REDSCAN™
CONTINUOUS DETECTION AND RESPONSE

RED TEAM OPERATIONS. CONFIDENCE RESTORED.

ARE YOUR INFORMATION SECURITY INVESTMENTS PERFORMING?

Improve risk management through effective cyber defence and preparedness to deal with a real-world attack.

A Redscan White Paper

EXECUTIVE SUMMARY

The intent of this white paper is to provide an introduction to Red Teaming - a real-world attack simulation that can assess and significantly improve the effectiveness of an entire information security programme. It provides insight to the processes, tools and techniques employed by Red Team Operations and the significant value that organisations can derive from this approach.

One thing is certain when protecting a business from cyber-crime – there is no silver bullet. The evolving nature of the cyber threat landscape means a business could be breached regardless of the security technology, people or processes in place.

Embracing this thinking and continuously challenging the ability to protect, detect and respond to breaches is essential to reduce the risk that a cyber-attack poses to a business's reputational and financial standing.

Red Teaming simulates the real-world attack Tactics, Techniques and Procedures (TTPs) that determined and persistent adversaries employ when targeting a victim. This enables a business to better prepare for the impact of current and future threats. By understanding the weaknesses more clearly and planning for worst-case scenarios, capabilities can be developed to rapidly detect breaches along with the ability to respond to them.

Effective defence is built around understanding the threat.

WHY A RED TEAM ENGAGEMENT SHOULD BE CONSIDERED

The level of concern amongst businesses regarding the risk of cyber-crime is well placed. Preventative security strategies have proven that they are incapable of guaranteeing safety from every attack.

It is essential to acknowledge that a breach has already occurred or that it is only a matter of time before one does happen. While it is important to prevent breaches before they happen, it is even more important to focus on detection and response capabilities. It is simply impossible to eliminate all cyber risks so the ability to rapidly shut down breaches is critical.

146 days

is the median number of days attackers stay within a network before detection

How compromises are being detected

47% Victims discovered the breach internally

53% Victims notified by an external entity

Source: M-Trends 2016

While investment in security is growing, executive teams are increasingly demanding visibility of the effectiveness of their defences to protect their critical business assets. More importantly, if a determined attacker was to target their enterprise, they need to understand how much damage could really be caused.

Effective risk management from an information security perspective is a critical component that protects a company's reputation, and can prevent large-scale financial penalties and customer loss. Similar to army war games, flight simulations or even fire drills - regularly practising for a real-world cyber-attack is a core component of risk management.

The average cost of the worst single security breach:

£1.46m - £3.14m
is the average cost to a large organisation.
Up from £600k - £1.15m a year ago.

£75k - £311k
is the average cost to a small business.
Up from £65k - £115k a year ago.

Source: UK Governments 2015 Information Breaches Survey

Knowing where to start can be difficult. Many organisations do not know what data is accessible to a determined attacker or what harm a breach could do to the organisation's financial standing. They are unsure how effective their security measures are, how skilled the defensive team are, whether they can identify when they are being attacked and if they can respond effectively should a breach occur.

A Red Team engagement is designed to test all of this and more. It is a comprehensive methodology and assessment of the impact such breaches might make and it gauges resilience to sophisticated, planned and sustained cyber-attacks. It also calculates and quantifies the business risks of a breach and in turn justifies defence priorities and investment so organisations can defend themselves more effectively.

