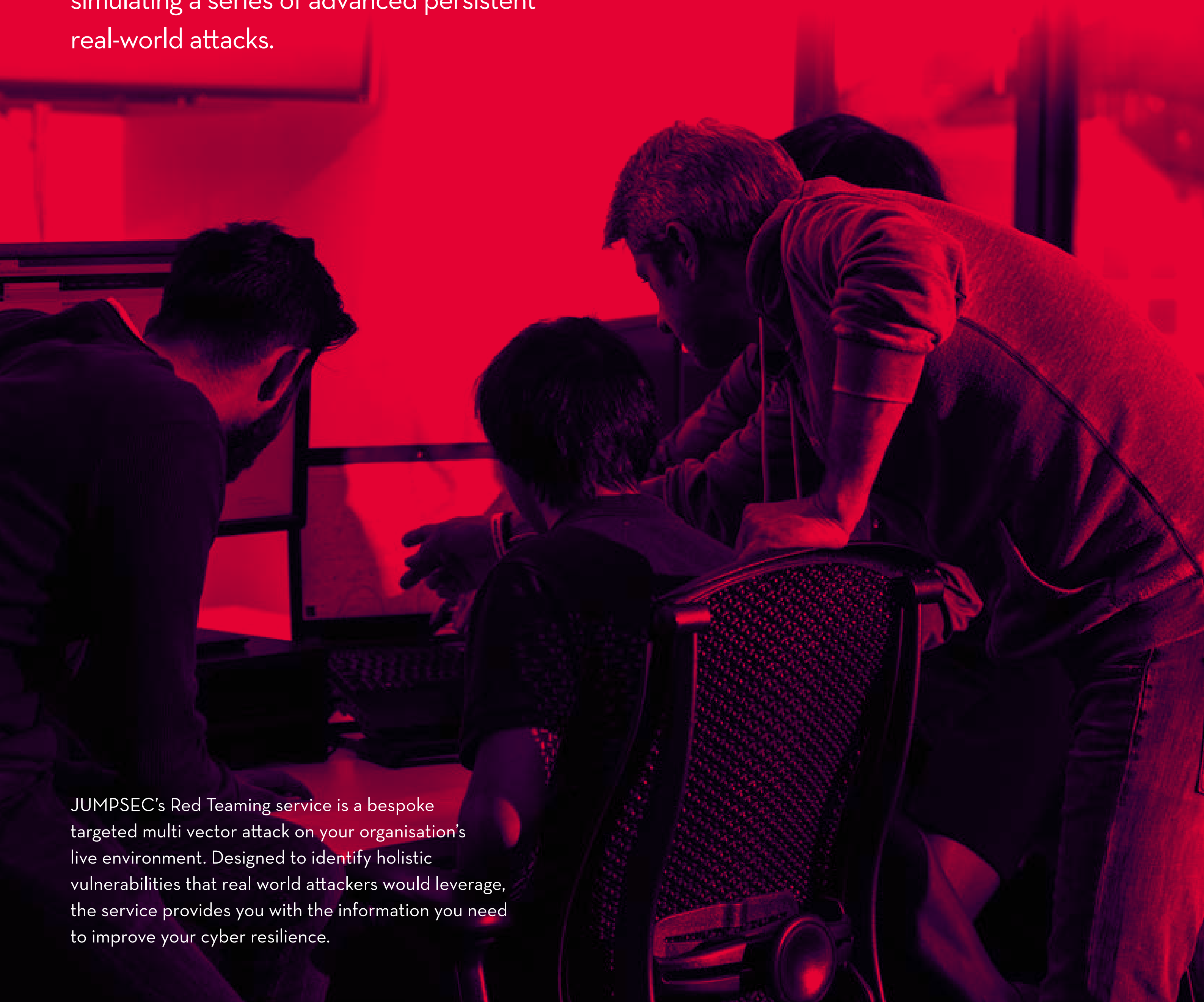
JUMPSEC

Assure | Advise | Respond

RED TEAMING (ADVANCED SIMULATED ATTACK)

Helping you assess the strength of your organisation's security posture by simulating a series of advanced persistent real-world attacks.



JUMPSEC's Red Teaming service is a bespoke targeted multi vector attack on your organisation's live environment. Designed to identify holistic vulnerabilities that real world attackers would leverage, the service provides you with the information you need to improve your cyber resilience.

Who needs Red Teaming?

JUMPSEC Red Teaming (Advanced Simulated Attack) is designed for organisations who desire a high degree of security maturity.

A Red Teaming exercise provides a comprehensive check of your organisation's overall security posture without limitations such as scope, time or omissions due to the operational impact of live testing.

It's suitable for organisations looking to quantify their ability to defend against systematic, persistent and organised threat actors. We identify weaknesses in your people, processes and technology and craft them into specific attack scenarios.

