Cyberint
Impactful Intelligence

CYBERINT ARGOS PLATFORM

RISK INTELLIGENCE FEED DATASHEET

Cyberint's Risk Intelligence Feed, API, and Google Chrome browser extension integrate IoC (Indicators of Compromise) data from multiple open feeds, as well as Cyberint's proprietary intelligence, into one comprehensive source. The tool enriches your security stack, blocklists, threat intelligence research, and threat hunting program with IoCs, risk scores and context.

Challenge

The cyber threat landscape is constantly evolving at a rapid pace. Threat actors are developing new techniques and exploits at a rate that exceeds the ability of security teams to manually ingest, analyze, and process those threats to stay informed, make timely decisions, and prevent as well as respond effectively to attacks.

Solution

Cyberint's Risk Intelligence feed provides cybersecurity teams with structured and automated access to curated, high-fidelity, up-to-date data about emerging cyber threats. These feeds help you proactively detect and defend against evolving threats, in turn saving time and resources while increasing the value you derive from existing security tools and investments.

Key Benefits:

- Supercharge your security stack with IoCs, their risk scores, and enrichments
- Improve threat hunting activities by gaining context and understanding of relevant threats and attack infrastructure
- Elevate threat research by enriching your IoCs through the risk intelligence API
- Enrich IoCs on demand via the API or the Google Chrome browser extension
- Customize your feed with smart filtering (e.g. only C2 servers' IP addresses)
- Easy integrate with other security tools with out-of-the box integrations plus a REST API

Risk Intelligence Feeds Architecture

Cyberint collects and analyzes IoCs from best-in-class OSINT sources, as well as Cyberint's unique array of open, deep and dark web sources. The feed can be downloaded manually or pushed into any TIP, SIEM, SOAR, XDR, WAF, and firewall.

Expand Proactive Cyber Risk Mitigation Capabilities

Enrich your security platforms, blocklists, and threat research program with IoCs and relevant enrichments. Use the API to provide complete alert handling cycles for your SIEM and SOAR systems.

Gain Necessary Context

The feed provides risk score, context, attribution, and enrichment to identify emerging risks and proactively mitigate them.

Build Your Own Feed

Adjust content according to your risk tolerance and other specifications.

Access Exclusive Intelligence

With over 800,000 detections every day, the Argos data lake is an extensive body of threat intelligence.

Automate detection and protection against malicious activities

Establish playbooks and automated response actions with a real-time IoC feed. Conduct deeper investigations, elevate threat hunting, and proactively block emerging risks.

C2 servers

Prevent outbound traffic to C2 servers.

Botnets

Prevent botnet attacks, such as DDoS attacks.

Infected Machines

Correlate organizational IPs with known infected machines.

Anonymization

Block and run automations against Tor exit nodes IPs.

Phishing

Prevent communication with phishing indicators.

Malware Payloads

Detect and receive alerts on malicious file hashes.

"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