bsi.

Enhancing your penetration testing regime

An insights paper

Executive summary

This whitepaper explores how utilizing red-team or objective-oriented penetration testing services can provide increased insight into the security posture of an organization, its susceptibility to varying degrees of attack and its ability to detect and respond to such an attack.

Due to the rising number of high-profile cybersecurity incidents and compromises, the need to more accurately simulate the Tools, Tactics and Procedures (TTPs) of the real-world adversary has become more important. Red teaming engagements are not a new concept, but have gained more prominence in recent years with the advent of CBEST (Bank of England), TIBER (De Nederlandsche Bank), iCAST (Hong Kong Monetary Authority) and CREST STAR (Simulated Target Attack & Response) schemes, the latter of which BSI is a member. All these schemes are similar in nature and bring a formalized framework to offensive testing techniques which have been around for a long time.

By utilizing this type of enhanced penetration testing, an organization can gain a greater understanding and appreciation of the likelihood of a successful compromise, the types of adversary they may face, and how well they are equipped to respond to and deal with such an incident.

This paper will explore what we currently know about penetration testing and two ways of enhancing penetration testing efforts and results; objective-oriented assessments and red teaming assessments.

Penetration testing

A typical penetration test follows a pre-defined and approved methodology during the execution of the assessment, with the end result being a report which highlights all of the security issues and vulnerabilities identified on specific assets.

In order to identify the vulnerabilities present on those assets, a penetration test includes performing offensive testing techniques against a pre-defined scope of assets. Assets can take on many forms; including web applications, externally facing networks and hosts, internal networks, network devices, cloud infrastructure, mobile applications and APIs, to name but a few.

Penetration testing has formed, and continues to form, a large element of cybersecurity efforts for many organizations, primarily due to the value that the results provide and that it gives the organization stable and measurable output relating to the security posture of the in-scope assets at a specific point in time.

However, traditional penetration testing has its limitations. For instance, a client could opt to remove certain assets from scope with specific hosts, areas of web or mobile applications or physical buildings, to name but a few. The result of such scope restrictions is that testing is done in isolation; the scope may have in-depth coverage of each asset, but could represent a lack of breadth across the organization as a whole.

Objective-oriented penetration testing

An organization can counter those limitations and obtain increased assurance over their security posture by introducing objective-oriented penetration testing alongside their usual testing regime in order to enhance their penetration testing output.

A real-world adversary who is targeting an organization is not concerned with any scope or time restrictions. Adversaries are interested in only one thing; compromising an organization they have targeted, via any means possible.

Objectives

In order to replicate the real-world attacker, the focus of the penetration test can be reviewed; rather than assessing the pre-defined assets with a single specific type of assessment. A more realistic penetration testing scope would be to focus on achieving pre-agreed objectives within a pre-agreed, reasonable timeframe.

With respect to this type of penetration testing, a goal can be defined in a number of ways, and can encompass the many domains of information security; network security, application security, physical security and user awareness.

As an example, we have tested against objectives like the following:

- Is it possible to access and compromise card payment data?
- Can personally identifiable information (PII), that can impact on GDPR, be compromised?
- Is it possible to gain access to a specific, high value host on a network or access a segregated or high-security network or physical location?
- Is it possible to achieve unauthorized access to an operational technology (SCADA / ICS) networks from an adjacent IT, corporate network or the Internet?

In order to satisfy these objectives, BSI use the methodologies from each of the corresponding assessment types as applicable, so for example, the "*Is it possible to access and compromise card payment data?*" objective, the testing team could have combined application testing, network infrastructure testing and perhaps mobile application testing (depending upon the use-case) as the means to achieve that objective. Similarly, for "*Is it possible to gain access to a specific, high value host on a network or access a segregated or high-security network or physical location?*", the testing team would have employed social engineering techniques in the form of physical security testing to first obtain unauthorized access to the target building, office or object, then, network infrastructure testing to attempt to access the target host or network.

Additionally, to test current detection and response capabilities on a reasonable scale, utilizing stealth can be one of the main objectives of object-oriented penetration testing, to determine whether it is possible to attempt attack the organization without detection. In cases where this is the first or introductory exercise to red teaming for the organization, this is what BSI refers to as "Red Team Lite" in our attack simulation portfolio.

Organizational buy-in

With respect to organizational buy-in, objective-oriented penetration testing would be handled in the same way as a normal penetration test, including engaging and informing all key stakeholders that the assessment is happening ahead of time. The testing team also require the client to supply the usual information to facilitate the test, like URLs, IP addresses, email addresses or target building addresses and credentials.

Whilst there are common themes, each engagement is developed in a bespoke manner working closely with the client and the penetration testing team.

By engaging an objective-oriented penetration test, an organization can gain valuable insight into their susceptibility to various types of attacks, increasing their ability to react to and defend against adversaries.

By engaging an objective-oriented penetration test, an organization can gain valuable insight into their susceptibility to various types of attacks.

Red team testing

Whilst objective-oriented penetration testing typically combines a number of complementing assessment offerings with a specific set of objectives in mind, fully fledged red team engagements take those principles and develop them further, emulating the Tools, Tactics and Procedures (TTPs) of real-world attackers. A red teaming engagement is objective-oriented and will focus on agreed objectives similar to the ones outlined earlier.

However, that is not the only intended outcome, such engagements are intended to provide an organization with insight into their ability to detect, prevent and respond to an advanced persistent threat (APT).

In contrast to a traditional or goal-based penetration test, a red teaming engagement is typically performed from as close-to-a-zero knowledge perspective as possible, with the offensive team (red team) performing the engagement from a black-box perspective. Similarly, the organization as a whole is not notified ahead of the engagement, thus removing its ability to prepare for the assessment.

