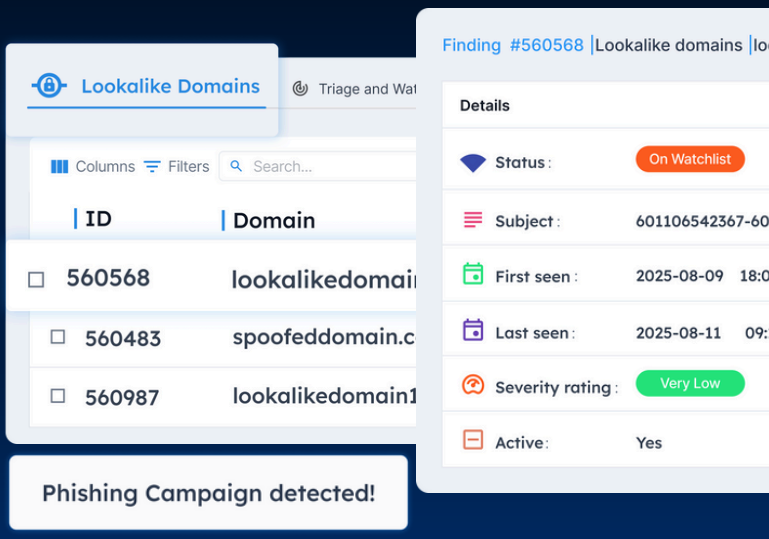
STYX INTELLIGENCE

DIGITAL RISK PROTECTION FOR FINTECH

Detect, monitor, and take down phishing domains, account scams, and data leaks targeting the Fintech Sector. Protect trust, meet compliance, and keep your customers and leaders safe.



Fintech companies are built for speed, access, and scale, but that also makes them high-value targets. From fake apps to spoofed payment pages, impersonation attacks now move faster than compliance teams can react.

What Makes Fintech The Perfect Target?

Holding sensitive financial data

Fintech holds what attackers want, including card data, logins, payment flows, and personal details. That makes your users, apps, and APIs a direct target for phishing, scams, and leaks.

Compliance rules are strict in Fintech

You must meet GDPR, CCPA, PCI DSS, and AML/KYC, and a single phishing incident or vendor leak can trigger audits and fines.

Trust and compliance go hand in hand

People choose fintech for speed and convenience, but they stay because they trust the brand. One impersonation scam or fake support account can break that trust overnight.

Fintech Unique Digital Threats

- Data Breaches & Information Exposure
- Account Takeover & Identity Theft
- Executive & Brand Impersonation
- Phishing & Domain Abuse
- Third-Party & Supply Chain Risks

STYX
INTELLIGENCE

How Styx Supports Fintech Companies

1. Brand protection built for Fintech

- Monitor and shut down lookalike domains, spoofed login pages, and phishing sites targeting your organizations and customers.
- Monitor and act on unauthorized use of your name, logo, UI, or copy across websites, marketplaces, and app stores.
- Find and take down rogue mobile apps and clones that harvest credentials for future financial scams.

2. Executive Protection & VIP Monitoring

- Monitor founders and executives across social, news, forums, and the dark web for impersonation, doxing, and payment fraud.
- Detect exposed credentials, emails, addresses, ID numbers, financial information, and leaked personal data that could lead to financial fraud or harm.
- Detect harassment, explicit threats, and location leaks tied to leaders, and alert physical security with preserved evidence.

3. Social Media & News Monitoring

- Identify and take down impersonation scams, phishing campaigns, and brand abuse on social media and news platforms.
- Track real-time conversation on outages, fees, features, and incidents across social, forums, and news, and route alerts to fraud, support, and comms.
- Detect and shut down scam promos, investment schemes, and account takeovers, with evidence capture and in-platform takedowns.

4. Data Leakage & Dark Web Monitoring

- Monitor surface, deep, and dark web for leaked credentials, API keys, card data, and cloud misconfigurations tied to your brand.
- Track mentions of your company, app names, BINs, and user lists in breach dumps, Telegram channels, and marketplaces to see what's being traded.
- Detect leaked proprietary code and confidential financial business files before they're used to map your systems and fuel future fraud.

5. Threat Intelligence for Fintech

- Global, data-driven view of ransomware and breach activity, enabling Fintech organizations to assess regional risks, track threat trends, and strengthen defenses based on real-world intelligence.
- Curate real-time and historical cybersecurity news to spotlight active threats, track past incidents, and reveal evolving trends that guide timely and informed security decisions.
- Gain insights into conversations on underground forums and dark web markets to identify emerging threats, attacker tactics, and potential data exposure risks.