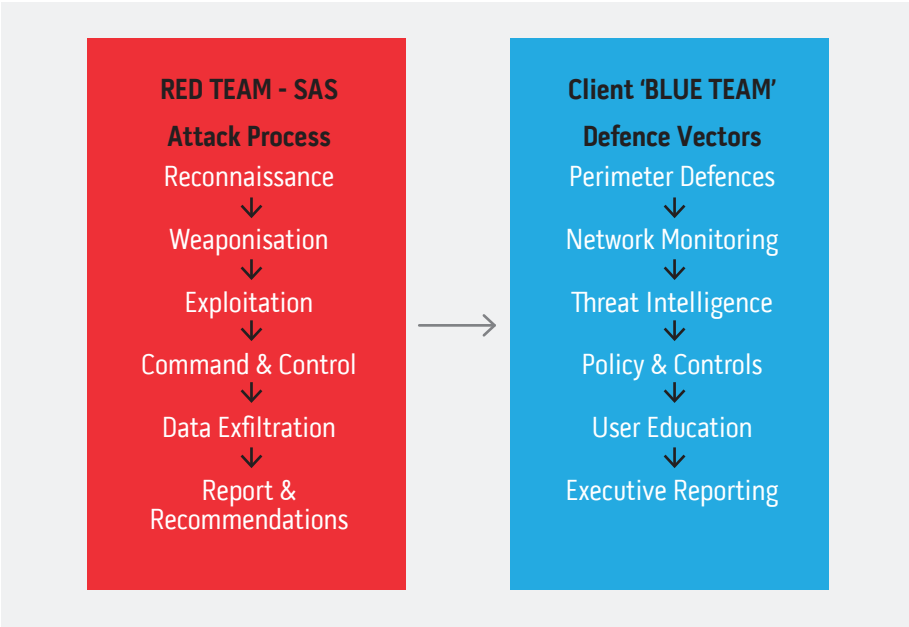
EMPOWER YOUR BLUE TEAM WITH RED TEAMING

Continuously improving defensive controls, detection and response capabilities is essential to manage the risk of cyber-crime. The defenders within an organisation that are responsible for this are frequently referred to as the Blue Team.

The Blue Team's critical functions can include:

- Continuous analysis of the IT environment to identify gaps and weaknesses that could result in a breach
- Proactive monitoring of the network to detect footprint of an attack
- Conducting triage on security alerts to establish if further investigation is required
- Gathering context and evidence to scope the breach
- Establishing a suitable incident response to contain or eliminate the breach
- Implementing the incident response plan to recover from the breach

To remain effective, the Blue Team must understand the Tactics, Techniques and Procedures that real-world cyber criminals employ. This enables them to ensure their detection and response capabilities are aligned to deal with these known approaches.



Engaging with a Red Team tests the Blue Team's ability to detect and respond to real-world attacks, measuring the readiness and impact of existing breach response capabilities. By increasing awareness of the threat landscape and exposure to the actual conditions when under attack, Red Teaming is an essential tool to enhance preparedness for managing breaches.

The process also highlights who within the organisation needs to respond to such attacks publicly. This may include the PR, investor relations, marketing and C-level executives.

THE RED TEAM ENGAGEMENT PROCESS

The purpose of a Red Team engagement is to simulate the approach a real-world attacker would adopt when targeting a business. While keeping this process as realistic as possible, it is also essential to ensure operational risk remains within the boundaries acceptable to the business.

To achieve this, key stakeholders should be involved in the planning and approval stages of the engagement. It is advisable that the number of people involved is kept to a minimum to ensure that the defensive team is not forewarned and therefore the integrity of the test is not compromised.

Key considerations for most organisations include:

- **Board/Executive**
  Red Team engagements can target many parts of the business and therefore Director, C-level or Board-level buy-in/approval is essential

- **Risk Management**
  Ensuring risk and audit management functions have oversight and governance over the activities of the Red Team will keep the engagement within the approved parameters

- **Legal, Compliance and HR**
  Input from legal and compliance is recommended during the planning and approval of a Red Team engagement. This removes the risk of non-compliance and liability for the business. As the targeting of specific individuals could form part of the engagement, notifying HR should also be considered.

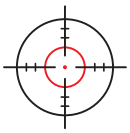
THE RED TEAM ATTACK METHOD

Red Team Operations follow a tried and tested methodology to attack the target, however each engagement is extensively tailored to the specific organisation, its sector, current security investments and business objectives.

A typical set of activities are described below. This list is by no means exhaustive.

Reconnaissance:

In-depth research and analysis to identify valuable information that can be used to exploit weaknesses within the target's systems, processes and people.



Weaponisation:

An attacker then develops malicious code to target the most vulnerable systems appropriately.

Delivery:

Malicious code is typically delivered by emailing a victim, with either an attack package or a link to a malicious website. Alternatively, Internet accessible services can be targeted on a number of levels from simple brute force attacks, to exploiting vulnerabilities.

Installation:

Malicious software can be installed on the target asset allowing remote access or visibility of information from the target.

Command and Control:

Multiple command channels are created to ensure access is maintained with the target.

Privilege Escalation:

Once a system is compromised, the attacker will attempt to increase their level of access on the target host.

Lateral Movement:

Attempts are then made to gain access to other systems and resources on adjacent network segments to find information and consolidate the compromise.

Data Exfiltration:

Once data of value has been identified, the Red Team will attempt to extract it from the target network without being detected.

