Means Business

Datasheet

Our Red Teaming services

Our red team specialists can identify lapses in the behaviour of your people, gaps in your procedures and determine the maturity level of your defence. We'll pinpoint any weaknesses before anyone with malicious intent can exploit them.

An approach without boundaries.

The security of your business is an ongoing challenge which needs your attention on a continuous basis. You've got solid security policies in place and an internal security team that regularly defends against malicious intent. But is that enough? Attackers are skilled at finding and taking advantage of your weakest points.

Our red teaming service looks at how prepared your organisation is to withstand and defend against an attack once you have been targeted by malicious individuals or organisations.

Unlike an ordinary penetration test, a red teaming exercise is carried out against a blank canvas with little knowledge of what to expect. We'll take a comprehensive view of the full spectrum of your policies, processes and defences. All boundaries regarding the attack surface and scope are removed, which also applies to the duration of the project.

Whilst most penetration tests generally last between 3-20 days, a red teaming project may run for several months. It aims to achieve the goals through a variety of attack scenarios. After an initial reconnaissance phase we'll attempt to obtain a foothold in your organisation, be that physically or via electronic means, followed by our red team infiltrating the network in the search for your crown jewels.

Are you protected?

Your team of security professionals protect your business on a daily basis using the right technical solutions. You've got security processes in place which means that you're in control. The networks, applications and the cloud services you use are frequently tested by ethical hackers. You've carefully vetted all your suppliers and your people are trained. Everything seems fine, but just to be sure you should test your defences!

Take your red teaming assessment to the next level: emulating nation state attacks. We'd like to demonstrate our capability and show you what we can do for you.

Purple teaming

When our red team effort is coordinated with your security team ("blue team") to defend against the simulated attacks, the project is then called a "purple teaming" exercise. This joint approach aims to identify possible issues in your current technology and procedures, or a shortage of skilled individuals, in order to prevent an attack on your organisation. We'll work closely with you during the project, sharing feedback, transferring knowledge or training your team as the attacks happen. These simulated attacks and "training on the job" for your employees is the most efficient way to keep pace with the changing threat landscape.

Our Approach

We've developed a standard way of evaluating the security posture of organisations. It's based on our own checklist, the current thinking from tech forums and publications, and our many years of experience.

While we're performing the assessment, we'll report any critical or high risk issues the moment we spot them. And when we're finished, you'll get a formal report including:

• A full explanation of what we tested and how.

• A list of all the vulnerabilities we identified, ranked by their risk rating (based on Common Vulnerability Scoring System if applicable)

• Your next steps: how to mitigate each vulnerability as well as follow up on the recommendations.

Rethink your risk

Running a business is about knowing which risks to take and when to take them. Firstly, you need to understand what you have that might be of interest to a nation state attacker. You will most likely have some of these on your list:

- intellectual property (inventions, designs or company secrets)
- personally identifiable information (PII) concerning customers and employees
- other data (stock sensitive, financial, sales).

Once you have identified what matters most to you, you can start thinking about how to protect it. Should you invest more in employee awareness training, improve your security monitoring or should you minimise your attack surface by completely isolating certain network segments from the internet?

How we might test your defences

Both our red and purple teaming assessment may contain several different attack scenarios, each helping to understand to which level your organisation is able to resist a physical or cyber security attack. Some of the following scenarios may be included:

- We'll look at the security controls and monitoring technologies employed at your physical sites as well as across your organisation's internet footprint.
- A variety of techniques will then be applied to circumvent physical and associated electronic access controls, attempting to gain access to your key buildings and the network infrastructure housed within them.
- We'll use social engineering tactics on your employees, via the telephone, email, or in person. Such an attack may be conducted at arm's length, or from within your network or physical perimeter.
- We'll attack your computing infrastructure, both from the internet and as an insider, moving laterally and building up our level of access until we have far-reaching administrative control within your company.
- We'll offer insight into the capabilities required of an attacker to successfully breach your perimeter. Can a "lone wolf" hacktivist reach your crown jewels, or do we need to call on our nation-state level skills to successfully compromise your business?

Ultimately, our aim will be to offer a holistic assessment of your physical, human, and electronic security posture – not in isolation, but as a layered security model.

How else can we help?

Alongside red teaming, we can advise on how to mitigate your vulnerabilities – particularly if that calls for you to redesign your network infrastructure, call centre architecture, install new technology or change your incident response capability. Talk to us about our consulting or managed services.

Why us?

We're experienced

In fact, we're one of the biggest security and business continuity practices in the world. We've got 3,600 security professionals working for us across the globe. And when it comes to ethical hacking, our team has more than 30 years' experience.

We operate across many industries, including industries that are significantly more advanced in dealing with cyber threats. This means we are ideally placed to bring expertise and know-how acquired with customers on the leading-edge of cyber security.

We're recommended

We're recognised as a Leader in ISG Provider Lens™ – Cyber Security – Solutions and Services 2024 in the UK. The report highlighted our strengths in managed security services, strategic security services, and technical security services in the UK.

BT has been named a Leader for the 20th consecutive year* in the 2024 in the Gartner Magic Quadrant™ for Global WAN Services based on its "Ability to Execute and Completeness of Vision".

*Magic Quadrant for Global WAN Services was previously named Magic Quadrant for Network Services, Global

We're qualified and security cleared

Our consultants hold industry certifications like OSCP, OSCE, OSWE, OSWP and CRTP.

Where appropriate, our consultants possess national security clearance for delivery to government customers.

We're accredited for ISO27001:2013 covering our security testing services to both internal and external customers. Next to our ISO27001 accreditation we're also accredited for global consulting by Lloyd's Register Quality Assurance for the ISO9001 quality management system. We've held that since 2003 – proof of our long-term commitment to improving our services.

We have first-hand experience

As a large organisation, operating in around 180 countries, we know all about keeping our intellectual property, customers, people and premises safe.

We work hard to protect our networks, systems and applications – our ethical hackers and red team specialists test everything. Additionally, we work closely together with our blue team to test the effectiveness of our defences by carrying out multi-layered simulated attacks against both our physical and cyber security infrastructure.

This unrivalled experience, gained over many years of full spectrum testing of our policies, processes and defences, keeps our brand safe.

Find out more about ethical hacking

Learn more

JN: 1611673531 | November 2024.