6. Third-Party Risk Management

- Assess the digital risk of payment processors, banking partners, and KYC/AML providers with a live risk scorecard and automated questionnaires.
- Rank vendors by exposure and business criticality in a clear matrix so your team knows where to act first.
- Get alerts when a partner leaks data, is named in a breach, or appears on the dark web, with details on what was exposed.

Business Benefits for Fintech Companies

Trust and Customer Retention

Protect your reputation and give customers confidence that their data, money, and personal accounts are safe.

Regulatory Compliance

Support compliance with data, fraud, and third-party regulations with clear evidence and faster response.

Operational Efficiency

Reduce time spent chasing threats by managing everything in one place with shared tools and workflows.

Revenue Protection

Prevent scams, impersonation, and fraud that can lead to lost transactions, chargebacks, churn, and direct revenue loss.

Cost Reduction

Avoid the legal, reputational, and support costs that come from delayed detection or slow response.

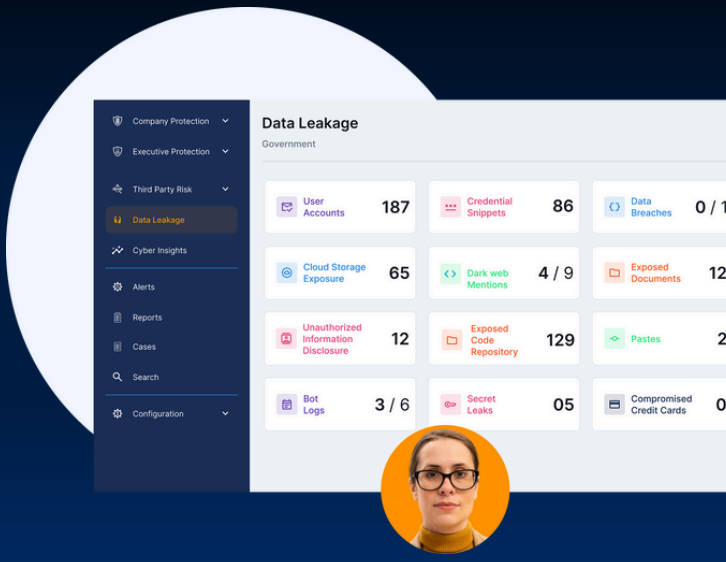
Risk Visibility

Get a full view of digital threats across your brand, vendors, and platforms, so you can take action before they spread.

STYX INTELLIGENCE

PROTECT PUBLIC TRUST ONLINE

Detect, monitor, and take down digital threats that target public institutions and political leaders. Protect trust, reduce risk, and keep services running.



Public institutions face constant online threats that move fast and confuse residents. Impersonations, leaks, and false narratives erode trust, disrupt services, and put leaders and citizens at risk.

Critical Threats for Municipalities and Political Leaders

Lookalike Domains and Phishing Websites

Scammers use these to steal logins, reroute payments, and install malware via emails and ads that copy your name and visuals.

Ransomware and Hacktivist Campaigns

Groups hit municipalities, encrypt systems, and leak samples to force payment, causing outages, recovery work, and extra costs.

Threats and Harassment (Doxing)

Exposed logins and files on paste sites, repos and forums enable account abuse, phishing, extortion, and identity fraud fast.

Impersonation Attacks

Fake leader or department profiles post false updates, solicit money, push phishing links, and hijack threads, damaging public trust.

Disinformation Campaigns

False claims about services, budgets, or elections spread via posts and group chats, driving confusion, press heat, and delays.

Sensitive Data Exposure

Exposed logins and files on paste sites, repos and forums enable account abuse, phishing, extortion, and identity fraud fast.

Third-Party Exposure

Breaches or mistakes at vendors with access pull in your domains, data, and leader IDs, creating entry points, and spillover.

Account Takeover

Hijacked websites, email, or official handles post fake notices or redirect traffic, eroding trust and blocking public updates.

STYX
INTELLIGENCE

The Solution: StyxView

1. External Attack Surface Management

- Map and monitor internet-facing assets across departments, utilities, transit, libraries, and remote sites.
- Manage risks tied to legacy systems, forgotten subdomains, and cloud misconfigurations.
- Detect exposed assets across departments, city halls, libraries, and remote offices, reducing entry points for attackers.

