Cyberint
A Check Point Company

Check Point External Risk Management

THREAT HUNTING LICENSE DATASHEET

YOU DESERVE THE BEST SECURITY

Check Point External Risk Management's Threat Hunting User license provides a suite of product modules to support the research, investigation, and hunting of cyber threats. These capabilities help you to proactively defend against probable attacks, investigate incidents after an attack is detected, and uncover hidden threats that bypassed existing 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

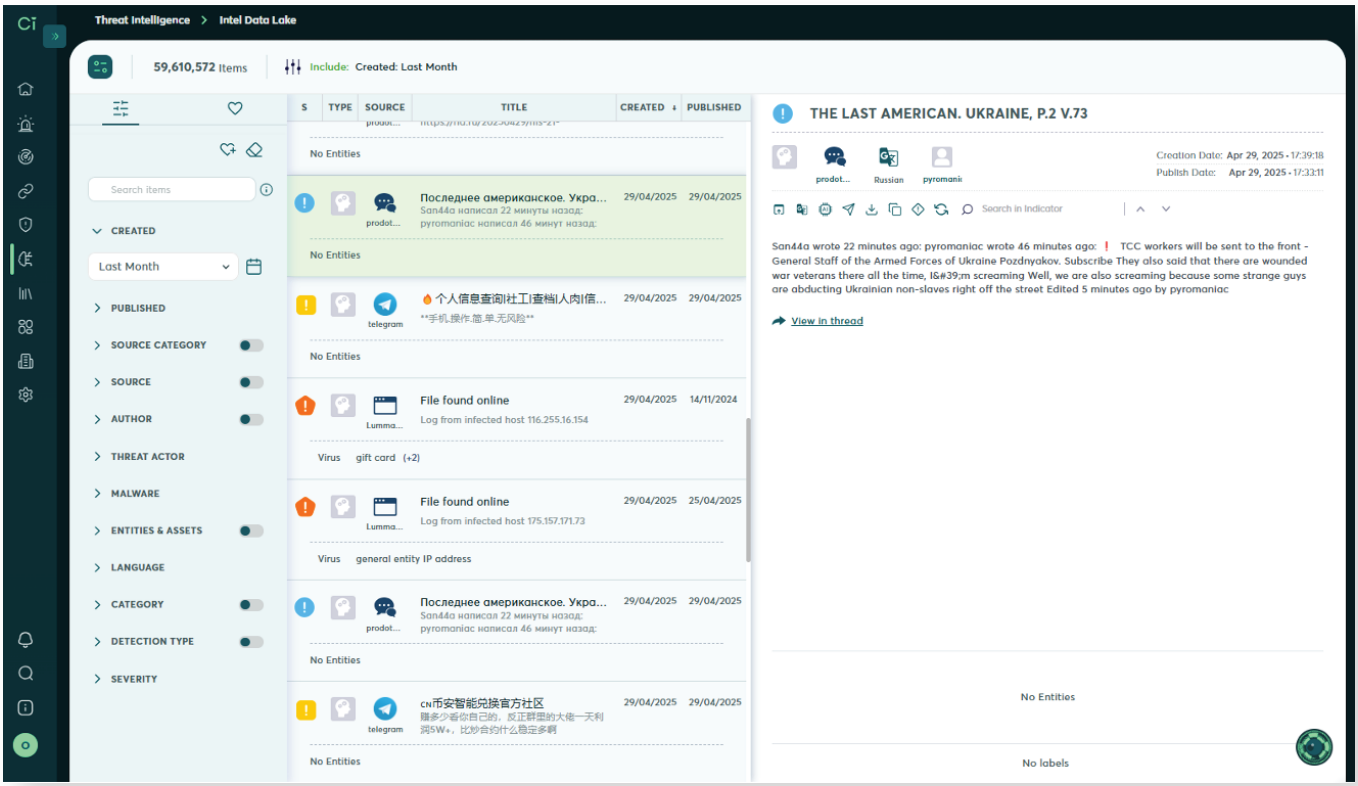
The External Risk Management (ERM) Threat Hunting License grants an existing user access to enhanced CTI capabilities with 5 modules: Intel Data Lake, Forensic Canvas, Threat Knowledgebase, Threat Emulation, and the ThreatScope AI tool. These capabilities enable organizations to conduct advanced risk assessments, threat modeling, investigations, and proactive threat hunting activities.

