Cyberint
Impactful Intelligence

Cyberint Argos Platform

Phishing Beacon Datasheet

The Cyberint Phishing Beacon is an innovative technology that proactively detects clones of your organization's websites. An alert is issued immediately when an exact replica of one of your webpages is published online, enable you to respond and disrupt the threat the moment it appears online.

Challenge

In the majority of phishing attacks, adversaries simply clone a trusted brand's website to fool unsuspecting victims into downloading malware or giving up their credentials. By using a clone of a legitimate website, threat actors can easily deploy a convincing lookalike site and reduce the amount of time they need to spend on the attack, thus increasing the success and profitably of the attack.

Solution

The Phishing Beacon, a patented technology from Cyberint, is an obfuscated script that you embed in all your organization's web properties. If bad actors create a clone of one of your pages, the Phishing Beacon sends a signal back to the Argos platform the moment the replica is published online. This enables you to proactively takedown the threat before the attack develops and causes damages.

Key Benefits:

- Protect your brand, customers, and employees from phishing attacks
- Get immediate alerts whenever a page from your web properties is cloned
- Receive only targeted, high-fidelity alerts relevant to your organization
- Proactively respond to phishing sites before the attack can fully develop
- Leverage Cyberint's fast and effective takedown services to eliminate risk

Immediately Identify Clones Of Your Website

Cyberint's Phishing Beacon technology is a unique solution for immediately detecting clones of your website, providing visibility on phishing threats the moment they come into existence.

Near-Zero False Positives

Because alerts are issued only when a replica of your site is deployed, there are virtually no false positives.

Accelerated Detection

Gain real-time alerts when a clone of one of your organization's webpages is published online.

Proactive Response & Takedown

Respond to phishing sites faster and eliminate the threats before they evolve into a costly incident.

Proactively Detect & Disrupt Phishing Threats

Cyberint uses multiple techniques to identify phishing threats as early in the kill chain as possible, helping customers to defeat attacks before they can develop and cause harm.

Domain Protection

Uncover typosquatting and lookalike domains that mimic your organization's legitimate domain.

Brand Protection

Detect unauthorized usage of your organization's brand names and logos on phishing sites.

Proactive Response & Takedown

Respond to phishing sites faster and eliminate the threats before they evolve into a costly incident.

Leverage Cyberint's Professional Takedown Services

After a phishing site is detected, Cyberint customers can choose to take action themselves or request a takedown that will be quickly managed by the Cyberint team.

200+ Takedowns Each Month

The Cyberint team average more than 200 takedowns per month, many within 24 hours of receiving the request.

95% Takedown Success Rate

Cyberint's team of cyber experts have has a 95% success rate in taking down phishing sites.

Simple & Fast Requests Process

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

About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.