RED TEAM ENGAGEMENT V PENETRATION TESTING

Traditional penetration testing uses tools to attempt to identify and exploit weaknesses, but does not use the full knowledge and capabilities a determined attacker would employ. It also does not test preparedness, detection and incident response capabilities. Another key feature of Red Teaming is that it is an ongoing engagement and does not stop once the test is complete.

	Red Team Engagement	Penetration Testing
Purpose	Real world simulated cyber-attack to determine performance of existing business defences, policies and user sophistication	Periodic technical network security testing for IT compliance, regulation and auditing requirements
Tools	Continuous research and development of attack approaches to exploit unknown vulnerabilities	Use of standard tools available; engagement required to move to next stage of testing
Evasion	A key objective is to avoid detection - when the intrusion detection processes are invoked the game changes	Intention is not to evade detection, but to identify technical vulnerabilities
Persistence	Stay resident for as long as possible to evaluate sophistication of detection and ability to remove breach	Stops when the environment has been compromised
Post-breach Activity	Use the breach to find and exfiltrate data to launch further attacks	Testing ends if access is achieved
Scope	Attempt to compromise everywhere, changing tactics as required	Test assumed environment, not testing outside of remit
Physical Attacks	Test physical security processes, access to network and sensitive information	Not in scope
Social Engineering	Target staff to obtain access	Not in scope
Reporting	Detailed evidence on when and how to breach the environment. How long it took to be detected, what assets were compromised and whether detection and response were successful. Remediation steps to improve defensive capabilities and attitude to security across the organisation	Details of tests conducted and if passed or failed

APPLYING THE LESSONS LEARNED

At the completion of the Red Team engagement, a formal process of feedback to all stakeholders is imperative to ensure that the organisation acts quickly and meaningfully on the recommendations provided.

The Red Team feedback will provide a clear and concise, prioritised action plan for the commissioning firm. This will take the form of specific recommendations addressing:

- Key findings the executive team should be aware of
- Technical team requirements
- Risk analysis of results
- Immediate and strategic improvements

In addition to the above, technical security advice is also provided. This can include upgrades that can be made to individual components of the perimeter defences, improvements to data storage and encryption policies, through to more long-term, wide-ranging recommendations regarding staff and senior management education programmes.

Each of the key stakeholders in the business, such as HR for education, IT for network infrastructure, Operations for data ownership and Executive Management for regulatory compliance should follow-up and implement the remedial actions recommended from the engagement.

It is generally accepted that the Chief Information Security Officer (CISO) is the responsible executive for the construction and delivery of the action plan, but it cannot be overstated that the security of an organisation's information policy now spans the whole of the executive and senior management teams, and the effectiveness of this policy resides in the ability of an organisation to ensure that every single employee clearly understands the threats that exist and the defensive actions that all must take to keep the company secure.

SUMMARY

Now more than ever, businesses and their executives need to ensure they are taking appropriate measures to protect their organisation's customers' and shareholders' interests.

Red Teaming is just one available option, however it is one of the most powerful and effective initiatives available to companies of any size. A well-conceived and executed Red Team engagement will highlight deficiencies in the key areas of people, process and technology, uncovering inherent weaknesses across the organisation, not just from a technical standpoint, but also from a risk control perspective.

Organisations will reap significant benefit in the form of a prioritised list of remedial actions that will strengthen an organisation's defences.

By constantly reviewing and reporting the organisation's attitude to security, its ability to resist the targeted attacks which are becoming the norm in today's business environment, will be significantly increased.

Today's businesses need detailed insight into their complete security posture that only a Red Team engagement can provide.

ABOUT REDSCAN

Redscan Cyber Security Ltd, is a Managed Security Services Provider (MSSP) that enables businesses to effectively manage their information security risks. Using a combination of security expertise, technology, processes and threat intelligence, the company's rapid detection and monitoring services help defend against today's sophisticated and targeted threats.

Designed for businesses of every size, Redscan's services include ThreatDetect™, its affordable Security Operations Centre as-a-service platform, CREST approved Penetration Testing and Red Team Operations.

Redscan's management team bring over 50 years of combined experience in cyber security across a range of industries, including banking, accounting, legal services, construction, retail and leisure. Enabling clients to adhere to PCI and ISO, GPG13 and Cyber Essentials Plus, Redscan is proud of the certifications the team holds, such as Crest, CISSP, CEH, CISM, OSCE, CISA, OSCP and OSWP.

STAY CONNECTED

w www.redscan.com

e info@redscan.com

t 0800 107 6098

Connect with us

Follow us