Means Business

Datasheet

Our OSINT & SOCMINT services

Our team of ethical hackers will deliver an independent open-sourced discovery on your publicly-facing estate so you can be confident you're not unwittingly exposing critical information.

Safeguarding your network infrastructure with ethical hacking can improve business profitability.

Your organisation faces complex challenges every day. Keeping focused on business objectives whenever and wherever you are across the globe requires a secure network infrastructure to support you.

Exciting new ways of working and new channels to market mean the company board are delighted, but will security be an enabler to this strategy? How vulnerable is your business today and into the future?

Is it a simple process to find weak spots in your business critical systems, procedures, policies and behavior of your employees? Or does the news of a new piece of regulation or legislation mean significant work which will cost time and money and potentially leave new security weaknesses?

So what is required?

It's about ensuring proactive protection of your brand, reputation and valuable electronic assets around the clock worldwide.
Secondly, it's about having a clear view of your overall risk profile from any potential financial impact, or as loss of customer trust which is very hard to recover.

At an operational level, it's also about understanding the countermeasures and actions that you may need to take if your information or services were compromised, as well as about having full visibility of your own security estate, your service providers and the services they are managing.

All of these combine to better support your organisation's business strategy.

Our approach

We've developed a standard way of evaluating employee behaviour on the Internet. We've created our own checklists, based on the latest Open Source Intelligence (OSINT) techniques, current thinking from tech forums and publications and our own years of experience.

Discovery is the first stage in any assessment

The Internet has become a necessary tool for everyone and it's not surprising that people make innocent mistakes. It's quite easy to leave sensitive or classified information exposed. The reason may be because IT services are too complicated for the majority of users or because users don't see any risk in publishing this information.

We can help you to deliver robust security in this area. The rapid digitisation of your business coupled with agile development and deployment models means new information about your organisation is potentially being exposed on a weekly basis.

With the results of our OSINT assessment we can discuss and agree next steps. This could be kicking-off a security awareness program, considering further more active testing of your estate or just rethinking whether certain technical solutions you have in place are supporting your information security strategy. Our independent assessment and agile reporting style helps you to further strengthen your security.

How can we help you?

Below a few examples of what could be included in your assessment:

- We establish what you think you have. A classic model of intelligence begins with planning and direction, so initially, we agree what kinds of information could be of interest to an attacker.
- Guided by that, we collect intelligence from the perspective of a potential attacker from openly available sources. This can be corporate sources (such as public corporate data, and the organisational internet footprint), social (such as openly-available material about persons of interest), or a mixture of the two.
- Then, we correlate those intelligence sources, processing and analysing the data, collecting additional information as needed, until we develop a profile of the target.
- When this analysis is completed, we write up the findings and vulnerabilities to give to you, align these with the initial brief, and give recommendations on how best to reduce your exposure. Individual identified vulnerabilities may vary, but typically show how corporate and individual information can be gathered and correlated by an attacker, invisibly and from a distance, discovering far more about your business than you might have imagined.

The Next Steps:

Once we've have completed all phases of the discovery assessment, our ethical hackers can take the next step. This is called a Red Team assessment. They start using the information gathered to gain further access to:

- Resources available on your network and/or cloud services (like O365, AWS, Kamatera, Adobe, Google Cloud Platform, Salesforce etc.)
- Company buildings by performing social engineering attacks, picking of mechanical lock systems or bypassing electronic access controls.

During this assessment our hackers will hunt for more sensitive and/or classified information. Why? To show the consequences to your business when sensitive data is unintentionally published on the internet.

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, OSWE 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

Offices worldwide

JN: 1611673531 | November 2024.