KEY BENEFITS

- Model probable attacks by researching your regional and industry-specific threat landscape.
- Run exhaustive investigations to uncover the full extent of malicious infrastructure.
- Gain visibility into the deep and dark web and run complex search queries with the Threat Intel Data Lake.
- Upload suspicious files to a secure sandbox environment for automated analysis and results in near real-time.
- Develop accurate threat hunting hypotheses and access the data you need to uncover hidden threats.

Access a Dark Web Search Engine

Every month, the ERM solution collects over 60 million intelligence items from across the open, deep and dark web, which are all structured and fed into the Intel Data Lake.



Gain Instant Visibility Into the Deep & Dark Web

ERM's Intel Data Lake is the aggregation of hundreds of millions of intel items collected from thousands of sources.

Run Complex Queries to Find Useful Intel

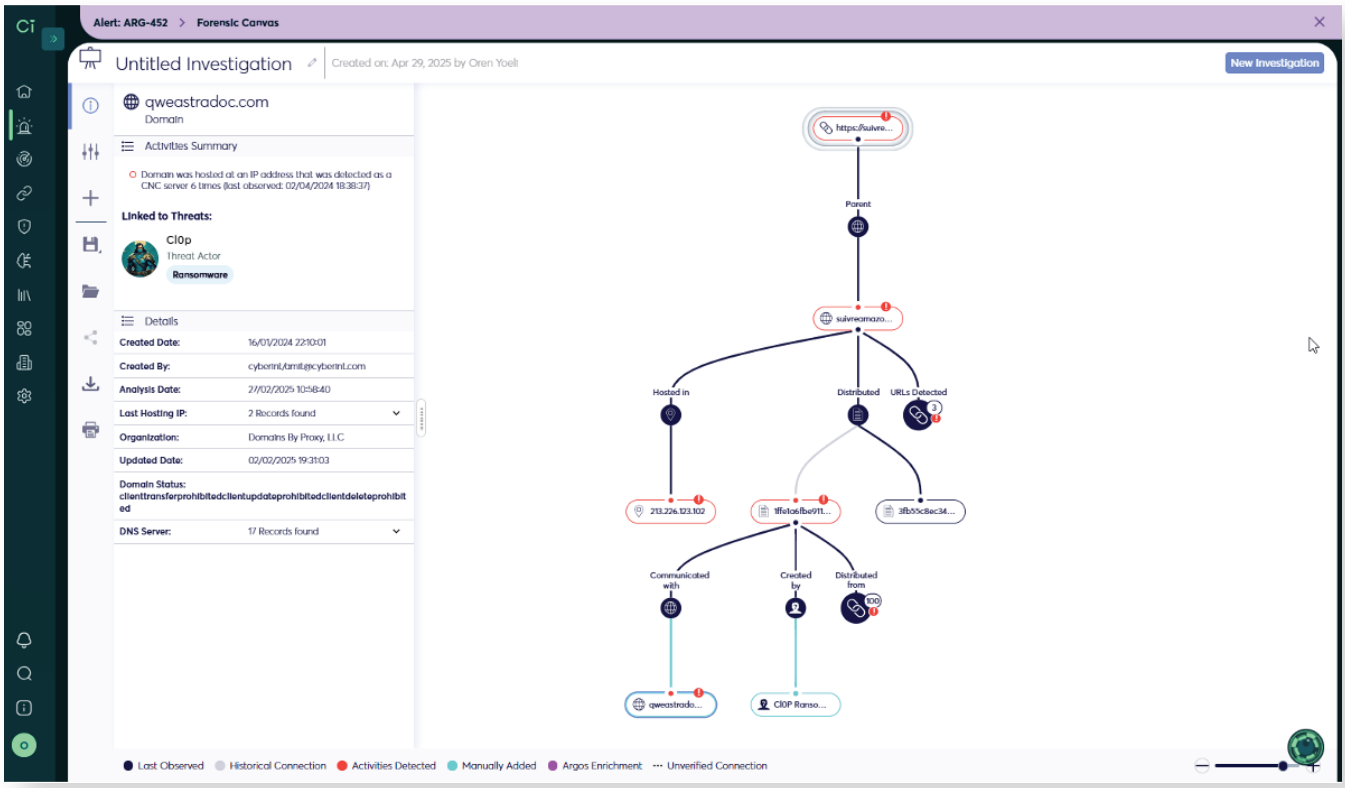
Set filters and enter complex queries to drill down on the intel that's most meaningful to your organization.

