



Amidata Cyber Resilience Testing

LEVERAGING AN ATTACKER MINDSET TO SHARPEN YOUR CYBER SECURITY



Don't let a cyber-attack be the first test of your organisation's security systems. With Amidata's Cyber Resilience Testing services, we can identify weaknesses in your IT infrastructure, network, and business applications. We can also simulate real-world attacks to ensure your internal processes and team preparedness are working as expected.

SERVICES



Penetration Testing

Ethical Hacking to identify areas of vulnerability



Phishing Awareness

Deploy phishing attacks to team members to raise awareness



Security Reviews

In-depth security review to ensure best practice across the organisation



Adversary Simulation

A simulation of a real-world attack to ensure your team is prepared



Training

Security awareness training and testing tailored to your business

LEVELS OF PENETRATION TESTING

One essential tool that we use is penetration testing. Penetration testing is when ethical hackers attempt to breach your IT system to evaluate your security.

BLACK BOX – the pen tester receives little to no information about the business's IT infrastructure. This simulates a real-world cyber-attack and involves extensive planning, deployment, testing and reporting.

GREY BOX – the pen tester has some knowledge of the IT infrastructure and may be provided with partial access to the internal network or business applications. They identify and thoroughly test the areas of greatest risk to the business.

WHITE BOX – the pen tester has detailed information about the IT infrastructure and access to the environment. The goal of a white box penetration test is to complete a detailed security review.

TRAIN – TEST – STRENGTHEN WITH PHISHING TRAINING

Hackers continue to exploit people through social engineering, with human error being associated with 90% of cyber breaches. To ensure that cyber security remains top of mind for your team, we offer phishing simulation training to test their response, identify any knowledge gaps, and support and upskill where required.

Our solutions and training include:

- ✔ Ransomware simulator
- ✔ Spear phishing tests
- ✔ Password strength tests
- ✔ Email exposure checks
- ✔ Domain spoof tests

Driving internal awareness is crucial to strengthening your organisation's cyber security posture.

HOW DOES THE PROCESS WORK?

It's easy to get started:

1. We scope out your requirements and security objectives.
2. We gather all necessary information to deliver the test or training.
3. The testing or training with your staff is completed.
4. A written report detailing the work undertaken and weaknesses identified is provided.
5. A Q&A session is scheduled, retesting is performed (if required), and other follow-up tasks are completed, to ensure your business objectives are achieved.

To find out more about our Cyber Resilience Testing, get in touch with us today!





Protect your data, protect your reputation.

Contact Amidata today on **1300 426 432**,

email us at **sales@amidata.tech** or visit **amidata.tech** today.

Amidata is an Australian-based international company offering specialist data protection services. We help you ensure that your valuable data resources are always secure, backed up and performing at their best. We offer advice, solutions and support, along with a utility-based pricing model. This will help you break free of resource constraints and give you the peace of mind of knowing that your data is fully protected.

Amidata Head Office
6/123 Chesterville Rd
Highett, Victoria, 3190

Amidata Sydney
17/122 Arthur Street
North Sydney, NSW, 2060

Amidata UK
24 Wellington Court,
Brighton Marina,
East Sussex,
England, BN2 5WE

Amidata Philippines
Unit 707, 7th Floor,
One Park Drive, 11th Drive
Corner 9th Avenue, BGC,
Taguig, Philippines