Critical Defence:

A Fresh View of Cyber-Defense

As enterprises make a shift from closely managed systems to a wide range of mobile devices and cloud hosted solutions, cybersecurity challenges are growing exponentially. New Jersey-based cybersecurity company, Critical Defence, focuses on alleviating the challenges posed by the widening threat vector. Discussing the solutions provided by Critical Defence to confront the challenges faced by companies worldwide, Jeffrey Bernstein, Managing Director, sheds light on the measures provided by his firm to improve cybersecurity, the protection of information and data privacy.

We help customers plan for and respond to the latest cybersecurity threats. We are results driven and deliver over and over without compromise

What are the challenges plaguing the industries with regard to cybersecurity?

With modern communication encompassing advanced conferencing systems, multi-functional devices, VoIP and BYOD programs that have the ability to connect with public and private wireless networks and access points, data is more vulnerable to exploitation than ever. In tandem with increased connectivity, the attack surface has increased phenomenally over recent years, extending to automobiles, wearable devices, and systems connected to IoT devices. The need to provide ease of use and access to customers and business partners has increased the level of data security challenges. Additionally, the entry of cloud service providers into the security equation sparks the debate about the safety of data stored in the cloud environment by third-party services providers.

Another major challenge for companies is the lack of security awareness among end-users and a susceptibility to social engineering exploits such as phishing attacks and malicious URLs. The URLs used by cyber-attackers trick unsuspecting end-users to visit malicious sites, download tainted payloads and provide private information and credentials which can be used later or sold. Meeting the challenge of regulatory compliance is also a daunting matter of great concern to businesses of all sizes.

Tell us about your unique strategy to address client's security challenges.

The solutions provided by Critical Defence can be classified into four core areas—Training, Response, Assurance, and Compliance (TRAC).

We perform vulnerability, penetration and red team tests against our clients' networks to show them where they are exposed and to help them fix these deficiencies. We also perform security tests on both web and mobile applications as well as their supporting code to provide organizations with independent 'assurance' of the security posture of these apps. We conduct social engineering studies on client personnel to understand their awareness and resiliency against possible attacks. To help our clients effectively govern the protection of their networks, applications, systems, devices, staff and third-party business partners, we help them develop security policies and procedures, business continuity and disaster recovery plans and incident response and crisis management strategies. When clients decide to move from a legacy infrastructure to cloud solutions, we perform third-party vendor audits to assess the security posture of the cloud service provider. We perform similar studies on other business partners with access to client data. We also design secure cloud strategies as well as strategic information security roadmaps.

Often, we help customers investigate cases where anonymity in the cyber world makes it effortless for an adversary to launch an attack on an individual or an organization. Companies are also dealing with a myriad of challenges created by their own internal users. The incident response and forensics area of our practice caters to the needs of customers of all sizes, sectors and geographies in these circumstances. Some of the sophisticated attacks that we help clients respond to involve website defacements, ransomware, internal employee behavior matters, thefts of funds and data leakages. We have an exceptional team of professional incident responders and we deliver anywhere in the world on a dispatch basis 24x365. More often than not we find ourselves responding to incidents and events on very short notice. We find that many clients lack an ability to effectively respond to security incidents and events properly. Our most popular offering is a retained "forensics and response" service. The clients that subscribe to it receive immediate expert support from us, on-demand at any hour of any day with a simple phone call.

On the compliance front, we focus on the different legal and regulatory issues that govern cybersecurity in industry as well as the various controls frameworks (NIST, ISO, etc.) available to help organizations improve their security controls and comply with these mandates. One main focus currently is the General Data Protection Regulation (GDPR), it goes into effect in May of 2018 and will govern all organizations that process, transmit and/or store citizen data from UK and EU. Our compliance programs ensure that our clients are meeting the requirements of their regulatory authorities while also improving the security and resilience of their critical computing infrastructures.

One of our most important solutions is the training of general audiences on security awareness topics. We deliver training programs specific to C-suite executives and client staff in particular roles including IS, IT, HR and development. When conducting table-top gaming exercises for companies, we immerse staff in simulations of real-world incidents and events to understand how employees will respond to different situations that they might face in the workplace. Being non-abrasive, fun and informative, the clients find the training sessions effective and educational.

We believe that Internet-connected organizations from all sectors are in need of training. Critical Defence sells directly to end clients but also through creative strategic partnerships with firms that have complementary offerings. These partner firms include law firms, insurance companies, physical security and investigative firms,CPAs, IT services companies and other value-added resellers. While we primarily serve the commercial sectors, Critical Defence is also an awardee of a subcontract for a Naval Space and Warfare Systems (SPAWAR) Center Atlantic Integrated Cyber Operations (ICO) initiative.

Jeffrey Bernstein, Managing Director

What were some of the recent landmarks events for Critical Defence and what does the road ahead look like for the company?

In the last year, we delivered successful programs to a long list of satisfied clients. We are results driven and meet or exceed client expectations every time. I don't think there is a single customer that we worked with in 2017 that wouldn't work with us again or recommend us. We also expanded our staff of forensics examiners and moved to a larger, enterprise-class facility that is commensurate with the plans for expansion that I am proud to say we are tracking closely to. Looking at the road ahead, we want to extend our footprint in Canada, particularly Calgary and build a base in Texas which has a significant oil and energy industry. We already have an office in London and want to spread to other parts of the UK and the EU. From the business development standpoint, we plan to grow organically and also acquire regional cybersecurity service providers. CA

CYBERSECURITY SPECIAL

CIO APPLICATIONS

APRIL - 2018
CIOAPPLICATIONS.COM

Company:
Critical Defence

Key Person:
Jeffrey Bernstein
Managing Director

Description:
Critical Defence is a provider of security assurance, response, compliance, intelligence and training services

Website:
criticaldefence.com

Top 25 Cyber Security Companies - 2018

In today's connected world, there is a sharp increase in the use of digital technologies, making businesses more agile and adaptable. However, this has lead to a surge in the number of potential ways cybercriminals can gain access to enterprise networks. Cyber attacks are constantly evolving and its detection is becoming tougher by the day, therefore, it is necessary for businesses to have apt cybersecurity measures in place to thwart these threats. At the helm of helping advance cybersecurity, experts are leveraging the latest technologies and architecting solutions that can proactively identify and eliminate these new-age threats.

Organizations are taking steps like patching and updating systems, regularly backing up data, and strengthening real-time defenses to tackle different kinds of attacks. Innovative technologies like artificial intelligence and machine learning are being used to predict and accurately identify attacks. Multifactor authentication is being implemented by businesses as they are more secure, usually involving biometrics like voice, retina, and fingerprint recognition, thereby making it harder for an attacker to breach a network. Technologies like encryption and tokenization are applied to protect data, dramatically reducing its exposure and risk. Furthermore, deep learning with its ability to identify safe and unsafe software is a significant boon to security practitioners who seek to decrease the time taken for advanced threat detection and eradication.

In the light of this, a distinguished panel comprising CEOs, CIOs, CTOs, and analysts including the CIO Applications editorial board has evaluated and selected the leading cybersecurity solution providers that have in-depth expertise and are at the forefront of tackling any type of cyber attack.

We present to you CIO Applications' "Top 25 Cybersecurity Companies – 2018."

CIO APPLICATIONS

44790 S. Grimmer Blvd
Suite 202, Fremont, CA 94538
T:510.757.1040

www.cioapplications.com