SALUS

CYBER

RED TEAMING SERVICES

WWW.SALUSCYBER.COM

RED TEAMING SERVICES

'We cannot solve our problems with the same thinking we used when we created them.'
Albert Einstein

Red Teaming is the process of using Tactics, Techniques, and Procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of the people, processes, and technology used to defend an environment. Red teaming has become more widely used in the UK over the last ten years. It has become recognised as a major aid to decision-making in the support functions of Defence and as a valuable tool for businesses of all shapes and sizes.

Red teaming is NOT a hunt for vulnerabilities, flaws, bugs, etc. The goal is to understand security operations (people, processes, and technology). The result of a red team engagement may identify vulnerabilities, but more importantly, red teaming provides an understanding of blue's capability to impact a threat's ability to operate.

The technique is widely used in Defence (Red Teaming Handbook) more broadly than just the cyber domain, but key themes remain relevant. Such as:

- **Uncover hidden biases.**
- **Challenge assumptions and beliefs in the quality of your processes.**
- **Identify flaws in logic and systems services/ processes.**
- **Widen scope of information searches.**
- **Identify different options and alternatives; and**
- **Stress-test a plan (e.g., incident response).**

Salus Cyber applies critical thinking as part of its red team engagements leading to robust analysis of facts to form a sound judgement. It involves the rational, unbiased analysis of factual evidence gathered through our red team methodology. Critical thinking is designed to overcome the natural biases that human beings bring to information processing, decision-making, systems management, and problem solving.

There are several advantages associated with using external red teams. They are:

- **Not invested in the plan/policies and agnostic about its success or failure.**
- **Able to be truly objective in analysis and not prejudiced by existing biases.**
- **Not involved in the planning and decision-making and so can bring fresh perspectives to established problems; and**
- **Made up of members with expertise or knowledge that does not exist in the original planning team.**

INTELLIGENCE LED TESTING

Cyber threats are both dynamic in nature and often evolving outside of a companies sphere of control. When scoping a Red Team assessment, we work with clients to identify key areas of concern and apply relevant elements of the MITRE ATT&CK framework to the exercise design.

Simulation of how a cyber adversary may approach targeting of a company involves a detailed understanding of Tools, Techniques and Procedures a range of different groups apply to hostile action against a company or organisation. We ensure that all our activities map to the Cyber Kill Chain™ to ensure your organisation can identify which stages are not being captured or prevented by your blue teams.

RED TEAMING SERVICES

Purple Teaming

RED VS BLUE - WHAT'S THE DIFFERENCE?

A red team is ordinarily a group of offensive security professionals tasked with using real-life adversarial techniques to help organisations identify and address vulnerabilities across infrastructure, systems and applications, and weaknesses in processes and human behaviour.

In contrast, a blue team is a group of analysts and engineers responsible for defending organisations from cyber-attacks through threat prevention, deception, detection and response.

RED VS BLUE - WHAT'S THE DIFFERENCE?

The stark reality for many organisations, is that red and blue teams are often entirely separate and disconnected entities. The Purple team concept addresses this disconnect and is a natural evolution for organisations looking to leverage more advanced security testing.

By creating a scenario where the two teams work together (Purple Team), organisations will be able to benefit from much more tailored, real-world assurance. The outcome is that the blue team can effectively identify their detection and response capabilities to be much more closely aligned with real-world threats.

Some organisations perform purple teaming as one-off focused engagements. Security goals, timelines, and key deliverables are clearly defined. There is a formal process for evaluating lessons learned over an operation. This includes recognising offensive and defensive shortcomings and outlining future training and technical requirements.

THE BENEFITS OF PURPLE TEAMING:

- Enhance security knowledge.
- Observing and participating in attacks gives the blue team a better understanding of how attackers operate, enabling them to employ technologies to thwart actual attackers more effectively.
- Boost performance without increasing the budget.
- Combining defence and offence through purple team exercises allows organisations to improve security monitoring function faster and at less cost.
- An alternative approach within the security industry is to view purple teaming as a conceptual framework. This outcome is usually that a collaborative culture forms that promote continuous cyber security improvement.

