Data Sheet

Cyberint

Risk intelligence feed

Enrich your security stack, blocklists, threat intelligence research, and threat hunting with Indicators of compromise (IOCs), risk score and context. Leverage daily feed or enrichment API to turbo-charge your security stack with hi-octane risk intelligence

Executive Summary

Cyberint fuses threat intelligence with 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, it allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier on the cyber killchain.

Cyberint now offers contextual indicators

Cyberint, a pioneer in attack surface reconnaissance, now offers contextual indicators of compromise (IOCs) API and daily feed for enriching your security platforms, blocklists, threat research, and threat hunting activities with IOCs and context.

Using the Argos chrome extension

Cybersecurity professionals can easily gain additional context for any IOC in their SaaS security products such as SIEM and SOAR to provide complete alert handling cycles.

⊘ Benefits

- **Supercharge your security stack** with IOCs, their risk score and context

- **Improve threat hunting activities** by gaining contextualized insights and understanding of relevant threats

- **Elevate threat research** by enriching your IOCs through the risk intelligence API

- **Enrich IOCs on demand** Via the API or the browser extension

- **Build your own feed** with smart filtering (e.g. only C2 servers' IP addresses)

- **Easy Integration into your security stack** with a simple script, based on REST:API

- **Highly Secured** ensuring the integrity, confidentiality, and security of all data

Architecture

Argos collects and analyzes IOCs from OSINT best-in-class sources as well as from Cyberint's unique array of open, deep, and dark sources. Leveraging this extensive database, Argos now offers a contextual IOC query API and a daily IOC feed for enriching your security technologies, blocklists, threat intelligence research, and threat hunting with Indicators, their risk score and additional context. The API can be used by different SIEM and SOAR systems to provide complete alert handling cycles. Cyberint's risk intelligence feed can be downloaded manually or pushed into any TIP, SIEM, SOAR, EDR, WAF, and Firewall.
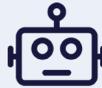

Crowd Sourced   Malware Analysis   Phishing Tracker

C3 Malware logs   TOR exit nodes   Proprietary

Cyberint

Trigger Playbook

Alert

Automatic Block

Use cases

C2 Servers
Prevent malware outbound communication afterinfection. Block C2 Servers.

Botnets
Prevent Botnet based phishing/DDOS attacks. Block known Botnet networks.

Infected Machines
Continuously correlate organizational IPs with detected Infected machines.

Anonymization
Detect TOR exit nodes IPs. Trigger SOAR playbooks when TOR communication to the organization is established.

Phishing
Prevent communication with Phishing sites. Block known phishing servers.

Malware Payload
Detect malicious file hashes. Alert security team when a malicious Hash is detected.

Coverage

Supported IOC Types

- IP
- Domain
- File hashes
- URL

Attributes

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

Detected activities

- Malware payload
- C2 servers
- Infected machines
- Phishing websites
- Payload delivery
- Botnet
- Anonymization

Chrome extension

Enrich any IOC and get its risk score, attribution, confidence and more. Detect C2 Servers, Botnets, Infected Machines and more within any webpage in a click of button. Works perfectly with your web interfaces of SOC systems, SIEM, EDR, and any blogs and news sites

IP.IP.IP.IP   IPv4 Address

RISK   90 ❗
Very High

Type	Observed	Description	Confidence
Payload Delivery	27 Feb, 2022	Detected hosting malware, recognized as Cobalt Strike	80
CNC Server	27 Feb, 2022	Detected hosting malware, recognized as Cobalt Strike	90

ENRICHMENTS

ASN
    Number:
    Organization:
Geo
    Country:

powered by **Cyberint**

Security

Cyberint is compliant with the highest information security standards. It leverages the greatest and latest technologies to make sure that data stays safe and private.
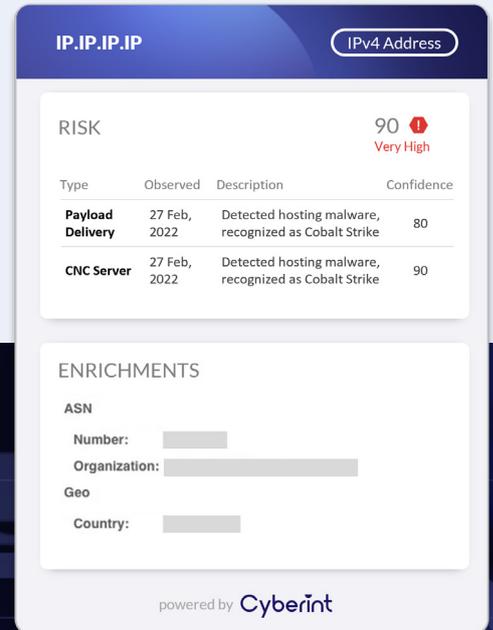
ISO27001   SOC2 compliant

The future of threat intelligence: attack surface focused intelligence

With the maturity of technologies such as attack surface management, and automated threat intelligence, Cyberint is taking the next step into attack surface reconnaissance. The synergy between external attack surface management and threat intelligence, provides a focused solution that increases cybersecurity teams' confidence in their ability to prevent, detect, understand and defend against external risks.

Cyberint fuses threat intelligence with 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.

Contact us at contact@cyberint.com
To learn more how Cyberint helps organizations uncover and mitigate their most relevant external risks earlier visit www.cyberint.com

Cyberint