2. Brand and Social Media Monitoring

- Monitor leaders' and municipalities' accounts across major platforms, domains, and apps.
- Detect and take down lookalike domains, phishing websites, and social media impersonations.
- Track the spread of fake news and disinformation that targets elections, government initiatives, or individual leaders.
- See sentiment shifts and coordination patterns, then trigger response workflows.

3. Leaders Safety and Reputation Management

- Monitor threats associated with named leaders and their families, as well as close staff.
- Detect dox posts, targeted abuse, and smear sites, with severity scoring.
- Provide evidence packs, preservation, and escalation guidance for legal and security.

4. Data Leakage and Dark Web Monitoring

- Monitor leader and city credentials, documents, and records across the surface, deep, and dark web.
- Identify leaked records like tax data, voter rolls, or public safety information
- Get alerts when political leaders are involved in data breaches, with full visibility into what was exposed.

5. Cyber Threat Visibility For Municipalities and Political Leaders

- Follow ransomware and hacktivist groups that target public sector orgs.
- Monitor forums for chatter on planned attacks, leaks, or exploits relevant to your tech stack.
- Get incident briefs with who is affected, what leaked, and immediate actions.

6. Third-Party Risk Monitoring

- Map your key vendors, cloud services, and comms partners.
- See breach history, live exposure signals, and impersonation events tied to suppliers.
- Get alerts for third-party leaks that touch your brand, domains, or leader identities.

7. Takedown Services

- Phishing and lookalike domain takedown.
- Fake social account and page removal.
- Data leakage removal (docs, repos, paste sites).
- Rogue mobile app and scam ad removal.
- Evidence of action with links, timestamps, and provider responses.

STYX INTELLIGENCE

AN AI-POWERED, UNIFIED PLATFORM TO PROTECT YOUR BRAND FROM CYBER THREATS

What Problem We solve

The modern attack surface extends far beyond infrastructure. Domains, apps, employee profiles, executive impersonations, and misinformation all shape how an organization is seen and targeted. These external assets are difficult to control, yet critical to monitor and secure.

Today's businesses need visibility into what's happening beyond their perimeter, not just to detect problems, but to act early and protect what matters most: their brand, reputation, and customer trust.

What We Do

Styx is an AI-powered, unified Platform built to help companies monitor, detect, and act on external threats across domains, social media, executive presence, third parties, and even activity on the dark web.

We bring everything together into one clear system of record, showing you what's happening, what to prioritize, and how to respond. From early detection to integrated takedowns, Styx provides your team with visibility and control where it matters most.

Why Styx

Executives and security leaders aren't looking for more alerts; they need visibility, clarity, and control. Styx helps organizations:

- **Protect brand reputation and customer trust by preventing risks before they escalate and affect your business.**
- **Reduce financial and operational impact tied to fraud, impersonation, and data loss.**
- **Consolidate tools and cut cost by managing everything from one platform.**
- **Enable collaboration across security, marketing, legal, and comms teams.**
- **Focus on what matters most with a digital risk score aligned to business impact and goals.**
- **Streamline reporting for leadership, compliance, and audit requirements.**

STYX
INTELLIGENCE

How We Do It

1 Identify

Identify domains, infrastructure, social handles, cloud assets, vendors, and other public-facing components tied to your brand.

2 Analyze

Analyze your digital surface to uncover gaps, misconfigurations, impersonations, and exposures, before they become problems.

3 Monitor

Get always-on visibility across social media, news, forums, marketplaces, open, deep and dark web and vendor ecosystems.

4 Prioritize

Quantify and prioritize external threats with a dynamic risk score, helping you focus on the most critical remediations.

5 Remediate

Submit and track takedown requests from within the platform for malicious domains, fake profiles, job scams, and leaked data.

6 Report

Generate role-based reports and insights to help both technical and non-technical teams understand, communicate, and act.

Styx Intelligence — All Solutions

Brand Protection

- Detect and shut down lookalike domains, fake websites, rogue apps, and logo misuse.
- Monitor brand abuse across marketplaces, job ads, forums, and web mentions.
- Instantly identify fake profiles impersonating your brand, and stop scams before they spread.

External Attack Surface Management

- Map all internet-facing assets that represent your brand, including unknown or forgotten ones.
- Identify misconfigurations, Internet-facing shadow IT, and exposed systems.
- Prioritize remediation efforts based on actual business risk.

