Cyberint
A Check Point Company

Infinity External Risk Management Services

RISK INTELLIGENCE FEED DATASHEET

YOU DESERVE THE BEST SECURITY

Cyberint's Risk Intelligence Feed is powered by the Big Data collected by Check Point's global network of firewalls, gateways, and other Internet-facing network security devices. With over 1.7 million malicious indicators detected and analyzed each day, Cyberint's Risk Intelligence Feed gives customers real-time threat data with unmatched breadth and depth.

CHALLENGE

The cyber threat landscape evolves at a rapid pace. Threat actors are constantly abandoning old infrastructure that has been identified as malicious, then spinning up new domains and IP addresses from which they can launch attacks. Cybersecurity teams struggle to keep pace. If old IOCs that are now benign persist in generating alerts, then the SOC team wastes valuable time on false positive alerts. Similarly, if new IOCs are not ingested and monitored, real attacks may go undetected.

SOLUTION

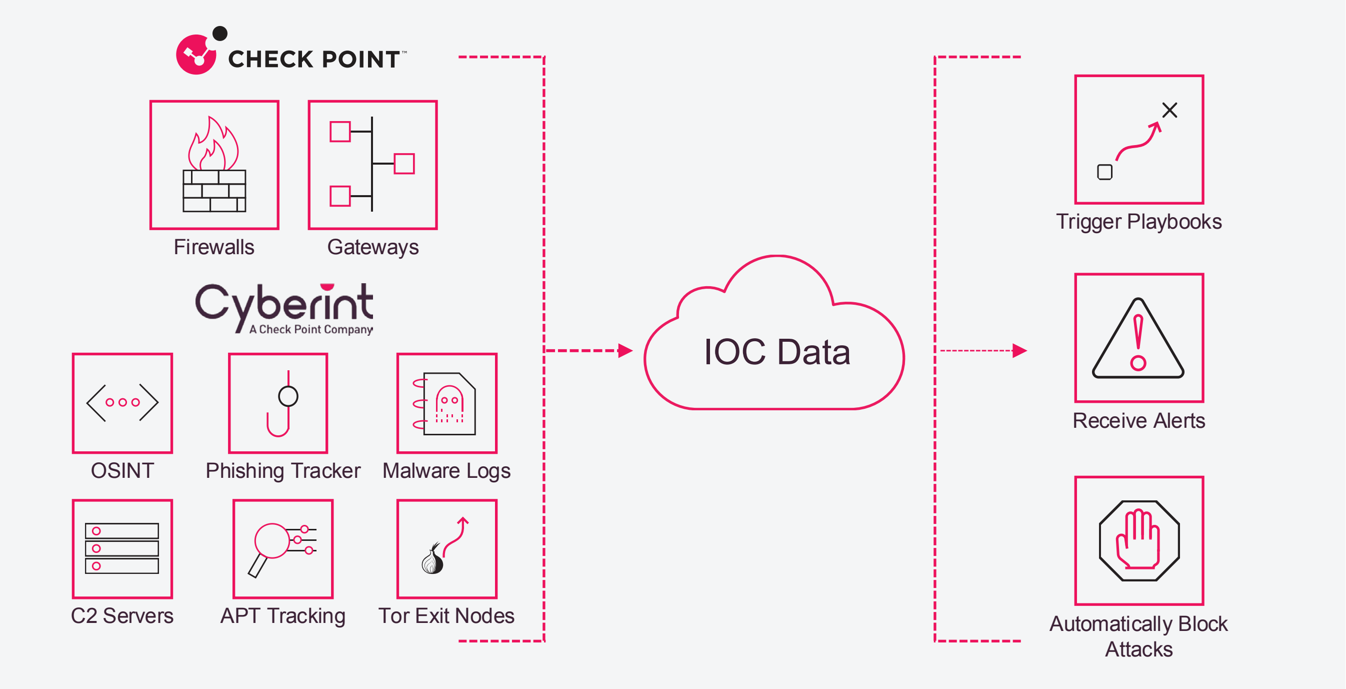
Cyberint's Risk Intelligence Feed provides cybersecurity teams with automated access to enriched, high-fidelity, up-to-the-second data about emerging cyber threats. With more than 3.7 billion websites and files inspected daily through Check Point's global network of firewalls and gateways, customers can trust that the data they receive is accurate and current. Cyberint's IOCs can be integrated into existing tools, such as SIEM, TIP, XDR, and SOAR, streamlining security operations.

KEY BENEFITS

- Supercharge your security stack with market-leading IOC data. Gain the intelligence you need, when you need it.
- Extend visibility with access to real-time threat data collected through Check Point's massive customer network.
- Filters IOCs along many dimensions, including IOC type, confidence level, threat category, region, and much more.
- Easy ingest IOCs into other security tools with out-of-the box integrations plus a REST API
- Improve threat hunting activities with IOC enrichments that provides context and insights on malicious infrastructure.

Risk Intelligence Feeds Architecture

Cyberint Risk Intelligence Feed combines best-in-class OSINT data with proprietary intelligence collected from Cyberint's sources across the open, deep and dark web, plus data gathered from Check Point's global network of firewalls and gateways. Threat data and IOCs can be consumed via a daily IOC feed, on-demand IOC enrichment through an API, Cyberint's Google Chrome browser extension, or through the Threat Hunting License.



Level Up To Preventative Security Posture

Enrich your security program with real-time access to industry-leading threat data collected from a massive network of data collection points around the globe. .

Access Exclusive Intelligence

With over 1.7 Million detections every day, the Cyberint Risk Intelligence Feed is unmatched by any other cyber vendor.

Global Visibility In Real-Time

Understand which IOCs pose a real risk and which can be ignored with real-time data validated globally from millions of collection points.

Gain Context & Enrichments

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

Leverage Threat Data Across Many Use Cases

Enrich your security operations tools, threat hunting activities, network security, and more with Cyberint's Risk Intelligence Feed.

Boost SOC Productivity

Use the Cyberint Risk Intelligence Feed API to streamline alert handling cycles for your SIEM and SOAR tools.

Elevate Threat Hunting

Threat hunters can quickly and easily enrich any IOC from the Google Chrome extension, the API, or the investigations tool.

Enhance Network Security

Cyberint's IOCs can be used to proactively block malicious traffic from your IDS/IPS, firewalls, WAFs, and more.

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 Check Point analysts are like an extension of us, which really helps from a risk management standpoint.**
>
> Evans Duvall, Cyber Security Engineer, Terex

> **We realized that Check Point 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

> **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 Check Point to help us automatically detect and takedown these threats.**
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies

SCHEDULE A DEMO

Recognition As An Industry Leader From Trusted Analysts

Gartner · FROST & SULLIVAN · G2 · IDC

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution 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 Check Point External Risk Management 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 / checkpoint.com/erm