Cyberint

Impactful Intelligence

CYBERINT ARGOS PLATFORM

THREAT HUNTING LICENSE DATASHEET

Cyberint's Threat Hunting license provides a suite of product modules to support the research, investigation, and hunting of cyber threats. These capabilities help you understand your threat landscape and the specific risks you face, enabling you to proactively defend against probable threats, investigate incidents after an attack has been detected, and uncover hidden threats that bypassed existing security controls.

Challenge

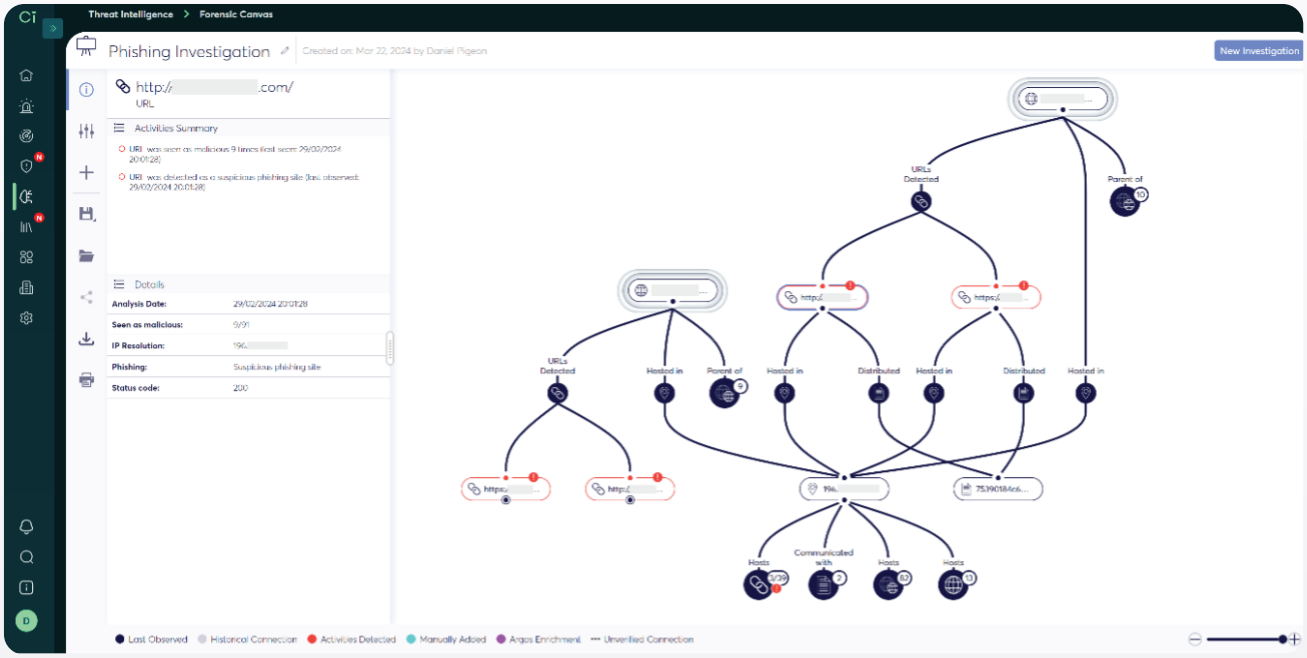
Many organizations seek to elevate their cyber threat intelligence program but lack the insights needed to do so. While IoC feeds and broad-scope threat reports are valuable, they aren't tailored to the defender's organization. Advanced CTI teams need access to relevant data to understand their specific threat landscape, conduct deep-dive investigations, and proactively hunt for threats that existing security controls may have missed.

Solution

The Cyberint Threat Hunting License enhances CTI capabilities along 3 dimensions: research, investigations, and threat hunting. Research capabilities shed light on the specific risks you face and the threat groups most likely to target your organization. Investigations tools help you understand the full scope of an attack after it's been detected so you can respond and mitigate all risks. Threat hunting activities are supported with a filtered view of your landscape according to region and industry, as well as enriched IoC data so you can root out previously undetected threats.

Key Benefits:

- Level up your CTI program to increase its impact, reduce cyber risk and demonstrate value.
- Research your regional and industry-specific threat landscape to understand the risks you face.
- Drill down on specific threat groups, malware families, or documented CVEs in the Threat Knowledgebase.
- Run thorough investigations to uncoverthe full extent of the malicious infrastructure targeting you.
- Gain visibility into the deep and dark web and run complex search queries through Cyberint's Intel Data Lake.
- Develop accurate threat hunting hypotheses and access the data you need to uncover hidden threats.



Research The Risks Most Common in Your Threat Landscape

The cyber threat landscape varies across regions and from one industry to the next. Cyberint reveals your organization's landscape and provides extensive data on relevant actors, malware, and CVEs.

View Your Regional & Sectoral Landscape

Filter by region or country plus industry to see the threat groups most active in your organization's specific threat landscape.

Access A Threat Intel Knowledgebase

Cyberint's Threat Knowledgebase provides a wealth of information on threat actors, malware families, and CVEs.

Monitor Threats On The Dark Web

Track and monitor specific threat actors, forums, and marketplaces with the Intel Data Lake module.

Conduct Investigations & Uncover The Full Scope Of An Attack

Once an attack has been detected, it's essential to quickly uncover the extent of the malicious activity so the risks can be fully mitigated. Cyberint provides the tools needed to run these investigations.

Investigate Malicious Infrastructure

Enter a malicious IoC to launch an investigation and uncover additional malicious infrastructure.

Leverage A Dark Web Search Engine

Cyberint's Intel Data Lake supports complex queries, providing exclusive insights into the deep and dark web.

Establish An Early Warning System

Run complex queries, save them as custom alerting rules, and receive notifications in real-time when there's a hit.

Leverage Intelligence To Proactively Hunt For Undetected Threats

Threat Hunting programs identify threats that have bypassed existing security controls and breached the corporate network. Cyberint provides deep insights and IoC data to support these activities.

View Your Landscape's Common TTPs

Understand the most common tactic, techniques, and procedures used by the bad actors in your landscape.

Craft A Threat Huning Hypothesis

Generate an accurate threat hunting hypothesis that will increase the probability of a successful hunt.

Access & Download Enriched IoC Data

Access enriched IoC data associated with the specific actors, malware families, or threats you would like to hunt for.

"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 G2 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