Establish an Early Warning System

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

Conduct Thorough Investigations

When an alert comes in, it's essential to quickly validate the threat and uncover the extent of the malicious infrastructure involved. The Forensic Canvas accelerates this investigation process.



Quickly Validate Alerts & Threats

Enrich IoCs associated with an incoming alert to quickly understand whether there is a real threat.

Investigate Malicious Infrastructure

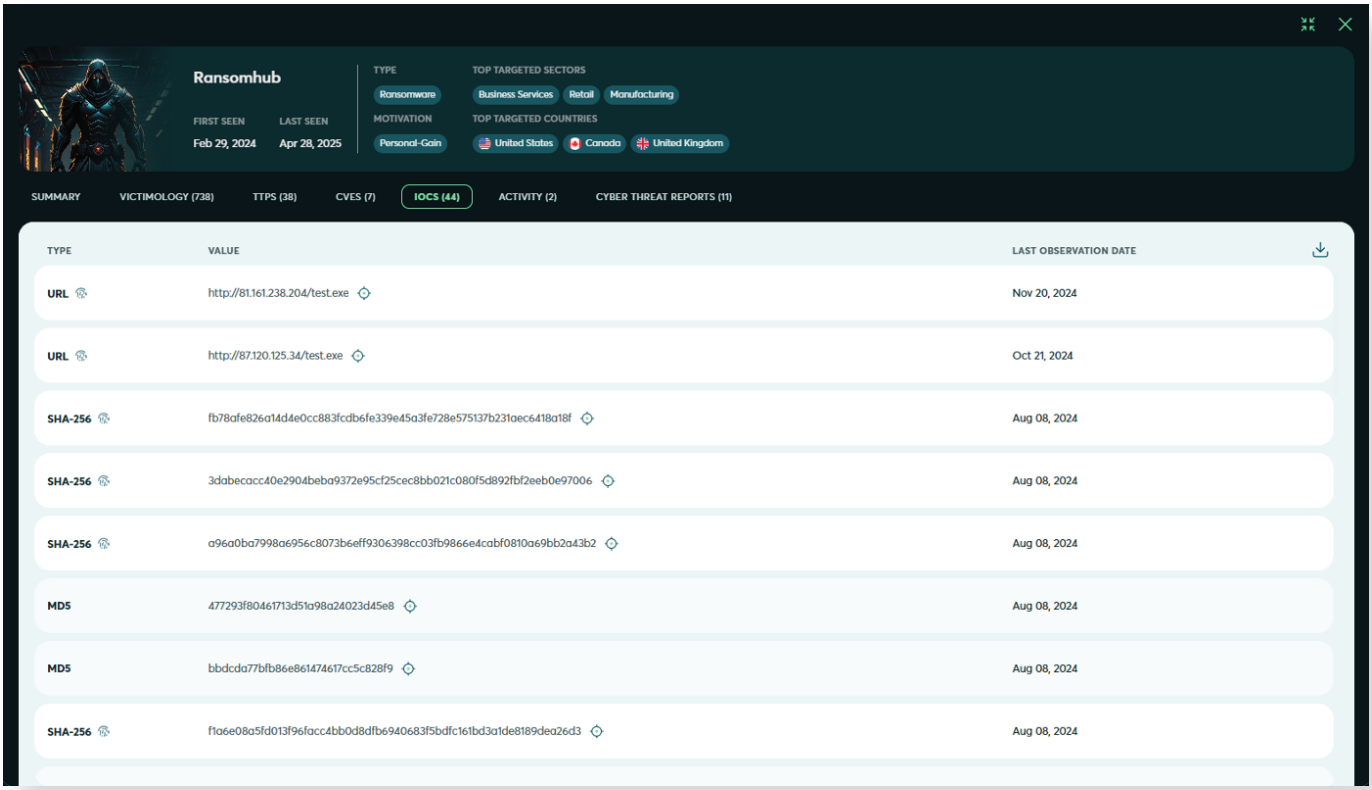
Enter a malicious IoC to launch an investigation and uncover additional malicious infrastructure.

