FUJITSU

Penetration Testing

Identify vulnerabilities across your digital environment through controlled, ethical hacking exercises.

We offer a variety of testing options tailored to different environments and needs. Each service includes a clear scope, pricing structure, and a detailed report with actionable recommendations. Optional workshops and follow-up support are available to help implement improvements effectively.

Delivered by certified experts, these services simulate real-world attack scenarios to assess the resilience of your systems, applications, and infrastructure.

- **External Penetration Testing**
- **Internal Penetration Testing**
- **Web App Penetration Testing**
- **Mobile App Penetration Testing**
- **API Security Testing**

Gain clarity, confidence, and control over your environment

Each engagement delivers a clear, outcome-driven report detailing vulnerabilities, risk levels, and tailored remediation guidance, while enhancing security posture and reducing risk exposure.

- **Security assessment** detailing vulnerabilities, risk levels, and potential business impact.
- **Remediation guidance** with steps to resolve identified security flaws.
- **Retest** of high-impact issues to confirm fixes.
- **Concise reporting** and insights that support optimisation, uplift, and strategic decision-making with minimal client disruption.

CREST

As a CREST accredited organisation Fujitsu Cyber is a recognised and validated for it's technical competency and adherence to high standards. Our understanding of the Security Testing domain stems from years of experience working with structured methodologies such as the OWASP, OSSTMM, MITRE, and other frameworks.

External Penetration Testing

Simulate attacks from external actors attempting to gain access to target infrastructure.

This engagement evaluates the security of internet-facing assets by simulating external attacks on perimeter defences, firewalls, VPNs, and public applications, testing exposed services like SSH and HTTP, and identifying entry points through realistic attack scenarios.

Key outcomes

- Confirms which internet-facing assets are exposed and how they could be exploited.
- Demonstrates how external attackers might gain initial access and escalate privileges.
- Identifies and ranks vulnerabilities based on exploitability and potential business impact.
- Assesses resilience of firewalls, VPNs, and publicly accessible assets.

Methodology: OWASP WSTG

Deliverables

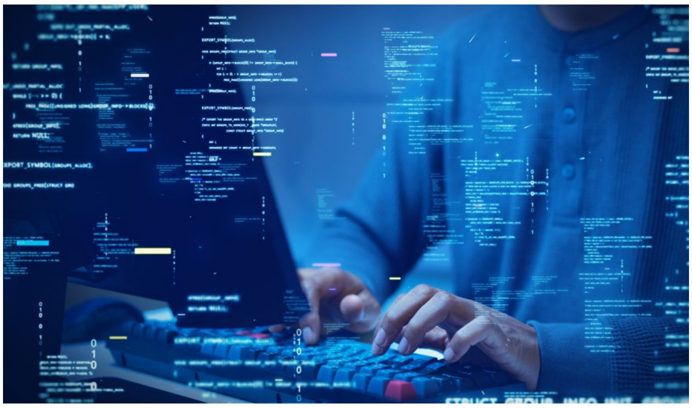
- Detailed security assessment with vulnerabilities and impact analysis.
- Remediation guidance: Steps to resolve identified security flaws.
- Retest of high-impact issues to confirm fixes.

Get in touch

www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security

Fujitsu
Cyber

Internal Penetration Testing



Expose internal weaknesses and limit the impact of an insider attack

Our internal penetration testing simulates an attack from inside your network to uncover vulnerabilities such as weak access controls, privilege escalation paths, and poor segmentation. This approach provides clear insight into the potential reach of a compromised account or malicious internal actor.

Key outcomes

- Simulate attacks from inside the network (insider threats, lateral movement, breached scenario).
- Evaluate network segmentation and access control policies.
- Test your organisation's response to real-world attacks from trusted insides.
- Evaluate the effectiveness of internal boundaries and user permissions.

