Silobreaker Cyber Threat Intelligence

See your threat landscape in context. Detect, analyse and prioritise cyber threats and vulnerabilities at unparalleled speed with a more streamlined intelligence process.

Stop cyber threats faster and with confidence

Silobreaker streamlines the intelligence process, enabling organisations to stop threats faster with actionable cyber threat intelligence in hours or even minutes. Silobreaker collects and connects more cyber intelligence data, accelerates analysis, and brings collaboration and dissemination together in a single workflow to save time, increase ROI and provide greater confidence to mitigate risks.

Deliver stronger intelligence from the full data set

Starting with identifying effective priority intelligence requirements (PIRs), Silobreaker works with you to establish and optimise your PIRs before fully automating data collection to increase team efficiency.

Based on PIRs, Silobreaker's Intelligence Hub automatically selects, collects and aggregates the most comprehensive range of cyber threat intelligence data. This includes millions of open source, deep and dark web and finished intelligence sources, alongside internal watchlists of company executives, credentials, suppliers, hardware and software - so you can detect the cyber threats and vulnerabilities that matter most.

Reveal who might attack you and how

The Silobreaker Relevance Engine generates cyber threat intelligence that is 100% relevant to your organisation. Using AI to provide multi-lingual entity detection and aliasing across structured and unstructured data while tuning out false positives. Mapping relationships between adversaries, your technology, organisation and industry in milliseconds. Surfacing actionable intelligence based on the visibility of threat actor TTPs, chatter on deep and dark websites, social media posts, malware, vulnerabilities, Indicators of Compromise (IoCs), code repositories, paste sites and more.

Save time with one connected intelligence workflow

The Silobreaker Workspace connects everything, providing a centralised view to monitor, analyse, collaborate and push your intelligence to stakeholders faster and straight from the platform.

Scale your capacity instantly, with a library of cyber threat intelligence dashboards and watchlists that can be customised by Silobreaker or your own teams to fast track the monitoring of ransomware, CVEs, threat actors, phishing and more. Silobreaker provides consistent visualisations, heat rankings, time series, and relationship maps - making intelligence output easy to understand for any audience. Findings can then be emailed with a few clicks, either as reports or scheduled alerts, preserving sources for later reference.

CREATE A NEW REALITY

- Optimise PIRs with best-practice cybersecurity dashboards and watchlists, tracking ransomware, CVEs, threat actors, phishing and more
- Increase efficiency with automated data collection, aggregation and processing from millions of sources
- Reveal connections between threat actors and TTPs targeting your organisation, industry or technology
- Push actionable intelligence reports and schedule alerts straight from the platform
- Preserve findings to back-up or re-evaluate incident response at any time
- Integrate with CTI and SIEM tools to operationalise threat intelligence across teams and systems

Connect intelligence subscriptions

Increase efficiency and reduce multiple vendor consoles with a unique ecosystem of finished intelligence reports and bulletins all in one place and not found anywhere else.

FLASHPOINT · DOMAINTOOLS · INTEL471 · OpenPhish · POLYSWARM

Integrate CTI workflows

Share IOC data with any compatible CTI solution via STIX/TAXII, or use the API to pull IOCs, documents and feeds from Silobreaker into the workflows you already use to share and enrich information.

EclecticIQ · MALTEGO · splunk> · ThreatConnect · THREATQUOTIENT · STIX TAXII

Primary cyber threat intelligence use cases

RANSOMWARE INTELLIGENCE

Identify ransomware and other malware targeting your organisation or industry, profiling threat actors, attack types and TTPs to deliver actionable intelligence.

VULNERABILITY INTELLIGENCE

Automatically identify and connect CVEs to threat actors and your technology with clear reports and alerts to effectively prioritise patching.

APT MONITORING

Discover APT group activities, including exposure of trade secrets, theft of data and compromise of critical infrastructure to proactively defend against them.

PHISHING INTELLIGENCE

Detect phishing campaigns targeting your organisation, employees, or customers with contextual analysis of threat actors, domains and infrastructure.

DATA BREACHES

Be ready to respond to data breaches and monitor for third-party vendor breaches that could impact your supply chains, such as ransomware and DDoS attacks.

ASSET MONITORING

Maintain visibility of employee credentials and other sensitive data across paste sites and dark web forums to prevent the misuse or sale of these valuable assets.

Reduce risk faster and with fewer tools

Silobreaker provides everything you need to make intelligence-led decisions. Faster

86% Faster actionable intelligence

Accelerate the intelligence cycle with a single workflow, providing aggregation, contextualisation and dissemination of intelligence.

27% Improved analyst productivity

Provide faster and higher-quality insight with automated and PIR-driven intelligence from millions of sources curated for over ten years.

401%+ Return on investment

Answer more security use cases with a single tool, streamline operational costs and improve decision-making from more actionable intelligence.

Source: ESG Economic Validation, analysing the economic benefits of the Silobreaker security intelligence platform

Learn more and request a demo
silobreaker.com