Cyberint

Impactful Intelligence

CYBERINT ARGOS PLATFORM

PHISHING PROTECTION DATASHEET

Cyberint provides comprehensive and proactive protection from phishing attacks. From lookalike domain monitoring and automatic detection of cloned websites to identification of brand impersonation and managed takedown services, Cyberint mitigates phishing risks from end to end.

Challenge

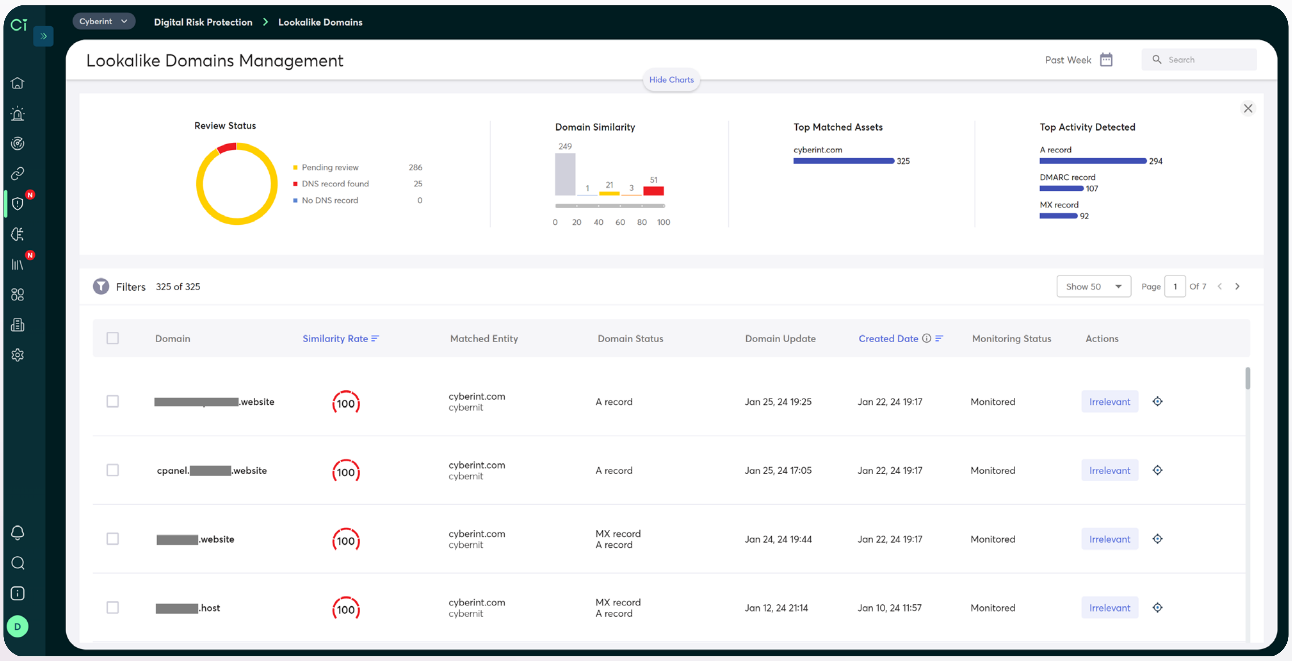
Phishing continues to be a top attack vector in corporate breaches. According to the IBM X-Force Threat Intelligence Index 2024, 30% of corporate breaches begin with phishing for initial access. Threat actors use a variety of phishing techniques, including brand impersonation and social engineering, to fool their victims into opening a malicious file, downloading a malicious app, or simply giving up their credentials.

Solution

The Cyberint Argos platform provides proactive, end-to-end defense against phishing risks. Domain protection quickly alerts you to lookalike domains and misuse of brand names. Argos also detects unauthorized use of your brands and logos. The Phishing Beacon, a proprietary technology developed by Cyberint, immediately detects clones of your organization's websites. The Cyberint team provides takedown services, ensuring that phishing sites are taken offline as quickly as possible.

Key Benefits:

- Identify lookalike domains that mimic your organization or one of its brands or products
- Detect misuse of brand trademarks and logos on third-party websites
- Receive immediate notifications the moment that a clone of one of your legitimate sites is published online
- Monitor the dark web for phishing kits and other signs of an impending attack
- Take down phishing sites as quickly as possible with managed takedown services from Cyberint



□	Domain	Similarity Rate	Matched Entity	Domain Status	Domain Update	Created Date	Monitoring Status	Actions
□	[redacted].website	100	cyberint.com cybernit	A record	Jan 25, 24 19:25	Jan 22, 24 19:17	Monitored	Irrelevant
□	cpanel.[redacted].website	100	cyberint.com cybernit	A record	Jan 25, 24 17:05	Jan 22, 24 19:17	Monitored	Irrelevant
□	[redacted].website	100	cyberint.com cybernit	MX record A record	Jan 24, 24 19:44	Jan 22, 24 19:17	Monitored	Irrelevant
□	[redacted].host	100	cyberint.com cybernit	MX record A record	Jan 12, 24 21:14	Jan 10, 24 11:57	Monitored	Irrelevant

Cyberint

Quickly Detect Lookalike Domains

Registration of a lookalike domain is a strong indicator that a phishing attack is imminent. Detect and monitor lookalike domains to stay two steps ahead of phishing attacks.

Continuous Domain Discovery

Cyberint continuously monitors the open web, WHOIS data, and DNS records to immediately detect suspicious domains.

Detect All Potential Risks

Uncover all typosquatting and lookalikes across domains, subdomains, and subdirectories.

Monitor For Malicious Activity

Monitor suspicious domains, even those with no DNS records or content, in case threat actors launch a phishing attack later.

Identify Clones Of Your Website & Misuse Of Logos

Cyberint uses a number of techniques to proactively detect phishing sites that mimic your organization's legitimate website, impersonate your brand, and abuse your logos.

Get Immediate Visibility On Clones

Cyberint's Phishing Beacon sends a signal within seconds of a clone of your website being published online.

Uncover Misuse Of Logos

Cyberint detects unauthorized usage of your organization's trademarked logos on phishing sites.

Protect Your Brands' Reputation

Prevent threat actors from damaging your reputation or hurting consumer confidence in your brand with phishing attacks.

Fast & Effective Takedown Services

After a phishing site is detected, Cyberint customers can request a fully-managed takedown from Cyberint's dedicated takedown team with just one click from within the platform.

850+ Takedowns Each Month

The Cyberint team averages more than 850 takedowns per month, many within 24 hours of receiving the request.

99% Takedown Success Rate

Cyberint's takedown team has held a 99% phishing site takedown success rate for the past 8 quarters.

Simple & Fast Requests Process

Customers can request a takedown with the click of a single button in the Cyberint Argos platform.

> “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

Cyberint