Executive Protection

- Detect fake profiles impersonating executives across social media, email, and messaging apps.
- Monitor leaked data, doxxing attempts, and chatter across surface, deep, and dark web.
- Track sentiment shifts and public exposure across news and social platforms.

Social Media & News Monitoring

- Identify fake accounts, scam promotions, and misleading content.
- Monitor mentions and brand sentiment across social media, news, and forums.
- Catch early signs of compliance risks, misinformation, or off-brand content, before they go viral.

STYX
INTELLIGENCE

Data Leak & Dark Web Monitoring

- Find exposed credentials, sensitive documents, or insider data on breach forums.
- Detect early signs of fraud, identity theft, or impersonation campaigns.
- Protect confidential information and sensitive data before it's exploited.

Takedown & Remediation

- Take down phishing domains, fake social accounts, fake job ads, rogue apps, and more.
- Submit takedown requests with one click for job scams, impersonations, and data leaks.
- Track takedown status and resolution, all in one place.

Third-Party Risk Monitoring

- Assess vendor cyber and brand posture and generate dynamic digital risk scores.
- Monitor third-party breaches, sentiment shifts, and brand mentions, even on the dark web.
- Distribute and manage security questionnaires and assessments to evaluate your vendors.

Threat Intelligence

- Stay ahead of emerging threats, malware, and adversary behavior.
- Detect indicators of compromise (IOCs) and improve internal defenses.
- Enrich investigations with real-world context from the external threat landscape.

Digital Risk Score

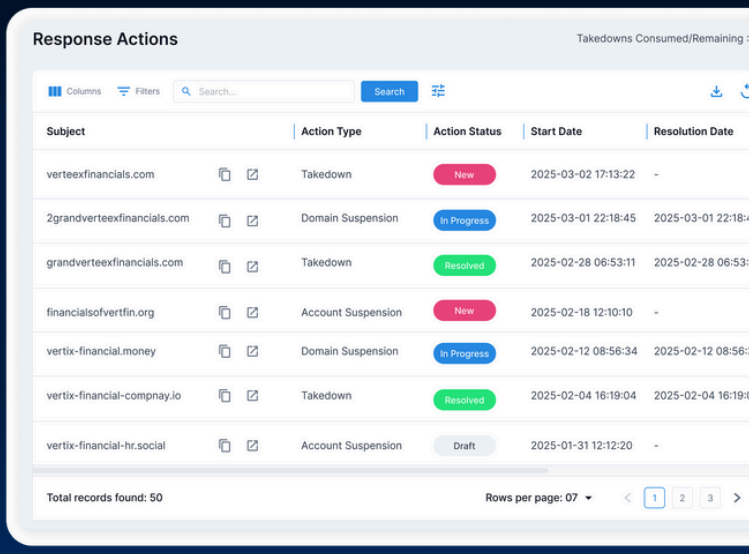
- Real-time, dynamic scoring based on live external signals across surface, deep, and dark web.
- Actionable and in your control. Review findings, mark resolved/false positive, submit takedowns, and see the score update instantly.
- Business-first prioritization & reporting. Rank by impact, map risks from your domains to vendors, and show progress with clear dashboards.

Brand impersonation, phishing scams, and data leaks can break trust in an instant. With Styx, you can detect and take down brand threats before they damage your reputation, mislead customers, or put executives at risk. Request a Demo at styxintel.com

STYX INTELLIGENCE

TAKEDOWN SERVICES
STYX INTELLIGENCE

Lookalike websites, impersonation scams, and fraudulent ads erode trust, harm reputation, and deceive customers.



Start takedowns in a few clicks, track status in one dashboard, and get proof when it's gone. Protect your brand, people, and customers from phishing and fraud.

Takedown Services Solution

Phishing Website and Domain Takedown

Scan the surface, deep, and dark web for phishing sites and lookalike domains. Get real-time alerts and shut down malicious domains to protect your brand, employees, and customers.

Social Media Impersonation Takedown

Monitor Social Media Platforms for fake accounts posing as your brand or executives. Receive real-time alerts and remove fraudulent profiles used for scams, phishing, or misinformation.

Rogue Mobile App Takedown

Identify unauthorized apps impersonating your brand across official stores and third-party sites. Shut down apps that spread malware, steal data, or mislead users to protect your brand.