Uncover Links Between IoCs, Malware, and Actors

Automatically view connections between an IoC and any associated malware families or threat groups.

Research Threat Actors & Malware Families

The Threat Knowledgebase contains a library of information on hundreds of specific threat groups and malware families. Research your landscape and drill down on relevant threats.



Explore Your Landscape's Common TTPs

Understand the most common TTPs used by the bad actors and malware in your specific threat landscape.

View a Threat Group's Latest Activity

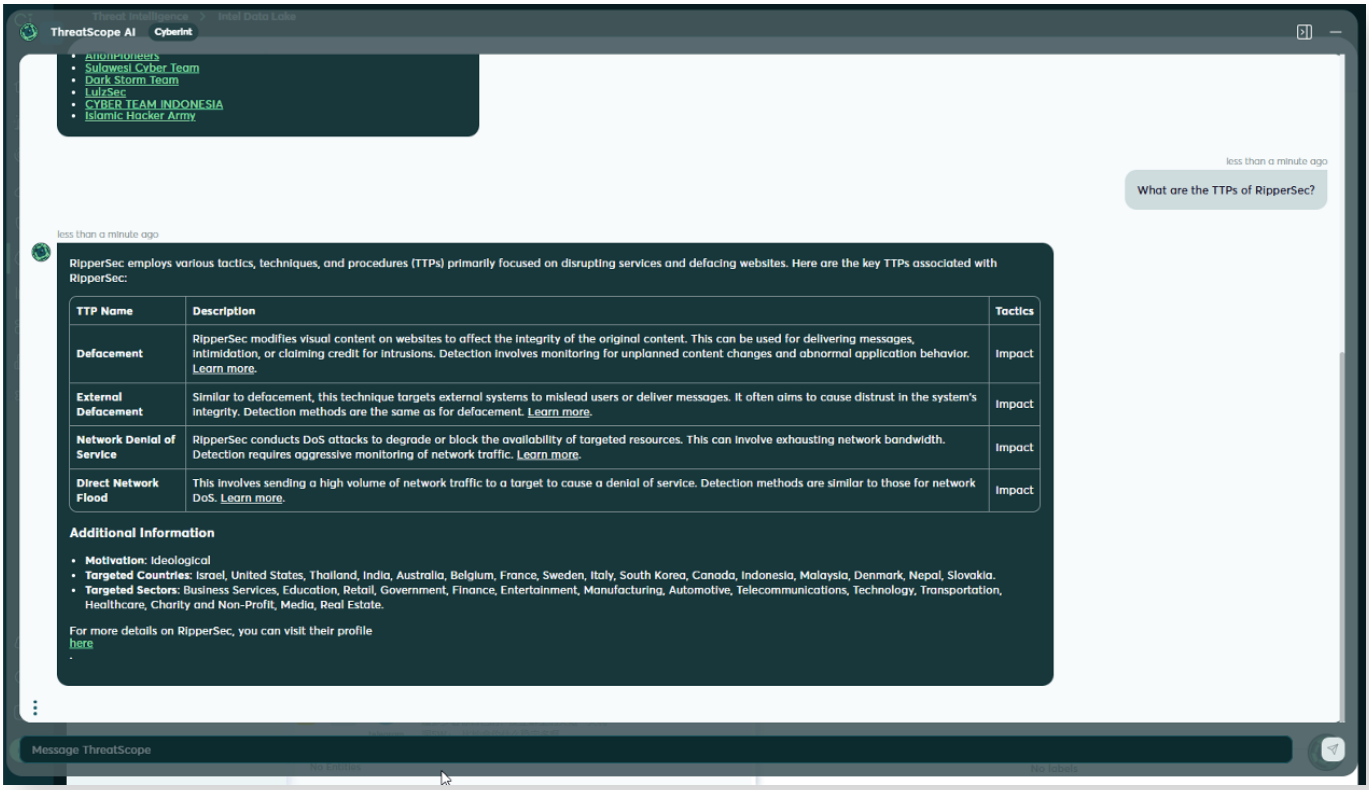
See the latest activity associated with a specific threat group and view the full intel items.

