TALION

# Security Testing Services

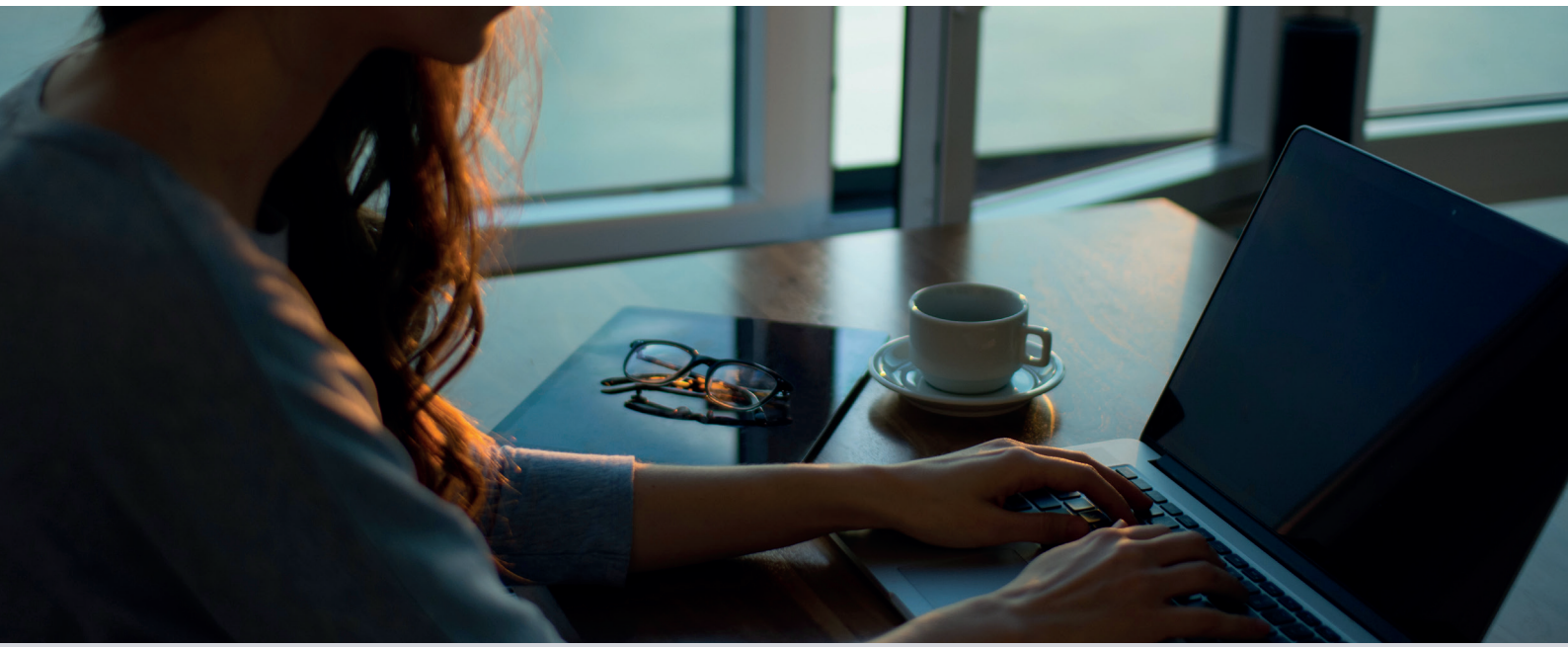
## Understand the effectiveness of your security controls

Our security consultants focus on bringing a customer centric testing service.  Our security testing combines the benefits of consultant-led penetration tests and vulnerability assurance with a technologically advanced delivery model.

Our security testers are CREST and CHECK accredited and have attained the NCSC Cyber Essentials and Cyber Essentials Plus accreditations. We are also accredited to ISO:9001 and ISO:27001.

Our specialised team of security consultants hold industry qualifications such as CHECK Team Leader, CCIE, CISSP and CEH and combine this with many years of industry experience.

Whether you require a one-time assessment or a series of testing to show improvements over time, our catalogue of services will deliver against these requirements and provide you with actionable outcomes.



# Security Testing Services

## Assessments

We offer a series of assessment services, that act as a point in time measure for potential risks within your business. For many, these assessments are driven by a business requirement; the need to achieve an accreditation, a high priority risk that needs to be understood, or a change in your way of working.

We offer the following assessments:

### Remote Working Security Assessment

Assess the security of your remote working solution, ensuring that configuration issues are not exposing your corporate data and systems to unauthorised users.

There are a variety of technical solutions on the market allowing remote workers to access corporate resources from any location. These include site-to-site and client-based virtual private networks (VPNs), remote email access portals, and document shares to name just a few. They allow business as usual activities to continue when employees cannot work from the office. However, with so many different solutions and possible configurations, there is the risk of a software or configuration issue introducing a vulnerability that could be exploited by a remote attacker.

Our Remote Working Security Assessment service is tailored around the unique needs of each client so you can be assured that you are not opening your corporate network to further risks.

### API Security Assessment

The versatility of APIs to interact with multiple technologies and languages provides businesses with greater opportunities to connect with other providers. However, APIs are not inherently secure, and often present new security concerns and potentially a wider attack surface.

