RAZORTHORN

Red Teaming

SERVICE BENEFITS

- ✓ Identifies the risk and susceptibility of attack against key business information assets
- ✓ Techniques, tactics and procedures of genuine threat actors are effectively simulated in a risk managed and controlled manner
- ✓ Assesses the organisation's ability to detect, respond and prevent sophisticated and targeted threats
- ✓ Identify methods that could be used to disrupt business continuity
- ✓ Obtain guidance on future security investments

OVERVIEW

Razorthorn's red teaming assessments are performed by our CREST certified ethical hackers. Our ethical hackers are highly trained and experienced red team experts who provide a customised experience to each customer. The assessment is intelligence-led, designed to thoroughly test organisations' cyber resilience plus threat detection and incident response capabilities. The red team assessment will mirror the conditions of a genuine cyber attack by utilising the same tactics, techniques and procedures used by criminal adversaries. Based on the initial results, our red team leverages custom tools, exploits and methodologies to break into the clients environment. Our full range of red team assessments includes threat intelligence, penetration testing, comprehensive open source intelligence (OSINT), digital and physical social engineering, APT simulations and many more.

The multiple methods used ensures that engagements are as realistic as possible and fully challenge the effectiveness of technology, personnel and processes. Typically, engagements are performed on average over a 30 day window, so that the assessment mirrors a 'real' world intrusion as closely as possible.

THE RAZORTHORN APPROACH

Razorthorn's red team assessment is designed based on an organisation's individual objectives, such as cracking credentials of admins, gaining admin access to exchange and/or remove an email from target mailbox, obtaining access to sensitive data, exfiltrating core file system data without being detected, weaponising and installing recon software.

Red teaming typically follows an intelligence-driven, black-box methodology to rigorously test organisations' detection and response capabilities. This approach is likely to include:

- Reconnaissance (OSINT)
- Staging and weaponisation
- Attack delivery
- Exploitation
- Establishing a backdoor (C&C)
- Installing multiple utilities
- Privilege escalation, lateral movement and data exfiltration

Reporting

Razorthorn's comprehensive reports outline any vulnerabilities uncovered, including how they may be confirmed and exploited in future testing. The activities and approaches that took place will be documented as well as observations and remedial recommendations. The report will be written in a way that it can be used to plan and develop future encounters. A debriefing session will also be arranged to walk you through the various breach scenarios emulated in the red team assessment.

The report will consist of two parts:

1. Management Summary - a clear, non-technical and precise overview on the outcome of the assessment.

2. Technical Report - designed for technical staff. The main purpose of the report is to show strengths and weaknesses of the environment, and to advise on how to improve its security.

Razorthorn Security
4 St Johns Road
Tunbridge Wells, TN4 9NP

razorthorn.com
0800 772 0625

office@razorthorn.com