We look broadly across your whole estate and then dive deep on any weakness or exploitable target – in just the same way a real-world attacker would.

What are the benefits of Red Teaming?

- **Discovery of vulnerable target systems and critical assets**
  We perform intelligence gathering to identify the potential targets an attacker would seek to exploit as well as any security vulnerabilities in your, technology, processes and people. Our OSINT process will identify what is exposed, what is at risk and what could be used by threat actors as leverage or a likely starting point for an attack. We will document and present back to you what information is available publicly that might be used by threat actors.

- **Comprehensive and persistent testing without limitation to give you peace of mind that your defences are working**
  Red Teaming does not have classic scope limitations. It is a goal-based approach that allows JUMPSEC to simulate targeted and persistent threats. This holistic approach discovers security weaknesses, vulnerabilities and areas of compromise that are only evident from the perspective of a persistent threat actor viewing an entire organisation with the determination to breach security for gain over time.

- **Confidence that the most up to date tools and techniques are deployed to test your security**
  Potential attackers are sophisticated and use a variety of techniques to infiltrate and gain access to your valuable data or assets. JUMPSEC tactics, techniques, and procedures (TTPs) are continually developed to emulate sophisticated threat actors. We utilise the latest tools and technology and will often write bespoke malware specifically targeting your systems, processes and vulnerabilities, just like a hacker would.
  Our team will perform real-world attacks based on accurate reconnaissance and actionable intelligence giving you confidence that your defences are put to a true test with multiple attack vectors covered in a safe and controlled manner.

- **Strengthen your security posture and fine tune your security professionals**
  Red Teaming exercises provide you with recommendations on how to remediate any vulnerabilities identified and give you knowledge of where to harden and tune your defensive systems for optimum security. Should our Red Team exercise be pitched against your security team (Blue Team) we can reveal how they work under pressure and test your incident response processes. We can assist with education and help them develop capabilities to frustrate similar attacks in the future. Red Teaming evaluates your ability to identity, detect, and respond to targeted and sophisticated attacks and allows you to quantify your defensive capabilities.

What makes up Red Teaming?

In house CREST STAR certified expert team

Performed by our in-house expert CREST Certified ethical hackers who understand the hacker mindset, objectives, strategies and techniques that are deployed in multi vector attacks. The team deliver real-world attacks while following strict codes of professional ethics, structured approaches and proven methodologies to assess your security posture holistically.

Intelligence gathering

We commence the exercise from a 'black box perspective'. i.e. with little or no information other than what is available publicly - much like threat actors would in a real-world attack. The team will conduct reconnaissance activities known as OSINT (Open Source Intelligence Gathering) designed to identify and collect as much information as possible about your organisation—all with the goal of conducting targeted multi-vector attacks.

Goal oriented real-world multi vector attacks

Utilising the intelligence gathered, our Red Team will design attacks mapped to your threat profile – targeting systems, data or information that threat actors would look to exploit. From customer records to credit card information, emails to board minutes, or critical operational systems – anything that an attacker would leverage to gain advantage and cause your organisation financial, operational or reputational damage. Our risk managed approach ensures we maintain contact with your organisation during exploitation to perform attacks catered to your risk appetite. Attack paths will be bespoke and comprise of the latest tools and techniques combined with social engineering.

Cyber resilience stress testing

We will execute carefully designed and planned attacks, to test your defensive (Blue Team) capabilities and actual detection and response to a persistent attack as well as your organisations overall security awareness.

Comprehensive reporting with evidential support

We will document all attack scenarios that have been completed and provide you with a comprehensive report, with evidential support, accurate timelines and practical recommendations to help your organisation improve its security posture.

Accredited standards

JUMPSEC is CREST approved and our expert team are CREST STAR Certified. Our Penetration Testing methodologies are extensive and drawn from CREST, OSSTMM (Open Source Security Testing Methodology Manual), and OWASP (Open Web Application Security Project) and designed to offer our clients maximum assurance whilst ensuring that testing does not disturb your ongoing operations.

Continuous Expert Support

We love what we do, and we are just a phone call away. When you take our Penetration Testing services you receive continuous expert support backed by rigorous processes and procedures. You can contact us at any time for any security related questions.

Why JUMPSEC Red Teaming?

JUMPSEC have been helping organisations overcome the continuously evolving cyber threat landscape since 2012. We know the cyber security landscape like no other because of our combined experience, passion for knowledge, and research driven approach. We are proud to have created a continuously improving cycle of people, technology and threat intelligence to help us stay at the forefront of cyber security. Our Red Teaming service benefits from this continuous improvement and will help you defend against real world cyber-attacks.

To learn more about JUMPSEC's services please feel free to get in touch

Give us a call
call. 0333 939 8080
www.jumpsec.com

Send us a message
email. hello@jumpsec.com