Trellix

DATA SHEET

Red Teaming Service

Improve the effectiveness of your defensive capability and resilience to sophisticated attacks

Performing red team exercise gain insight into how the environment will fair in a real-world attack scenario. The Trellix Guardians Red Teaming services deliver security testing using industry experts to assess the effectiveness and readiness of security controls, awareness, incident detection, and response capabilities. Attack scenarios can be crafted to emulate specific types of threat actors (enthusiasts, organized groups, and cyber-criminals) employing both traditional and non-traditional techniques to test your resilience against intrusions, data exfiltration, lateral movement and ransomware mitigation, etc.

Exercise Scope

The scope of each engagement is custom fits your organization's needs and goals. Scenarios are defined based on a combination of our guidance, and what concerns you the most about your current security posture, or what you have heard and read from colleagues and in the news.

Type of Attack

Engagements in which only a few individuals know you are "under attack" so you can test actual reactions and responses. These scenarios are highly customized to cover a wide range of either general or specific goals. Some examples:

- EDR Evasion, attackers bypass with legitimate tools (Powershell yet)
- Hybrid Cloud Misconfigurations, over-permissioned roles, misconfig logging etc
- Supply Chain & 3rd Pary Access Exploitations: compromise vendor portals, API success abuse
- Zero-Day Exploit Simulations, exploit outdates drivers, vulnerable software etc

Not Your Father's Pen Test

This exercise differs from a classic penetration test in that the team leverages tools and techniques that are often outside the scope of most pen testing. This includes phishing, simulated malware payloads, physical attacks, social engineering, and more. This more comprehensive engagement is performed over a less restrictive timeline to allow us to fully probe your network and people.

Attack scenarios can be crafted to emulate specific types of threat actors (enthusiasts, organized groups, and cybercriminals). We employ both traditional and non-traditional techniques to test your resilience against intrusions, data exfiltration, fraud, internal attack, corporate espionage.

Our Red Team services can help you:

- Validate the Security Operations Center (SOC) or MDR's ability to detect and respond in real time.
- Identify and protect your most critical assets and vulnerabilities
- Reduce your response time to events and incidents
- Alignment with MITR ATT&ACK, other industry standards and compliance requirements.
- Test success metric: Time to detect, time to respond, and accuracy of threat containment.

Speak with your technology advisor about integrating our services. You can get more information at Guardians@Trellix.com.