

CYBERINT ARGOS PLATFORM

FORENSIC CANVAS MODULE DATASHEET

Cyberint's Forensic Canvas module integrates data from multiple sources into one, easy-to-use graphical interface to accelerate the investigation of IoCs. The tool displays links between domains, IP addresses, and other IoCs to help uncover threat actor infrastructure, display related threats, and identify the source of the attacks.

Challenge

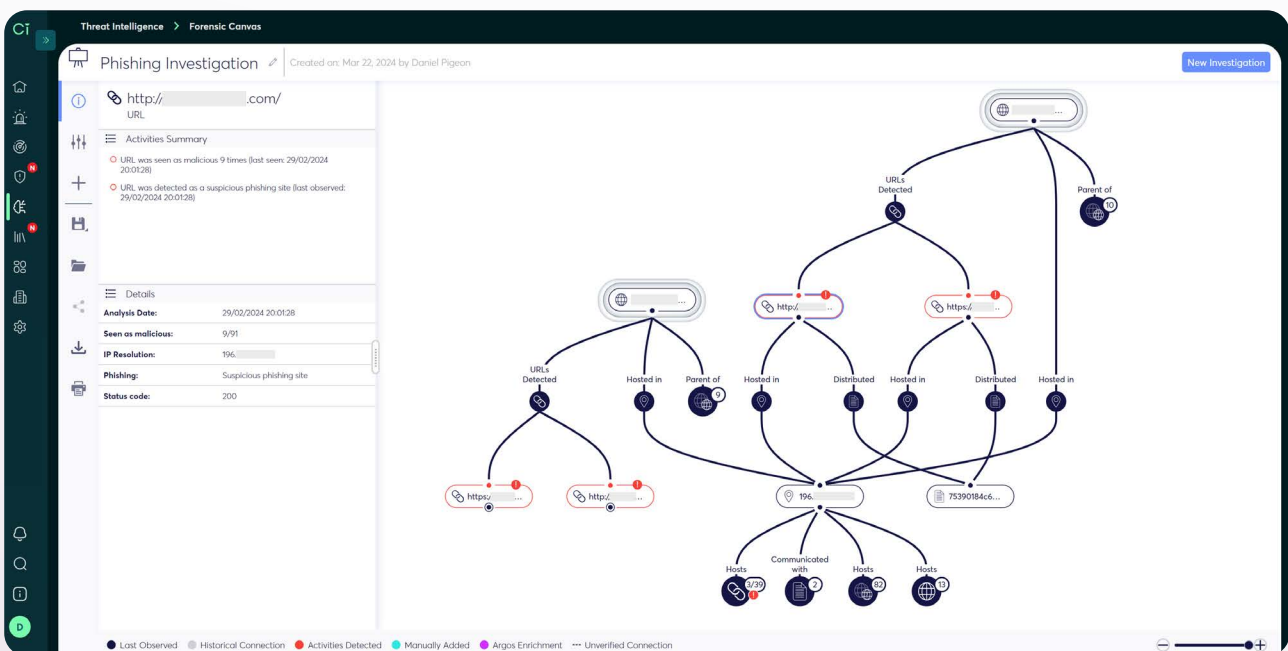
Security teams deal with hundreds or even thousands of alerts every day. Each alert must be triaged to verify whether it represents a real threat but this process requires data from multiple sources, from WHOIS data and DNS lookups to community-sourced IoC feeds and other open source tools. Validating an alert takes time and, all too often, results in wasted resources if the alert turns out to be a false positive.

Solution

Cyberint's Forensic Canvas module saves time by integrating many open data sources, plus proprietary threat intelligence, into a single tool. Security analysts can quickly get all the information they need by simply entering an IoC, then receiving immediate insights into whether the threat is a real risk or a false positive. The tool also supports more robust investigations by revealing malicious infrastructure and other attack campaigns that may be deployed by the same actor.

Key Benefits:

- Quickly gain data from multiple sources with one, simple tool
- Understand if an IoC is truly malicious and requires further analysis
- Optimize your team's efforts and reduce the time spent chasing down false positives
- Accelerate investigations into threat actor infrastructure and related attacks
- Detect & disrupt threats as early in the cyber kill chain as possible



Gain Access To All The Data You Need In One Simple Tool

The Forensic Canvas module ingests and centralizes data from multiple public sources as well as proprietary threat intelligence collected across the open, deep and dark web.

View All The Data You Need In 1 Tool

See WHOIS data, domain registrations, DNS records, file hashes, and other essential data from a single tool.

Explore IoCs In A Graphical Display

Click through IoCs in a graphical interface to reveal additional data and uncover related infrastructure.

Access Proprietary Threat Intelligence

Cyberint incorporates unique threat intelligence so you can uncover risks like malware, phishing, botnets, and more.

Quickly Triage Alerts & Accelerate Advanced Investigations

Streamline security operations and reduce the amount of time your team spends triaging alerts and conducting investigations.

Quickly Triage Alerts & Validate IoCs

Empower your security analysts to immediately understand whether or not a specific IoC is malicious.

Reduce Time Spent On Investigations

Accelerate in-depth investigations with the Forensic Canvas module to save time, defeat threats faster, and stay secure.

Uncover Attack Infrastructure & Source

Protect your organization by unveiling threat actors' infrastructure and viewing any related cyber attack campaigns.

Increase Resilience & Eliminate Threats As Quickly As Possible

The sooner a threat is validated, the sooner it can be mitigated. The Forensic Canvas module speeds up investigation processes to ultimately result in faster remediation and reduced risk.

Identify The True Positives Faster

Filter out the noise and find the real threats faster so you can proactively mitigate security risks.

Leverage Cyberint's Takedown Services

Request a takedown with one click and leverage Cyberint's in-house takedown team that has a >95% success rate.

Protect Your Organization & Stay Secure

Arm your security team with the tools they need to efficiently and effectively protect your networks, systems, and data.



“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



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>