Methodology: MITRE ATT&CK Framework

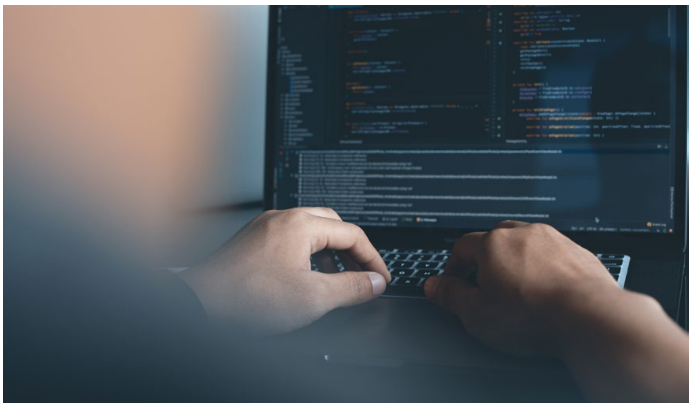
Deliverables

- Detailed security assessment with vulnerabilities and impact analysis.
- Remediation guidance: Steps to resolve identified security flaws.
- Retest of high-impact issues to confirm fixes.

Get in touch

www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security

Web App Penetration Testing



Real-world adversary techniques to assess the security of web applications and their infrastructure.

Using OWASP WSTG and focusing on the Top 10 threats, it delivers expert-led testing, clear reporting, and remediation guidance to strengthen security and support compliance.

Key outcomes

- Identify weaknesses through automated and manual testing. Covers OWASP top 10.
- Safely exploit key findings to demonstrate real-world impact and validate risk exposure.
- Uncover weak points before attackers do.
- Align findings to PCI-DSS, ISO 27001, SOC 2, and other security standards to support audits.

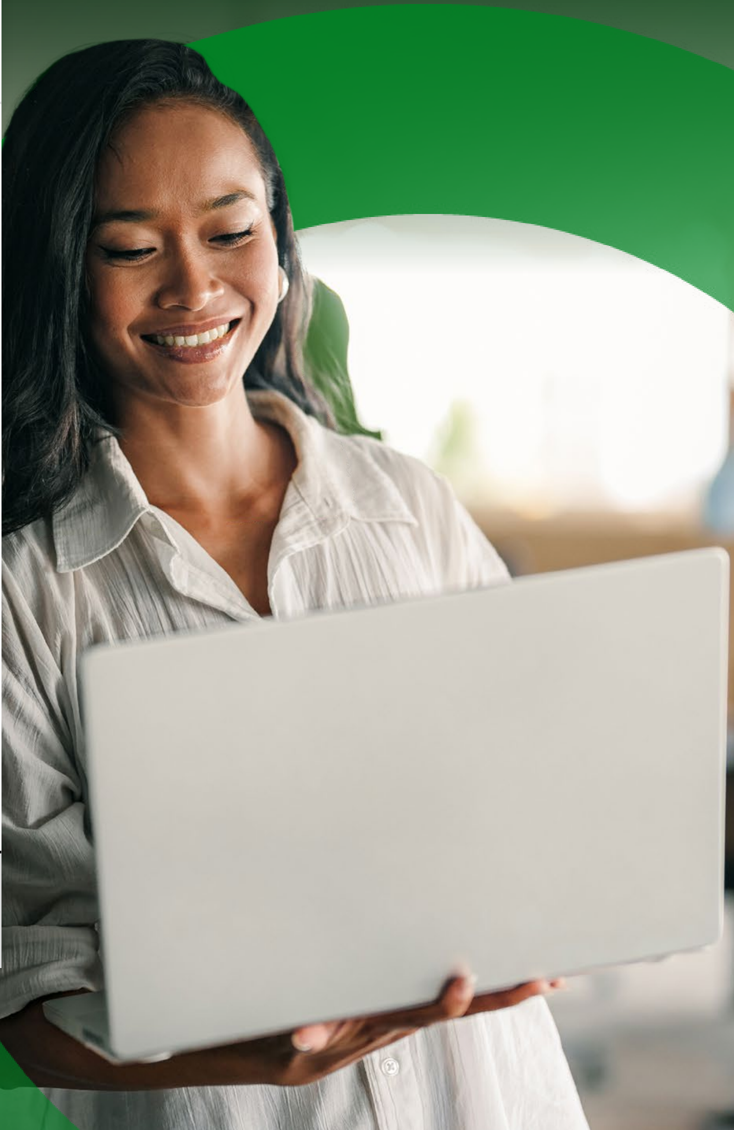
Methodology: OWASP WSTG

Deliverables

- Detailed security assessment with vulnerabilities and impact analysis.
- Remediation guidance: Steps to resolve identified security flaws.
- Retest of high-impact issues to confirm fixes.

