INFINIA
CYBER CONSULTING

INFINIA CYBER CONSULTING
INFORMATION SECURITY

SERVICES OVERVIEW
2019-2020

Introduction

Information Security is a foundation for business growth and sustainability. Safeguarding spiraling volumes of corporate data against unauthorised access, disclosure or misuse has become critical to maintaining operations and meeting increasingly vigorous data privacy compliance requirements.

The “more data problem” comes at the same time as threats from cyber adversaries continue to grow in scale and sophistication. Attacks are very much global and persistent and continue to plague businesses. Regulators, keen for the situation to change for the better, also add to the pressure on CISOs. You need a partner.

Infinia Cyber Consulting is a London-based UK company set up by industry-leading professionals in 2019. The Founders of Infinia have worked together since 2010 largely on Cyber Defence and Information Security Investigations. They combine significant data, legal and financial expertise with unparalleled technical operational subject matter expertise (from 20 years in government and 15 years in the commercial arena) allowing us to create a winning formula for a significant base comprising super-majors, FTSE100 & ‘Big 4’ clients (including BP, Shell, Hess, Lloyds TSB, BAE, HSBC & PwC).

The team can perform full ISO27002 or SOX security audits anywhere in the world through to mobile app decompiling and API testing. The team also performs a significant of red team/blue team type consulting, having been thought leaders in this space since the start.

Remote Security Auditing

Penetration Testing is a two-stage process:

Stage 1 - OSINT (Open Source Intelligence) review of the customer organization:

- Asset discovery of the organization’s networks, services, websites, domain registrations combined with Network mapping.
- Org Chart: email addresses, employee positions, social media accounts, leaked passwords and other available information from breaches. Will include available Darknet sources.
- This stage is largely passive, no active probing, aside from minor port scans take place. We report uncovered flags and endpoints and provide recommendations to correct the organization’s security posture.

Stage 2 - External Penetration testing

- Here we actively attempt to breach the uncovered endpoints in Stage 1 using a combination of manual and semi-automatic tools. Requires detailed terms of engagement - with an approval letter from the end customer and coordination.

On Site Security Services

Tailored to each customer including:

- Architecture Review and IT Security Auditing Services
- Customer DMZ Traffic analysis and IPS rule review
- Full network mapping and vulnerability scan of internal networks
- Client Mobile survey
- Digital forensics

On site Full Security Audit

Offered as a one-off, where an organization wants a single snapshot-in-time of their level of exposure to internet-based risks, or as a recurring exercise, where an organization operating at a higher risk level needs close tracking of possible internet-based problems within specific facilities.

Using the external Pen Test as its first stage, we move within the organization using specialized tools (Intrusion detection devices, network traffic indexing server, wireless survey equipment and so on) to review the internal IT security as seen from an internal attacker. Given that a large percentage of breaches (using client-side malware) are operate as virtual internal attackers, this service is becoming more popular in recent years. With the information provided by these two services, we will review the level of IT defences and management systems within the organization and then perform a weighted risk assessment using the information gathered (test results, internal IT review, the perceived value of each system and the organization policies and procedures). The output is an illuminating report on the next steps to reduce IT related risks within an organization or set of facilities over the medium term (6-24 months).

The test plans and results could be framed within a known control framework (CIS 20, COBIT, NIST) in order to provide supporting evidence for external auditors in jurisdictions with IT regulatory requirements or in order to help customers achieve or maintain quality certifications such as ISO 27001.

Core Values

Confidentiality

Practicality

Timeliness

Professionalism

INFINIA
CYBER CONSULTING

Contact

sales@infinia.cc

London & UAE