The API Security Assessment service can be used to identify vulnerabilities that exist on your API. These tests can be performed on an API directly, or in accompaniment with any associated Web application assessment.

### Server / Endpoint Build Review

When building multiple servers and workstations in an office environment, it is typical for a 'standard' build image to be used. This image has been built with a fully patched operating system and configured following the business server/workstation hardening procedure. This procedure is designed to reduce the risk of configuration vulnerabilities leading to a security breach.

The Server / Endpoint Build Review provides the assurance that the business host hardening procedure includes all the necessary steps to sufficiently secure the host. The assessment identifies issues such as missing operating system and third-party software patches, but also examines the myriad security configurations that mitigate the risk of privilege escalation exploits, network-based attacks, and weak passwords.

# Security Testing Services

### Firewall Configuration Assessment

A well configured firewall can significantly mitigate the risk of unauthorised connections to services and can be placed at the network layer both internally and externally, or be software based on a single host. However, the granularity of configuration options increases the likelihood of vulnerabilities or misconfigurations; these could expose hosts and services that are fully segmented.

The Firewall Configuration Assessment can identify general configuration, software, and rule set specific vulnerabilities or misconfigurations that exist on the firewall device(s). Testing includes not just an assessment of the chosen authentication controls, but also a thorough examination of other wireless attack vectors.

### Red Team Assessment

The typical approach for security testing is to perform modular tests with clearly defined scopes. However, this is not usually the approach taken by real-world attackers who don't have rules to abide by and time restraints to adhere to. Therefore, to simulate a realistic targeted attack, the same approach needs to be taken by security consultants, opening up the scope to all aspects of the entire target company. The primary aim would be to exfiltrate data, rather than to identify as many vulnerabilities as possible. Talion's Red Team Assessment will simulate a real-world targeted attack by a team of highly trained and experienced security specialists. The results can then be used to understand the most significant vulnerabilities spanning the full scope of the company, and the issues most likely to be exploited in a real world scenario.

## Penetration Testing

We offer different levels and types of Penetration Tests to help you understand risks to your business, comply with audit requirements or meet the contractual needs of customers.

Our Penetration Tests range from a targeted test against a specific aspect of your environment to a full end to end assessment. These can be offered as a one-off exercise or as part of a continuous compliance requirement.

We offer the following Penetration Tests:

### Infrastructure Penetration Testing

Infrastructure Penetration Testing to provide a thorough and independent examination of your corporate infrastructure and systems to identify software and configuration based security vulnerabilities.

There are two components to delivering Infrastructure Penetration Testing and these are Internal and External assessments. It is commonplace to combine these into a single test that covers both the internal and external components of the network.

We help alleviate the risks associated with IT Security issues by performing regular Internal and External assessments of your corporate infrastructure to identify if any issues exist and to give you an ability to remediate these before an attacker could exploit them.

# Security Testing Services

### Wireless Infrastructure Penetration Testing

Having both a corporate and guest wireless network infrastructure is now commonplace. Whilst these networks provide convenient access for portable devices, they also present another service for attackers to target. Configuration vulnerabilities are common and could allow an attacker to access corporate resources from guest networks, attack business managed hosts, or even bypass well-established enterprise authentication controls.

Wireless Infrastructure Testing can identify the various configuration vulnerabilities that exist on the wireless networks. Testing includes not just an assessment of the chosen authentication controls, but also a thorough examination of other wireless attack vectors.

### Web Application Penetration Testing

The advancement in web applications and reliance upon such services has exposed users to a variety of new security risks, and made them an ideal target for attackers, demonstrated by the many publicised major data breaches. Protecting these applications from new threats is a constant challenge.

We have a professional Web Application Assessment service that can be used to identify vulnerabilities that exist on your Web applications. We have a wealth of knowledge around application security testing, and their testers have created and contributed to many open-source web application security projects.

### Cyber Essentials Accreditation

Cyber Essentials is a UK Government led and industry-backed scheme that helps organisations of all sizes protect themselves against common cyber-security threats.  From the 1st October 2014, the UK Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

There are currently two levels of certification, Stage 1 which is the basic level and Stage 2 which is also referred to as Cyber Essentials Plus. We can help you with the full certification at both levels including performing the certification assessment.

## About Talion

At Talion, we're changing the way organisations interact with their Managed Security Service Provider.  Born out of BAE Systems, our service is built on first-hand knowledge of military engineering and defence-grade security, together with an in-depth understanding of the threat landscape facing the commercial world today.

When it comes to cyber security, we believe every organisation deserves full visibility and complete control over how threats are monitored, how decisions are made, and how their business is protected. That's why we prioritise transparency and collaboration across our service lines, implementing security programs that give businesses the control and freedom to pursue ambitions and realise goals, safe in the knowledge that we've got their back, 24 hours a day, 7 days a week.

**HQ**
The Hub, Fowler Avenue
Farnborough GU14 7JF

**Security Operations Centre**
Marshall's Mill
Marshall Street
Leeds LS11 9YJ

**Engineering Centre**
Unit 32-01, Level 32
The Vertical Corporate Office
Tower B, Avenue 10
Bangsar South, No 8
Jalan Kerinchi, 59200
Kuala Lumpur, Malaysia