Cyberint
Impactful Intelligence

Cyberint Argos Platform

Threat Intelligence Data Lake Datasheet

The Cyberint Argos platform continuously scans and gathers intelligence from the open, deep and dark web. All intel items are added to an intelligence data lake, which can be filtered and queried by source, threat category, risk level, language, date of publication, and more. Custom queries can be saved to trigger automatic alerts.

Cyberint's Argos platform provides real-time threat intelligence, gathered from thousands of sources across the open, deep and dark web. The intelligence that Cyberint collects is augmented with operation intelligence from numerous feeds and enriched with insights on the threat groups and TTPs associated with the flagged indicator.

An array of advanced crawlers and proxies enable exhaustive data collection while maintaining anonymity. Examples of current sources include social media feeds (Facebook, Twitter, YouTube, etc.), online cyber-dedicated sources (XSS, Exploit DB, Hack Forums etc.), paste sites (such as pastebin.com, pastie.org, etc.) and a continuously updated list of dark net marketplaces, chat rooms and forums where bad actors convene.

The Cyberint Argos platform correlates your digital assets with the intelligence data lake to identify relevant information and threats.

Key Benefits:

- Improve visibility on potential threats across the open, deep and dark web
- Uncover relevant, impactful intelligence items to eliminate risks faster
- Accelerate investigations and threat hunting processes
- Create complex queries using a number of parameters and data filters
- Establish rules and custom alerting based your organization's threat profile

Complete Visibility Across the Open, Deep and Dark Web

Cyberint collects over 40 Million intelligence items every month, which are continuously added to our security data lake, providing complete and real-time visibility across the web.

Open Web Sources

Cyberint continuously scans 2.5 billion IP addresses, plus paste bins, data dump sites, & phishing sites that misuse brands.

Deep Web Sources

Cyberint monitors chatter and data dumps on Discord, Telegram, and other closed threat actor groups.

Dark Web Sources

Cyberint infiltrates hidden threat actor forums and marketplaces on the dark web to gather intelligence.

A Searchable Data Lake Of Real-Time Threat Intelligence

All the intelligence that Cyberint gathers is automatically sanitized, structured, and added to the data lake. Customers can make and save complex queries to receive immediate alerts about new threats.

Establish Complex Queries

Search Cyberint's data lake with complex queries across many different dimensions and parameters.

Customize Your Alerts

Establish custom alerts to detect relevant and respond to threats the moment they are added to the data lake.

Set Up Automated Playbooks

Integrate the Argos platform with your SIEM, XDR, and/or SOAR to run automated playbooks against alerts.

Accelerate The Detection & Disruption Of Relevant Threats

Reduce the amount of time your team needs to spend on investigations and threat hunting with Cyberint's intelligence data lake and the forensic canvas module.

Proactively Hunt For Threats

Use the Argos platform's threat intelligence data lake to simplify and accelerate threat hunting processes.

Speed Up Investigations

Use Cyberint's intelligence data lake and forensic canvas module to streamline investigations and save time.

Identify & Eliminate Risks Faster

Find and takedown relevant threats before they develop into full-blown attacks that cause financial damages.

About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.