

VULNERABILITY ASSESSMENT

Organisations are experiencing threats originating from all parts of the globe, as well as from within their own network. And the number, type and sophistication of cyber security threats are constantly increasing. The motivations of cyber adversaries targeting Australian organisations are many and varied. So even if you think the information held in your business is not valuable, it could still be a target for malicious activities.

How we can help

The Vulnerability Assessment identifies and rates internal/external network infrastructure and web applications for common security vulnerabilities. It evaluates threats to daily operations, and offers insight into your network to prioritise security investment. The service is especially valuable if you're upgrading or moving applications to the cloud, or have to comply with Payment Card Industry security, ISO 27000 and APRA PPG234 standards.

An essential and basic security precaution, we recommend that Vulnerability Assessments are conducted regularly to keep abreast of new threats and vulnerabilities.

The Vulnerability Assessment provides a best of breed scanning platform, QualysGuard, to perform:

- External vulnerability assessment. Conducted from the internet. This tests the network perimeter infrastructure
- Internal vulnerability assessment. Scanning is conducted from within your corporate network. Typically, a scanner is temporarily deployed in the environment

Web application security testing. Conducts a risk assessment of
externally facing web applications against the most common risks
(e.g. OWASP Top 10 risks). This is automated testing, not a manual
application penetration testing (i.e. the service does not attempt
to exploit the vulnerabilities identified). This testing is preferably
conducted in a test environment.

Key benefits

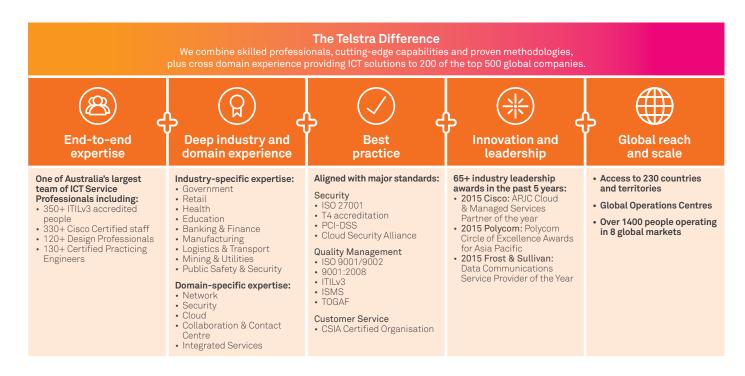
- Find and fix vulnerabilities before hackers can exploit them
- See your network assets the way hackers do
- Address new security and compliance needs as your business expands
- Focus investment on security priorities

ASSESS DISCOVER ANALYSE RECOMMEND What you do What we do What you get Prompt notification when a critical Provide program/project management and co-· Obtain a high-level view of the environment to ordination be tested vulnerability has been identified. Provide all required technical information e.g. • Confirm the systems and IP ranges to be tested This may be before the report is delivered. A draft report in PDF format. IP ranges Confirm required agreements are in place. • Executive Summary: a business view of the when applicable, with any third parties involved · Identification of web applications to be tested results and what they mean in the external hosting and management of the · Possible test user account details, etc. systems to be tested • Methodology: what testing was done and how · Confirm the testing logistics (e.g. times testing Vulnerabilities & Recommendations: a list of can be conducted - e.g. out of business hours) identified and rated vulnerabilities with remediation recommendations • Define the test plan Follow-up call or meeting · Configure the vulnerability assessment platform. This may include the deployment · Discussion of the report and remediation of a virtual internal scanner progress · Run the scan

Why Telstra for Security Consulting?

Our consultants draw on deep practical experience improving security for some of the country's largest mission critical environments, including the largest networks in Australia - our own. They possess internationally recognised qualifications such as CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), CRISC (Certified in Risk and Systems Control) and SANS GIAC (Global Information Assurance Certification).

Our consultants leverage the capabilities of our Security Operations Centre which constantly collects data from the internet, our networks and customer networks. They also access local and international threat intelligence from industry bodies, critical infrastructure forums, security partners and vendors. This enables them to gain a comprehensive view of threats to recommend the most appropriate defence measures.



For more information on Security Services visit telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/security-consulting-capability-statement.pdf

contact your Telstra account executive

telstra.com.au/business-enterprise/solutions/security-services/security-consulting

