Privasec | RED
RED TEAMING & ADVANCED ETHICAL HACKING

Attack Simulation & Detection Testing (Purple Team)
Fact Sheet v2.2

CAN YOU **REALLY** DETECT AN INTRUSION WITHIN YOUR ENVIRONMENT?

More often than not, when it comes to security technologies, organisations are forced to accept the "it works, just trust us" marketing copy without ever being able to validate their effectiveness within their own environment. Post mortems and satistics show that, despite having the technology for it, the marjoty of companies simply can't detect intrusions.

Privasec's Attack Simulation & Detection Testing Service helps organisations rapidly replicate real-world attacks from initial compromise through to data-exfiltration and everything in between.

By working hand in hand with your internal security SMEs to simulate attacks and test your detection capabilities in real time, our security experts will dramaticaly and quickly uplift your secuirty tools' ROI and upskill your security operations.

THIS IS NOT YOUR USUAL TESTING

Offensive security test (Penetration test or Red Team exercice) points out some of your security flaws but leave it up to you to actually fix them. None of these tell you how to improve your tools to detect breaches and detect them faster.

Our Attacks Simulation & Detection focuses on helping you, hands-on, to fine tune your tools, processes and train your SME to actually detect when you are under attack.

OUR SERVICE

Privasec's c takes security assurance well beyond the penetration test to comprehensively replicate all known attacker Tools, Techniques & Procedures (TTP) in a safe and secure manner within the organisation's own environment. Leveraging the MITRE ATT&CK framework, Privasec is able to test over 150 different attacker techniques and behaviours in a controlled environment with zero impact to the organisation.

- Sleep better: KNOW (don't just assume) that you can quickly detect intrusions.
- Fine tunes your secuirty solutions and product to make the most of them.
- Very tangibly measure the effectiveness of your Security Operations Centre.
- Identify and leverage under-used features in your security products.
- Save money by identifying ineffective solutions that can be removed.
- Safely conduct effective periodic incident response 'fire drills' that go beyond compliance-driven table-top simulations.
- Train and upskill existing security team members.
- Provide confidence: Tell the board how long it takes to detect an intruder.

METHODOLOGY

1. We understand your business, security concerns and financial constraints to construct a threat models and build scenarios which are relevant to your organisation and can be mapped out on the MITRE ATT&CK framework.
2. We emulate, without disruption, these scenarios within your environment and simultaneously help your security team understand the technical details behind the attacks as we carry them to see if they can detect it.
3. We uncover the root cause of missed detections and provide tailored technical remediation steps to fine tune your security and detection tools and processes and ensure that each component of an attack can be detected by their own toolset.
4. We map each implemented security technology against the scenarios to look for zombie technologies that serve no purpose and can be decommissioned, thus saving you money.
5. Finaly, we compile a comprehensive report detailing the before and after improvements achieved during the exercise, with personalised sections for the CISO & Executive Teams, Security Operations Team, Security Engineers and Security Analysts

By the time we finish, your environment will already be in a better condition than before we started, with improved staff skill levels and reliable metrics that can be used to measure the ROI of your security investments.

HOW TO PREPARE FOR YOUR SERVICE?

1. Discuss with your security and infrastucture teams to identify which resources would be the most effective candidates to serve on the Purple Team.
2. Nominate and book with Privasec a tentative window period when the Purple Team would have the most bandwidth to take part in the service.
3. Pick a sample set of assets within the environment that most accurately reflect the majority of deployments on which the simulations will be carried out.
4. Configure the necessary user accounts and firewall rules detailed on the pre-engagement checklist provided by Privasec.

Dont worry if you lose track. A Preparation Meeting will be held with you to make sure you have all of the above covered before the start of the Purple Team

Note: This service is designed to create artefacts and alerts on security products and therefore it's essential that the necessary stakeholders and security teams within the organisation are aware of this ahead of time.

GET THE BALL ROLLING

Speak to one of our consultants to discuss your particular use cases and how the Privasec Attack Simulation & Detection Testing Service (Purple Team) can be tailored to your specific requirements.

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia