RADSENTRY

HACKERS ARE ALWAYS LOOKING FOR WEAKNESSES IN YOUR SYSTEMS. DON'T WAIT FOR THEM TO FIND THEM FIRST.

With RADSENTRY, we provide expert penetration testing and vulnerability scanning to help you identify and fix security gaps before they can be exploited.

RADSENTRY
Penetration & Vulnerability Testing

FIND OUT MORE

STAY AHEAD OF CYBER THREATS!

OPTION 1

RADICAL PEN TEST

Penetration testing (pentesting) is a security assessment that identifies vulnerabilities in your systems by simulating real-world cyberattacks.

So you understand your weaknesses and receive actionable insights in order to mitigate risks.

We focus on compliance (POPIA, CDPA, GDPR, etc.), fast report delivery, and **actionable recommendations.**

Starting from $4,680 /
1 - 50 Assets
Project time: 24hrs

OPTION 2

RAD SENTRY

Vulnerability scanning offers continuous 24/7 security assessments for web applications, identifying vulnerabilities across various environments, including external, internal and cloud systems.

We provide real-time vulnerability detection, actionable reporting, and insights to mitigate risks.

The testing helps organisations to stay compliant (POPIA, CDPA, GDPR, etc.) while preventing false positives and improving overall security posture.

$495 per scan

***NOTE:** In-person testing, geographical limitations, or other special requirements may incur additional fees.

RADICAL CLOUD SOLUTIONS
RUN YOUR BUSINESS ANYTIME, ANYWHERE

sales@radicalcloudsolutions.com

We are **IT Management & Cloud Solutions Specialists** dedicated to getting your business into the cloud and getting your brand noticed.

Core Services: *Cloud Solutions | Digital Marketing | Hosting & Email | App & System Development | Cybersecurity & Backup*

www.radicalcloudsolutions.com

RADICAL PEN TEST

(Active exploitation testing)

Penetration Testing simulates real-world cyberattacks to identify vulnerabilities in systems, applications, and networks before malicious actors can exploit them.

EXTERNAL PENETRATION TESTING

Simulates attacks from outside an organisation's network to identify weaknesses in internet-facing systems.

INTERNAL PENETRATION TESTING

Mimics an insider threat or compromised credentials scenario to assess security gaps within the corporate network.

CLOUD PENETRATION TESTING

Examines cloud environments for misconfigurations, insecure APIs, and identity management weaknesses.

TYPES OF PENETRATION TESTING

- **Web App -** assesses web applications for security flaws such as SQL injection, cross-site scripting (XSS) and authentication vulnerabilities.
- **API -** evaluates application programming interfaces for weak authentication, improper data exposure and injection attacks.
- **Mobile App -** analyses mobile applications for insecure data storage, improper session handling and vulnerabilities in API communications.
- **Hardware -** focuses on embedded devices, assessing physical security, firmware vulnerabilities and data extraction risks.
- **Medical Device -** ensures the security and integrity of healthcare devices by identifying vulnerabilities that could impact patient safety.
- **Wireless -** evaluates wireless networks for weak encryption, rogue access points and unauthorised access risks.
- **Physical -** tests physical security controls, such as access restrictions and surveillance, by simulating unauthorised entry attempts.
- **IoT/OT -** assesses Internet of Things (IoT) and Operational Technology (OT) devices for weak authentication, outdated firmware and network security risks.
- **Industrial Control Systems (ICS) -** analyses critical infrastructure systems to prevent cyber threats targeting SCADA and other industrial processes, applications, or infrastructure requirements.
- **Source Code Review -** involves analysing application source code to identify security vulnerabilities at the code level before deployment.
- **Phishing -** simulates social engineering attacks via email to evaluate an organisation’s resilience against fraudulent messages and credential theft attempts.
- **Vishing -** conducts voice-based social engineering attacks to test an organisation's ability to recognise and respond to fraudulent phone calls.
- **Smishing -** assesses security awareness by simulating SMS-based phishing attacks that trick users into clicking malicious links or sharing sensitive data.
- **Custom -** tailors security assessments to unique business environments, applications, or infrastructure requirements.

COMPLIANCE PENTESTING

(Identifying and assessing weaknesses)

Ensuring compliance with security frameworks and industry regulations is crucial for avoiding penalties, maintaining trust, and securing sensitive data.

Compliance assessments are part of our comprehensive penetration testing services, which aim to identify vulnerabilities and ensure adherence to industry regulations and standards.

FIND OUT MORE

- SOC 2
- HIPAA
- PCI
- NIST CSF
- CIS
- GDPR
- FDA
- ISO 27001
- HITRUST
- CMMC
- Others

RADSENTRY

(Identifying and assessing weaknesses)

RADSentry Vulnerability Testing is a **proactive security assessment** that identifies weaknesses in systems, applications, and networks before attackers can exploit them. Unlike penetration testing, which simulates real-world attacks, vulnerability testing focuses on **systematically scanning** for known security flaws, misconfigurations, and outdated software.

This helps you to prioritise remediation efforts, maintain compliance, and reduce overall cyber risk.

TYPES OF VULNERABILITY TESTING

- **Internal Vulnerability Testing -** scans internal network assets to detect security weaknesses that could be exploited by insider threats or compromised accounts.
- **External Vulnerability Testing -** assesses internet-facing systems for publicly exposed vulnerabilities, misconfigurations and unpatched software that attackers could exploit.
- **AWS Cloud Vulnerability Testing -** evaluates Amazon Web Services environments for security gaps in identity management, storage permissions and misconfigured services.
- **GCP Cloud Vulnerability Testing -** identifies risks within Google Cloud Platform configurations, including IAM roles, storage security, and exposed APIs.
- **Azure Cloud Vulnerability Testing -** analyses Microsoft Azure deployments for improper access controls, insecure networking configurations and compliance risks.
- **Dark Web Monitoring -** scans underground forums, marketplaces, and breached databases for leaked credentials, sensitive data or mentions of the organisation in cybercriminal activities.

RADICAL CLOUD SOLUTIONS
RUN YOUR BUSINESS ANYTIME, ANYWHERE

sales@radicalcloudsolutions.com

www.radicalcloudsolutions.com