business files traded on dark web marketplaces.

- Full visibility into breach sources, timelines, and data types involved
- Searchable index of breach records for fast investigation



Indicators of compromise detection

Identifies malicious IPs, domains, file hashes, and URLs tied to phishing, malware, or command-and-control infrastructure.

- Detection rules update continuously from threat intel feeds
- Analyst insight layered on top of automated detection

01

Respond before threats escalate

Context arrives with every alert, so your team acts on threats instead of researching whether they matter.

02

Prioritize by actual risk, not just severity

Vulnerabilities ranked by exploitability and threat actor activity, so effort goes where it counts.

03

Brief leadership with real intelligence

Global incidents, actor trends, and TTPs give security teams the context to strengthen reporting.

CONNECTED IN STYX INTELLIGENCE

Iris AI Assistant · New

Ask plain-language questions about threats, CVEs, and actor activity affecting your organization.

Attack Surface Management

Map the internet-facing assets that threat intelligence is matched against.

Third-Party Vendor Risk

See how emerging threats and vulnerabilities touch the vendors connected to your business.

Less risk, less manual work.

Styx turns scattered intelligence into context your team can act on, mapped to the assets, vendors, and exposure that are actually yours.

Talk to Us

styxintel.com