Access & Download Enriched IoC Data

Access enriched IoC data associated with the specific threats you would like to block, research, or hunt for.

Leverage AI to Gain Quick Insights

Use natural language queries to interact with ThreatScope AI, a GenAI tool that has access to all of the relevant data in your organization's ERM environment.



Quickly Prioritize Alerts, Threats, and Tasks

Leverage AI to analyze your tenant and provide guidance on tasks that need attention.

Receive Summaries of Relevant Risks

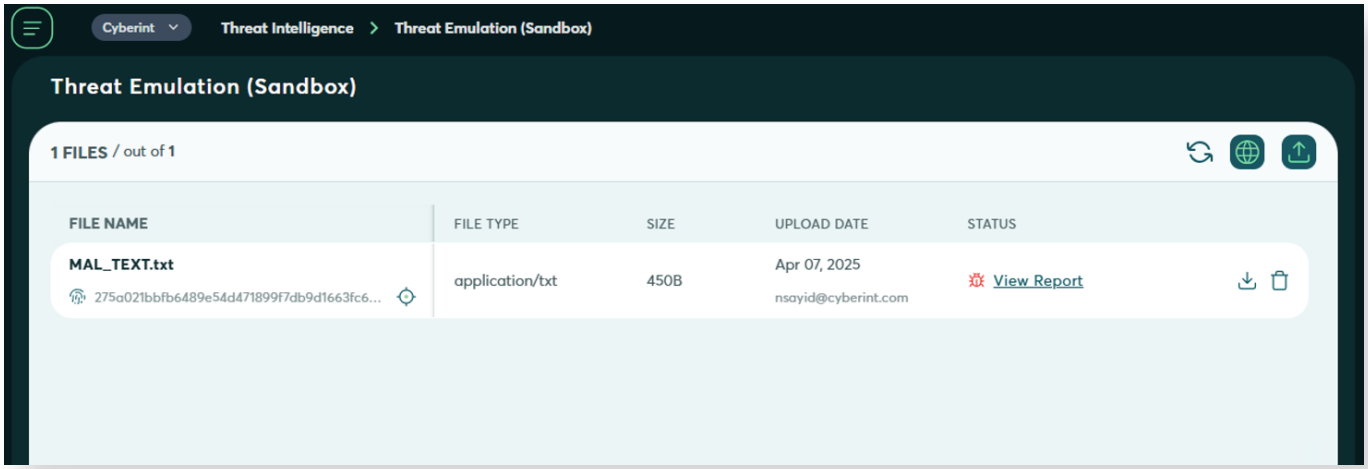
Quickly get data about a CVE, IOC, threat group, malware family, or other threat.

Request Data and Stats for Your Environment

Analyze your organization's external risk posture with a few quick queries.

Quickly Analyze Suspicious Files

Threat Emulation is a secure, virtualized sandbox environment that automatically opens and analyzes files for anomalies, unusual behavior, and other malicious indicators.



Upload Suspicious Files for Fast Analysis

Upload files to the Threat Emulation module to quickly understand if it is malicious.

Uncover Malicious Files & Save Relevant IOCs

View the full analysis, malicious indicators and IOCs associated with a file.

Download Reports to Share with Stakeholders

Download the file analysis results to PDF format to share with colleagues as needed.

> **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