Evil Twin Website Takedown

Detect websites that copy your legitimate site to mislead visitors or capture sensitive information. Shut these sites down quickly to stop impersonation and reduce risk to customers and reputation.

Fake Job Ad Takedown

Find fraudulent job postings that misuse your company name to trick applicants and collect data. Take them down to protect job seekers and prevent misuse of your brand's reputation.

Data Leakage Takedown

Detect exposed internal data across document sharing websites and the surface web. Take down leaked content quickly to prevent misuse, support compliance requirements, and reduce risk.

STYX
INTELLIGENCE

Process Advanced Takedown Requests for High-Priority Threats

Engage platforms, registrars, and legal channels, when needed, to resolve high-priority threats as quickly as possible.

The Takedown Process

1. Investigation

Evaluate the malicious activity, scope of impact (e.g., phishing, malware), and whether it violates laws, brand policies, or terms of service.

2. Takedown Request

Submit requests to domain registrars or hosting providers with evidence of malicious activity, including intellectual property violations.

3. Engagement with Authorities

If necessary, escalate unresolved cases to organizations like ICANN or local authorities.

4. Monitoring and Enforcement

Post-takedown, ensure continued compliance by monitoring domain activity for recurring threats.

When to Pursue a Takedown

Clear Malicious Intent

Evidence shows the domain is used for phishing, malware, or other harmful activities.

Brand Infringement

The domain risks reputational damage or customer confusion due to trademark infringement.

Violation of Terms

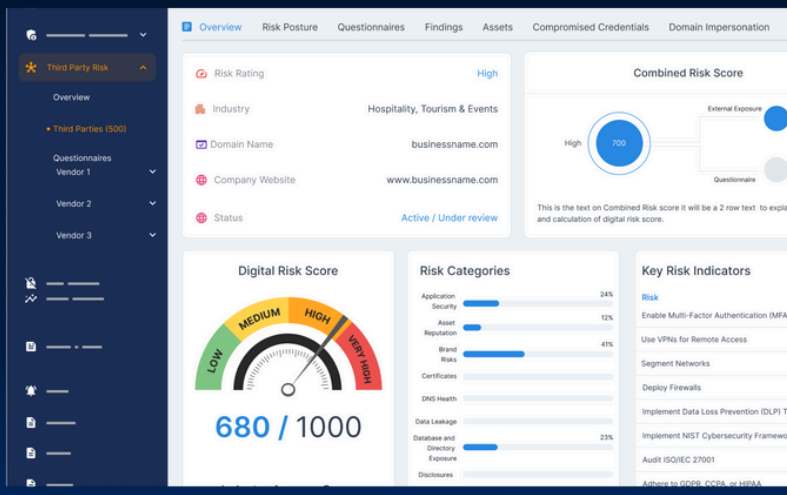
The domain breaches the registrar's or hosting provider's terms of service.

With Styx, you can confidently protect your organization, employees, and customers from the growing threats of digital impersonation and fraud. Request a Demo at styxintel.com

STYX
INTELLIGENCE

THREAT HUNTING WITH STYX INTELLIGENCE

See your company through the attacker's eyes, and stop them before they strike.



In today's threat landscape, your attack surface doesn't stop at your firewall. From exposed cloud assets to leaked employee credentials on the dark web, and from brand abuse to active adversary campaigns, every gap is an opportunity for exploitation.

The Styx solution centralizes, normalizes, and enriches threat data from internal, external, and dark sources — giving security teams the ability to search any company, at speed, for digital exposure and adversary activity.

We combine **Attack Surface Management (ASM), Dark Web Intelligence, Brand Monitoring, Threat Actor TTP/IOC Correlation**, and A**I-powered investigation tools** into a single platform.

Key Benefits

1. Smarter Threat Detection

- NLP-driven entity recognition automatically identifies and links company names, brands, and key personnel across millions of unstructured data points.
- Image recognition flags fraudulent logo usage or phishing site visuals — even if attackers alter them.
- Automated TTP classification aligns new activity with MITRE ATT&CK techniques without manual tagging.

2. Faster Investigation Workflows

- Semantic search, powered by vector embeddings, enables analysts to ask natural language questions, such as: *"Show me all companies with critical unpatched vulnerabilities with active exploits in the last 90 days."*
- AI surfaces the most relevant matches, not just keyword hits.
- Pivot recommendations suggest the next logical steps in an investigation based on past analyst actions and historical patterns.