Get in touch

www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security



Mobile App Penetration Testing

Ensure mobile apps are secure against various attack vectors.

A comprehensive security assessment of mobile applications on iOS and Android platforms, including testing for data leakage, insecure storage, and improper session handling; review app permissions and perform both static and dynamic analysis.

Key outcomes

- Discovers security flaws in iOS and Android apps using OWASP MASTG.
- Evaluates how the app interact with the mobile OS and backend APIs.
- Simulates attacks to show how vulnerabilities can be exploited.
- Improves code quality through static and dynamic reviews.

Methodology: OWASP MASTG & OWASP MASVS

Deliverables

- Detailed security assessment with vulnerabilities and impact analysis.
- Remediation guidance: Steps to resolve identified security flaws.
- Retest of high-impact issues to confirm fixes.

Get in touch

www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security

Fujitsu
Cyber

API Security Testing

Ensures that APIs are robust against cyber threats, safeguarding sensitive data and system integrity.

Covers authentication and authorisation for access control, encryption and data exposure checks, rate limiting to prevent abuse, injection detection (SQL, XML, NoSQL), business logic flaw identification, and validation against OWASP API Security Top 10.

Key outcomes

Uncover security flaws before they can be exploited.

Reduces the likelihood of breaches, data leaks, and service disruptions.

Validate that APIs meet industry and regulatory security standards.

Demonstrates a proactive approach to protecting systems and data.

Methodology: OWASP API Security Top 10

Deliverables

- Detailed security assessment with vulnerabilities and impact analysis.
- Remediation guidance: Steps to resolve identified security flaws.
- Retesting support: Verification of high-impact issues fixes upon request.

Get in touch

www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security

Seeing your defences through the eyes of an attacker

This perspective enables you to make informed decisions about where to invest, what to fix, and how to strengthen your security posture before real threats emerge.

Why Fujitsu Cyber?

Fujitsu Cyber delivers penetration testing that's precise, risk-driven, and aligned to real-world threats.

Structured approach with minimal disruption.

Deep expertise across enterprise and government clients.

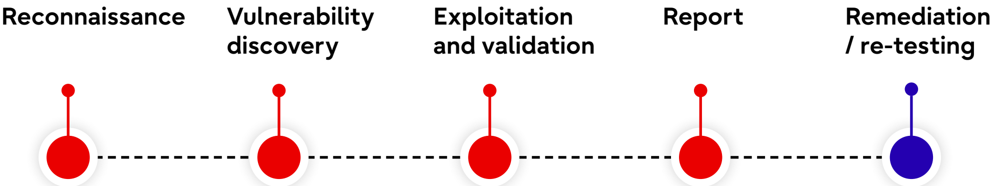
CREST-accredited testing team based in Australia and New Zealand.

Realistic adversary simulation.

Framework alignment with standards such as OWASP, MITRE ATT&CK, and Essential Eight.

End-to-end support from scoping to remediation, ensuring readiness and resilience.

Penetration testing involves gathering and analysing system documentation, interfaces, and authentication mechanisms using automated tools and manual techniques, simulating attacks to identify vulnerabilities, and delivering actionable insights to enhance security.



Reconnaissance

Vulnerability discovery

Exploitation and validation

Report

Remediation / re-testing

Duration: Typically, 4-7 days

Outcomes of Penetration Testing

- **Validates** effectiveness of existing security.
- **Identifies** security vulnerabilities.
- **Provides** actionable recommendations.
- **Improves** compliance posture with industry standards and regulatory requirements.

Our team is here to help you build a stronger, more resilient cybersecurity posture, through expert-led testing, actionable insights, and trusted guidance.

Let's work together to uncover vulnerabilities before they become threats.

Get in touch

Fujitsu Cyber
www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security