Cyberint
Impactful Intelligence

Cyberint Argos Platform

# Risk Intelligence Feed Datasheet

Cyberint's Risk Intelligence Feed, API, and Google Chrome browser extension integrate Indicators of Compromise (IOC) 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 score, 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 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

## Expand pre-emptive capabilities across the board

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 better understand 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

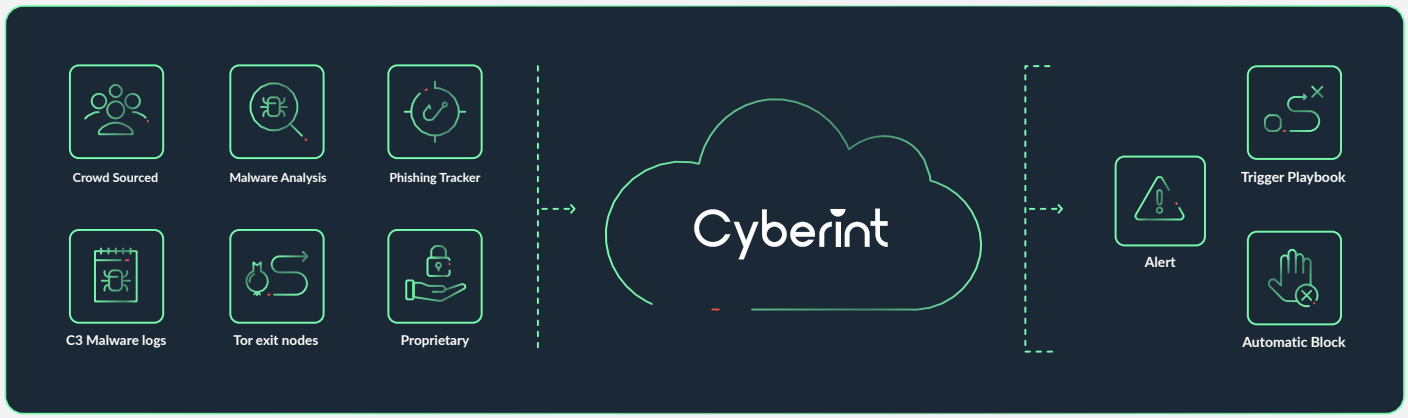
Prevent communication with phishing indicators.

### Malware Payloads

Detect and receive alerts on malicious file hashes.

## 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, EDR, WAF, and firewall.




## Cover and enrich a broad array of IOC types and attributes

The feed provides risk score, context, attribution, and enrichment so you can better understand emerging risks, optimize mitigations, and prevent security incidents.

### Supported IOC Types

- IP addresses
- Domain names
- File hashes
- URLs

### Attributes

- Maliciousness score
- Context
- Activity classification
- Confidence
- Detection date
- Enrichment (API only)

### Detected Activities

- Malware payloads
- C2 Servers
- Infected Machines
- Phishing Websites
- Payload Delivery
- Botnets
- Anonymization

## 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.