3. Predictive Intelligence

- AI models forecast which vulnerabilities or exposed assets are most likely to be exploited based on attacker trends.
- Risk scoring dynamically adjusts based on new intelligence feeds, dark web chatter, and global attack patterns.

4. Automation with Guardrails

- AI handles repetitive tasks (such as log parsing, IOC enrichment, and report drafting) so that analysts can focus on critical decisions.
- Retrieval-Augmented Generation (RAG) ensures that AI answers are grounded in verified data from the Data Lake.

Strategic Outcomes

Proactive Defense
Spot emerging threats before they hit production systems.

Speed to Action
Move from detection to decision in minutes, not days.

Consistent Accuracy
AI-powered analysis with human oversight reduces false positives.

Cross-Team Enablement
Security, marketing, legal, and compliance teams use the same validated intelligence.

Scalable Insights
Handle hundreds of targets or entire sectors with the same resources.

Core Capabilities

Attack Surface Mapping (ASM)

- Aggregate domains, subdomains, IP ranges, services, and ports from internal scans and third-party feeds.
- Normalize and de-duplicate asset records for a clean view.
- Instant exposure profiles with severity-based risk rankings.
- Styx Risk Scoring (DRS) provides comparison across clients and industries.

Dark Web Exposure

- Continuous ingestion from dark web forums, marketplaces, leak sites, and breach dumps.
- NLP & entity recognition to identify company names, credentials, and PII.
- Pivot analysis to connect leaked data to infrastructure and prior incidents.

STYX
INTELLIGENCE

Brand Intelligence

- Monitor for logo misuse, phishing pages, fraudulent campaigns, and typo squatting.
- Automated alerts for security, marketing, and legal teams.
- Trend dashboards for brand-related threats.

Threat Actor TTP & IOC Intelligence

- Map attacker tactics, techniques, and procedures (TTPs) to MITRE ATT&CK.
- Track malicious domains, hashes, IPs, and C2 infrastructure.
- Link IOCs to known threat groups and build campaign timelines.

Real-World Threat Hunt Example

Scenario

A Styx client in the financial sector experienced a spike in phishing attempts.

How Styx Data Lake Caught It:

- **Attack Surface Mapping:** Detected an exposed dev server running outdated software.
- **Dark Web Exposure:** Flagged stolen employee credentials on a closed Telegram group.
- **TTP/IOC Correlation:** Linked malicious IPs to a known ransomware group.
- **AI-Enhanced Pivoting:** Suggested further checks for brand misuse, uncovering phishing sites using the company's logo.

Outcome

- **Server isolated in 2 hours.**
- **Phishing campaign was disrupted before reaching customers.**
- **Credentials reset.**

Results: Incident contained without financial or reputational damage.

Key Differentiators

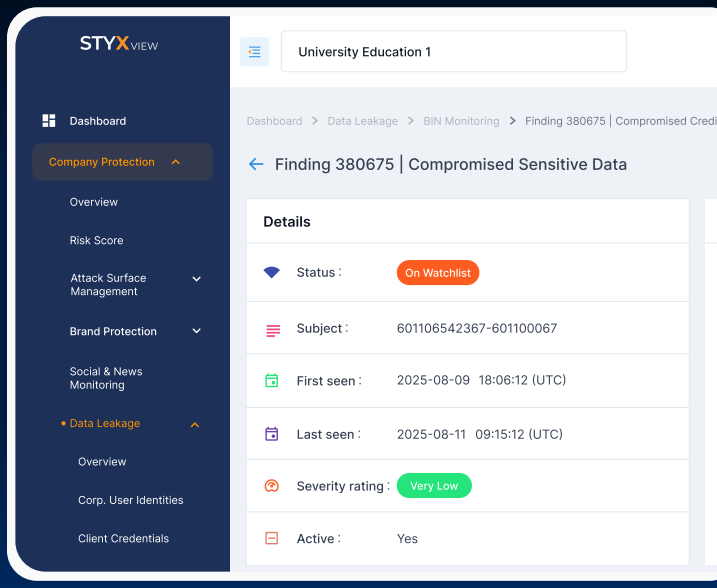
1. **AI + Human Synergy:** Automation where possible, analyst judgment where critical.
2. **Speed:** Sub-second search across massive datasets.
3. **Contextual Intelligence:** AI surfaces related to IOCs, campaigns, and TTPs automatically.
4. **Predictive Defense:** Risk forecasting to anticipate the next move.