Purple teaming gives your internal security team a critical understanding of gaps in their security posture and helps identify capability enhancement areas.

RED TEAMING SERVICES

Phishing Simulation

Phishing is still one of the highest successful attack vectors for malicious threat actors. Therefore, understanding how your organisation stands up to a phishing attack is essential in making decisions related to cyber security. Salus Cyber can perform one of or a combination of the following scenarios:

LINK CLICKING

This phase is primarily to test the awareness of your users, helpful in conjunction with analysis of the tickets that are received – to verify education and users' response to generic phishing attempts.

PASSWORD GRABBING

A custom website will be built to attract users and trick them into typing their passwords or any sensitive information. In addition, the website will typically replicate or spoof an existing company to maximise the engagement rate. This is similar to link clicking but with more real-world impact. This can be especially useful when going through other testing scenarios to ascertain the likelihood or impact.

MALICIOUS DOCUMENT

Malicious documents will be attached to phishing emails to trick users into running them. This will include executables, executables masquerading as legitimate files, and macro-enabled documents. Note that malicious documents used by Salus Cyber will be benign. However, it is a standard method for APTs and other attackers to gain access to an organisation.

SPEAR-PHISHING

Spear-phishing is a phishing program whereby only specific individuals are targeted. This allows for more personal, persuasive, and realistic messages and is usually sent to high-ranking individuals in the company due to their access or influence. An additional element of open-source intelligence (OSINT) will be conducted to perform this phase, increasing the time taken.

All of these can be used as part of a regular phishing service if required.

RED TEAMING SERVICES

Ransomware Simulation Testing

Ransomware is still one of the biggest threats facing an organisation, both from external attacks or supply chain attacks.

Salus Cyber consultants will not simply run malware on your system and tell you that "you're vulnerable", this is cutting-edge custom payloads and attack vectors written as threat actors without the malice element.

Some of our ransomware tests can emulate specific ATP TTP, and as part of designing your exercise, we would ask you to choose your features. Plug and play modular design allows custom attacks based on your threat intelligence, key risks, or gut feelings.

SOC Maturity Assessment

A SOC maturity assessment is similar to purple teaming but without as much collaboration by the red and blue teams.

The approach for this type of test is more audit-like into the effectiveness of the detection capabilities in line with the MITRE ATT&CK framework.

Each of the tests is performed with a pass/fail criteria. Any gaps in capability are highlighted for the blue team to investigate further with guidance for improvements on the fine-tune of tooling and capability gaps.

RED TEAMING SERVICES

Covert Entry Disruption (Black Team) Exercise

Exercising an organisation's physical security and personnel security policies and processes is essential for getting a complete picture of any security vulnerabilities you face.

Black teaming is an approach to security testing that aims to identify the gaps in these safety measures. It also strives to bridge the gaps and ensure that these safeguards work effectively.

A black teaming exercise involves assessing security vulnerabilities from a hacker's perspective. It empowers the organisations to imbibe their weaknesses and strengthen their safety mechanisms. Like other security testing exercises such as red teaming, it helps organisations fix their vulnerabilities before an attacker exploits them.

However, covert monitoring of any form needs careful planning and a detailed scope which does not put the business or the testing organisation in conflict with the guide to Employment Practices code issued by the Information Commissioners Office (ICO).

The ICO guide for employers makes the position clear. It is critical that planning does not create a scenario where a security exercise gets confused for "The covert monitoring of workers" which can rarely be justified.

Black Team Exercises, therefore, need to be authorised by the highest level in your business.

Salus Cyber can work with you to create a legally safe and appropriate approach to this type of exercise.

SALUS

CYBER

RED TEAMING SERVICES

WWW.SALUSCYBER.COM
01242 374087

CYBER ESSENTIALS CERTIFIED PLUS

THE CYBER SCHEME

Assured Service Provider
in association with
National Cyber Security Centre

CHECK
IT Health Check Service

Crown Commercial Service
Supplier

ISOQAR REGISTERED
UKAS MANAGEMENT SYSTEMS
0026
Certificate Number 18737
ISO 9001