Cyberint
Impactful Intelligence

CYBERINT ARGOS PLATFORM

THREAT INTEL DATA LAKE DATASHEET

The Cyberint Argos platform continuously collects mass quantities of data from the open, deep and dark web. All intelligence items collected are aggregated into a data lake, which can be filtered and queried by source, threat category, risk level, language, date, and more. Custom queries can be saved to trigger automatic alerts.

Challenge

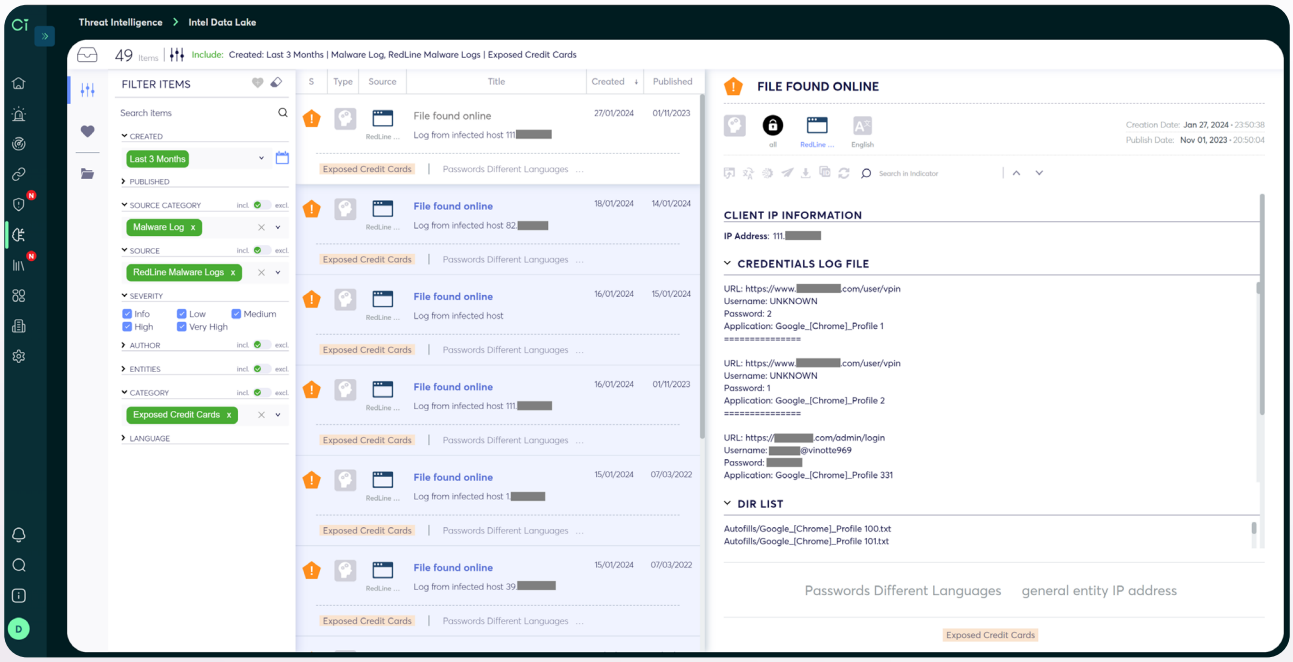
Cyber attacks are becoming more frequent, more sophisticated, and more costly for businesses. To proactively mitigate the risk of a cyber attack, enterprise security teams need extended visibility into the hidden corners of the Internet where threat actors coordinate and execute their attacks. It's impossible to gain this visibility manually and building an automated system requires expertise, time, and lots of additional IT infrastructure.

Solution

Cyberint's Argos platform is a cloud-based SaaS solution that provides real-time cyber threat intelligence gathered from thousands of sources across the open, deep and dark web. The Intel Data Lake grants access to a massive quantity of intelligence, which can be filtered along many different parameters and searched using complex queries, enabling extensive visibility into the web.

Key Benefits:

- Improve visibility on potential threats across the open, deep and dark web
- Uncover relevant, impactful intelligence items to eliminate risks faster
- Elevate and 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 55 Million intelligence items every month, which are continuously added to the threat intelligence 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 Tor sites, such as threat actor forums and marketplaces, to gather intelligence.

A Searchable Data Lake Of Real-Time Threat Intelligence

All the intelligence that Cyberint gathers is automatically structured, tagged, 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.

Enhance Threat Hunting & Investigation Capabilities

Level-up cyber investigations and threat hunting activities with access to an enormous intelligence data lake that provides unparalleled visibility into cyber criminal behavior, communications, and TTPs.

Proactively Hunt For Threats

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

Speed Up Investigations

Use Cyberint's intelligence data lake and forensic canvas module to gain new insights and streamline investigations.

Identify & Eliminate Risks Faster

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

> “Because we’re a small team, the Cyberint analysts are like an extension of us, which really helps from a risk management standpoint.”
>
> Evans Duvall, Cyber Security Engineer, Terex
>
> Read more in the customer case study.

> “We realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.”
>
> Benjamin Bachmann, Head of Group Information Security, Ströer
>
> Read more in the customer case study.

> “Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Cyberint to help us automatically detect and takedown these threats.”
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies
>
> Read more in the customer case study.

Recognition As An Industry Leader From Trusted Analysts

Gartner FROST & SULLIVAN IDC

Discover Cyberint with a personalized demo

About Cyberint

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform’s patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com