Every second counts — intelligence at the speed of the threat, enhanced by AI.
Request a Demo at styxintel.com

STYX INTELLIGENCE

SAFEGUARDING STUDENTS, RESEARCH, AND REPUTATION

Detect, monitor, and take down digital threats that target universities, students, and leaders.
Protect trust, reduce risk, and keep systems running.



Universities Today Face a Perfect Storm of Digital Threats

Expansive IT Footprint

Large campuses often have 100's of domains, legacy systems, and cloud services, many unmanaged or outdated. Each is a potential entry point for attackers.

Leaders & Researches Harassment

Presidents, deans, and top researchers often face harassment, impersonation, or targeted fraud campaigns.

Brand Impersonations

Universities are seen as trusted institutions by students, parents, and alumni, making them prime targets for phishing scams, job fraud, and fake scholarship offers.

Sensitive Data & Research

Universities hold valuable intellectual property, medical records, financial aid data, and personal information of tens of thousands of students and staff.

Third-Party Exposure

Vendor breaches or cloud mistakes expose your domains, sensitive data, and leader profiles, creating new entry points and spillover risk.

Traditional firewalls and endpoint security protect internal networks. But most university threats originate outside the firewall, on the open web, social media, or the dark web.

STYX
INTELLIGENCE

How STYX Protects Universities

1. External Attack Surface Management (EASM)

- Map and monitor internet-facing assets across departments and university locations.
- Manage risks tied to legacy systems, forgotten subdomains, and cloud misconfigurations.
- Detect and mitigate exposed assets, reducing entry points for attackers.

2. Brand and Social Media Monitoring

- Detect and take down lookalike domains, phishing websites, job scams, and brand impersonations.
- Monitor universities' and leaders' accounts across major social platforms and news outlets.
- Track the spread of fake news and disinformation that targets universities or individual leaders.
- See sentiment shifts and coordination patterns, then trigger response workflows.

3. Executive Impersonations

- Monitor threats associated with leaders, as well as close university staff.
- Detect dox posts, targeted abuse, and executive impersonations, with severity scoring.
- Provide evidence packs, preservation, and escalation guidance for legal and security.

4. Data Leakage and Dark Web Monitoring

- Continuously monitor hacker forums, marketplaces, and paste sites for leaked credentials, student data, or research IP.
- Get alerts when university leaders are involved in data breaches, with full visibility into what was exposed.

5. Cyber Threat Visibility For Universities

- Follow ransomware and hacktivist groups that target universities.
- Monitor forums for chatter on planned attacks, leaks, or exploits relevant to your tech stack.
- Get incident briefs with who is affected, what leaked, and immediate actions.

6. Third-Party Risk Monitoring

- Map your key vendors, cloud services, and comms partners.
- See breach history, live exposure signals, and impersonation events tied to suppliers.
- Get alerts for third-party leaks that touch your university’s brand, domains, or leader identities.

7. Takedown Services

- Phishing and lookalike domain takedown.
- Identify and take down fake job ads using your university’s name to scam applicants.
- Shut down social media accounts and pages impersonating universities.
- Mitigate executive impersonations.
- Evidence of action with links, timestamps, and provider responses.

STYX
INTELLIGENCE

Benefits For Universities

- Protect Students & Families from scams and fraud.
- Safeguard Research & IP from cybercriminals and nation-state actors.
- Preserve Brand Trust across admissions, athletics, and alumni relations.
- Enhance Campus Safety by detecting threats in real time.
- Meet Compliance Obligations
- Strengthen Resilience against ransomware, phishing, and misinformation.

Why Styx Intelligence

Unified Platform

Combines attack surface management, brand monitoring, executive protection, social/news intelligence, and dark web monitoring in one pane of glass.

Customization & Fine Tuning

Styx Intelligence's detection algorithms can be tailored to specific industries, ensuring maximum relevance and accuracy.

AI-Driven Insights

Styx's machine learning models correlate threats across multiple channels and prioritize them with a Digital Risk Score (DRS).

Rapid Takedowns

Built-in workflows remove phishing domains, fake accounts, and rogue content quickly, cutting response from days to minutes.

Cross-Functional Value

Supports cybersecurity teams, campus police, and communications/PR simultaneously.

Resource Multiplier

Acts like an extra 24/7 team member, crucial for universities with lean IT and security staff.