Cyberint

Introduction to **Digital Managed Detection and Response**

Overview

While businesses are looking to unlock the potential of digital transformation, they are essentially opening themselves up to far greater risks and an even greater threat environment. CIOs and CISOs are therefore beginning to look at their security environment through a digital lens. In order to be protected in the age of digital transformation, you need to assure you have technology that understands your environment and that can automatically detect and respond to any possible threats. This is where a Digital MDR comes in.

What is Digital Managed Detection and Response Services?

- Identify and respond to threats before they affect your brand and business.
- A service that augments your current cyber security controls with the technology and expertise built for digital.
- Seamless setup means you're better protected within minutes.
- Full discovery and mapping of all your digital assets, including: domains, IPs, websites, landing pages, social media accounts, mobile apps and more.
- Discover and remove rogue and malicious digital assets, such as: Typo squatting domains, assets infected with malware and unknown public facing assets (demos, dev or staging environments).
- Validating your cyber posture, across all business aspects in a rapidly changing threat landscape. Detect and take-down of web-based and mobile phishing.
- Continuous monitoring of your 3rd party vendors' cyber posture.

Why CyberInt?

Our key differentiator is that we provide a holistic approach for protection beyond the perimeter. By identifying threats in advance and checking the company's resilience to the threat from the attackers' perspective. All delivered as a managed service.

Don't take our word for it, here's what our customers had to say.

"Over the last year, CyberInt has helped us re-enforce our defences, improve our detection and response capability and help us reduce our fraud with their detection and response capabilities, in both the technology that they offer and their experienced teams."

Cliff Cohen, CIO Asos

BDO Unibank, Inc. · Groupe Casino Nourrir un monde de diversité · WIX.com · Globe · NICE · Playtika · UOL 华业集团 · ASOS discover fashion online · BPI · SEGA · 888 HOLDINGS · Singtel · amdocs · GIGYA

Why Do You Need Digital Protection?

Attacks Are Moving to Digital

Attack vectors have moved and are more predominant now on digital channels, which include: email, social media, mobile as well as other digital assets. The fact is that your digital assets are continuously used to collect data about you, your employees and customers. As companies continue their digital transformation, the need for digital protection grows.

Cost of cyber crime:

USD **$450 Billion**
in 2016 which is $856,164/minute.

156 Million Phishing Emails
are sent every day, that is 108,333/minute.

50% of Alexa top
500 Sites are Spoofable


allowing threat actors to send their employees spoofed phishing emails resembling their peers.

23% of all attacks in 2016 spawned within the target's supply chain.

Our research shows that you're **74%** more likely to follow through on a spoofed email.

1.92% of all comments, posts and tweets in social media, with a URL in them, lead to malicious content.

Every **3 Minutes** a new malicious app is created.

Almost 100 phishing sites are created **Every Minute.**

Cyberint

United Kingdom
Tel: +442035141515
sales@cyberint.com
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +972-3-7286-777
sales@cyberint.com
3 Columbus Circle | NY 10019 | New York | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
sales@cyberint.com
Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
sales@cyberint.com
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com **www.cyberint.com**