NEXT GENERATION PENETRATION TESTING

Mossé Security offers penetration testing services that simulate an attack on your IT network. We use the same techniques and tactics as cyber threats targeting your type of company, thus allowing for targeted allocation of security investments and a vastly improved defense system. Call or email us today to identify and fix your network's vulnerabilities.

OVERVIEW

Mossé Security offers penetration testing services that simulate realistic attackers. We replicate the same techniques, tools, and tactics employed by attackers targeting our specific clients' industry and company profile. As a result, we can offer security defenses tailored to the threats your company is most likely to face, as well as general attacks.

Goals & Capabilities

- **Goal:** Initiate and simulate the strongest attacks against our clients' defenses.
- **Methodology:** Use the same techniques, tactics, tools and procedures as the threat actors targeting your type of organization.
- **Custom Tools:** Program custom malware meant to test the effectiveness of anti-espionage and advanced security endpoint technologies, such as Windows OS zero-days.

MOSSÉ SECURITY

- **Industry Reputation:** Mossé Security has been operating since 2010, providing service and Red Teaming learning programmes to numerous top private sector companies and government entities worldwide.
- **Expertise:** In all, Mossé Security's consultants have manually compromised over 100,000 machines in simulations. We are constantly researching and building new and innovative offensive security capabilities to better test our client's defenses.
- **Exposure:** Mossé Security responds to hundreds of cyber incidents per year. This allows us to see how cyber threat actors are targeting a range of industries and regions of the world. This scope and experience makes us uniquely qualified to design realistic attack scenarios.
- **Trusted Deliverables:** Our services are delivered with the reliability and professionalism expected of a company in our field.

BENEFITS:

Improved ROI:

Running attack scenarios relevant to your organisation ultimately allows you to more effectively allocate security investments and increase your overall cyber security ROI.

Due Diligence:

Realistic attack scenarios allow you to test the effectiveness of your current security programme and identify where defenses may need to be adjusted.

Risk Reduction:

Improving defenses against threat actors relevant to your organisation's profile reduces the likelihood of security breaches and the financial losses they generate.

Mossé Security, 454 Collins Street. Melbourne, 3000, Victoria, Australia
www.mosse-security.com contact@mosse-security.com