

Infinity External Risk Management Services

SUPPORTING SERVICES DATASHEET

YOU DESERVE THE BEST SECURITY

Cyberint, a Check Point company, provides supporting services to help your team save time and reduce risk, maximizing the value of your deployment of the Infinity External Risk Management solution. An assigned analyst triages and enriches alerts, proactively hunts for threats, and directly supports your team. Our cyber threat intelligence experts conduct investigations, generate custom reports, and manage takedowns.

CHALLENGE

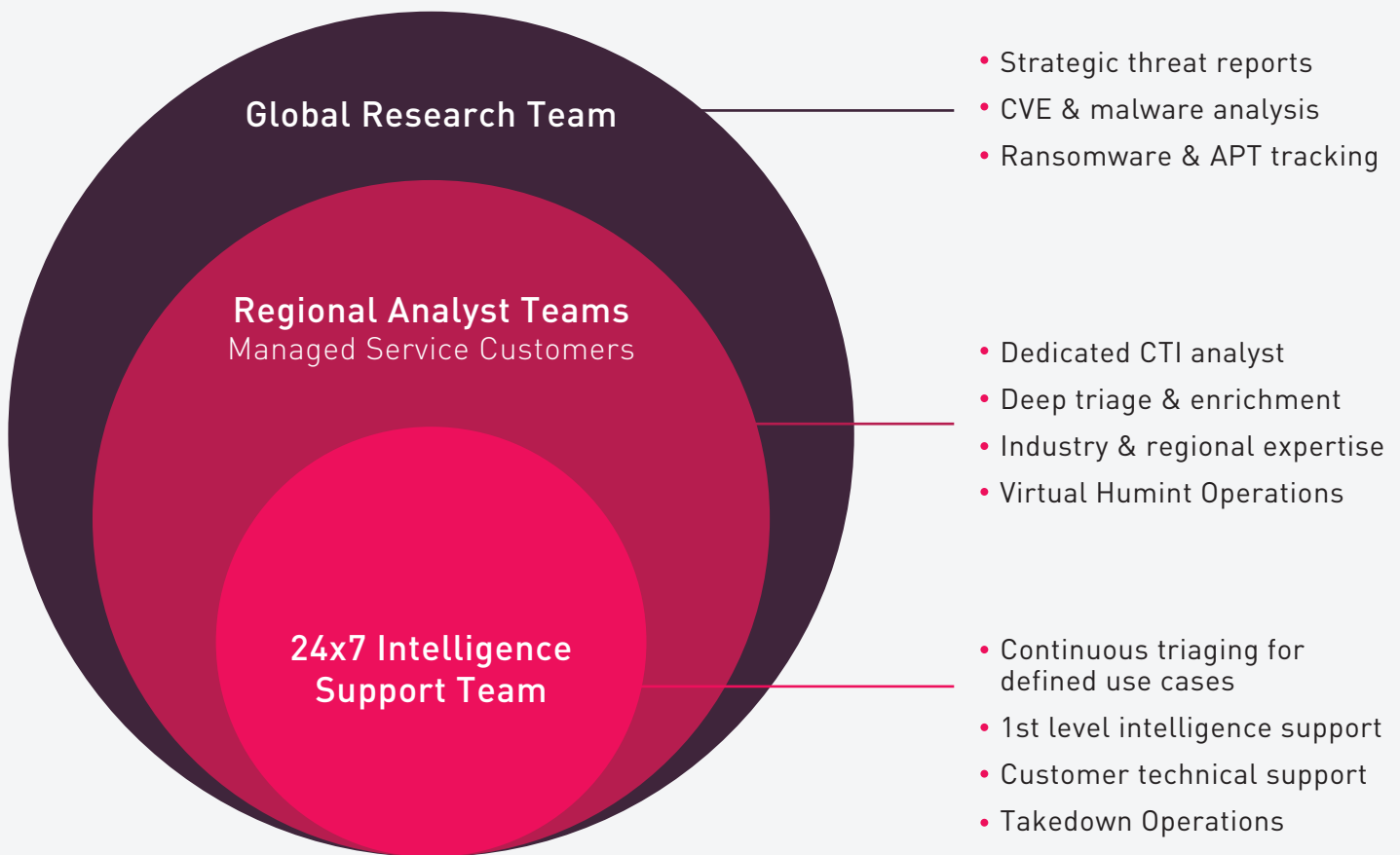
Cyber security teams are short on talent and time, even at large organizations with ample resources. Cyber attacks are becoming more severe and more frequent, forcing SOC and threat intelligence teams to manage a constant flood of alerts. A high rate of false positives consumes valuable time, distracts from the real risks, and increases the probability that a true positive alert gets overlooked or ignored.

SOLUTION

Supporting services help you gain maximum value from the Infinity ERM solution by directly assisting in the management of your tenant and relevant risks. A dedicated intelligence analyst with regional cyber expertise acts as an extension of your team by triaging and enriching alerts, proactively hunting for threats, and serving as your point of contact for technical questions. Our global support team provides 24x7 support while cyber experts conduct investigations, produce custom reports, and takedown malicious content.

KEY BENEFITS

- Leverage our team's deep cyber security expertise with an assigned analyst that serves as an extension of your team.
- Save time with impactful intelligence alerts that have been triaged, validated, and enriched by your named analyst.
- Receive 24x7 support to ask questions, request additional information, and accelerate response and remediation.
- Request customer investigations, bespoke threat intelligence reports, and other human-driven darkweb operations.
- Reduce cyber risks by quickly taking down malicious content, compromised credentials, and leaked data.



Extend Your Team With An Assigned Expert

Our expert analysts reduce your team's workload by surfacing only the most impactful intelligence, thus accelerating response and remediation activities and saving your team time.

Triage & Enrichment Of Alerts

An expert analyst triages low-confidence alerts and adds important enrichments to true positive alerts.

Proactive Threat Hunting

Your assigned analyst learns your environment, as well as your PIRs, and uses that info to hunt for relevant risks.

24x7 Support & Enablement

We run a 24x7 support team to ensure that help is available whenever your team needs it.

Leverage Exclusive Access To The Deep & Dark Web

Our team's threat intelligence experts maintain avatars on dark web forums and marketplaces to gather intelligence, conduct manual investigations, and run other dark web operations for our customers.

Bespoke Investigations

Launch custom investigations to better understand a specific threat, the bad actors targeting your organization, and the best ways to mitigate the risks.

Threat Landscape Reports

Request strategic risk assessments and threat landscape reports to understand the top threats in your organization's industry and geography.

Threat Actor Profiling

Leverage Cyberint's dark web avatars to chat with threat actors, understand their motivations, reveal their TTPs, and ultimately shut down their operations.

Remove Malicious Content & Leaked Data As Quickly As Possible

We have an in-house takedown team that can quickly take malicious and illegal content offline, from phishing websites and impersonation on social media to stolen credentials and leaked data.

Takedowns Of Illegal Content

Takedown illegal use of trademarks, such as logos and brand names, on phishing sites or social media profiles.

Removal Of Leaked Data

Remove sensitive data, like PII, intellectual property, or source code, if it is leaked by a bad actor on a pastebin or code repository.

Purchase Of Stolen Credentials

Purchase stolen credentials that are offered for sale on dark web marketplaces or forums to mitigate the risk of breach.



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

F R O S T
S U L L I V A N



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