Red teaming objectives

A red team testing objective can be defined in the same way as was explored in the objective-oriented penetration testing section. By setting the objective to reflect a real-world attack scenario, the engagement becomes representative of the specific threats facing an organization. As previously mentioned, however, red teaming is also designed to exercise the internal teams and their procedures for responding to and defending against attacks, as they are not afforded prior knowledge of the test.

Red team vs blue team

As per a typical war game-based scenario, a red team engagement consists of attack vs defence, respectively the red team vs blue team; the roles of both teams are now explored a little more closely.

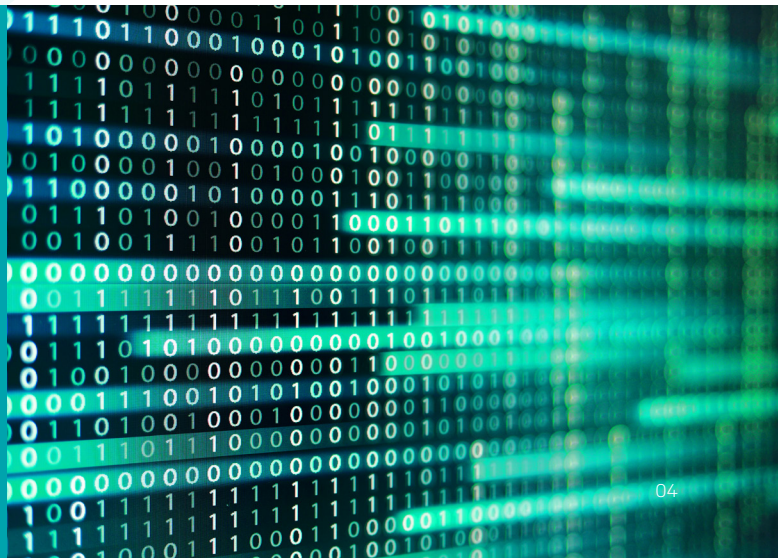
The red team would utilize the necessary TTPs and offensive techniques in order to establish a foothold within the organizations network and achieve the outlined objectives of the engagement. They generally perform the assessment from a black-box perspective, with as wide-ranging a scope as possible, covering all assets that are defined as belonging to the organization. Information like IP addresses, URLs and key assets would not normally be shared prior to the start of a red team engagement. A red team would also look to establish persistence within an organization over a period of time, such that should the blue team identify their efforts to establish unauthorized access, they would be easily able to regain the necessary access.

In contrast to the red team, the typically internally resourced blue team, has a primary focus to proactively and reactively defend an organization against attacks, in this case, those originating from the red team. They would typically have zero knowledge of the assessment, lending itself to accurately emulating a real-world situation. Operating this way ensures the optimum level of realism by offering no means for the blue team to prepare for the attack, be on the lookout for suspicious activity or raise awareness amongst staff members, all of which may impact the effectiveness of a red team engagement. For smaller organizations, the blue team effort may well be outsourced through the use of a Security Operation Centre (SOC), who will monitor a network for suspicious activity.

By testing the blue team, the red team engagement is designed to allow an organization to have insight into the suitability of their incident response policies, procedures and technical ability. A full timeline of events is also provided to the blue team following the engagement to allow for the identification of attacks that occurred and to bolster detection capabilities if they were missed.

Additionally, BSI deliver a workshop with relevant staff and key stakeholders as part of a standard red team engagement. Over the course of this workshop, BSI will walk through each of the attack scenarios, timelines and outcomes in detail, as well as review the actions performed by the blue team. The objective of this workshop is to identify, discuss and advise on opportunities for improvement to further align the organization with cybersecurity best practice.

By setting the objective to reflect a real-world attack scenario, the engagement becomes representative of the specific threats facing an organization.



Enhancing your penetration testing regime
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (IE)
Email: cyber@bsigroup.com

Assessment levels

Within a red teaming engagement, there are a number of different levels of testing, each of which are intended to represent the types and levels of attack an organization may face, dependent on their risk profile.

Threat intelligence is the first phase of a red team engagement and is used as a way to inform the assessment, and to highlight the type of threats that the target organization may face and from which adversaries. The output from this phase dictates the type of adversary and their skill level that will be imitated during the testing.

Examples of types of adversaries could range from an opportunistic attacker using off-the-shelf products, exploiting known vulnerabilities within common frameworks or performing a generic phishing campaign, to a slightly more sophisticated attacker who may be using more advanced techniques, being spear phishing, using private or commercial-only exploits or commercial level implants and Remote Access Tools (RATs).

There are even further levels of adversaries that exist beyond this level, including nation states, who would perform very sophisticated attacks, including using custom implants and RATs, unpublished zero-day vulnerabilities or advanced physical attacks. The assessment level required to be replicated should be based on the risk profile of the organization.

During the assessment, there are also varying levels of "noise" that can be replicated which correlate to the level of adversary being emulated. The lowest level of adversary highlighted here would typically be quite noisy on a network by performing activities which should be easily detected. The more advanced adversaries would perhaps be a little less noisy minimizing scan activity and avoiding techniques for instance brute-forcing to further minimize the likelihood of detection. The nation state adversaries would typically be very stealthy, often performing these attacks over a long period of time whilst evading security products, for example, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and anti-virus solutions. The levels of "noise" can be tuned up or down during the engagement to simulate the level at which attacks are formed.

Organizational buy-in

In comparison to penetration testing or objective-oriented testing, a red teaming assessment does require a much higher level of organizational buy-in from the outset to be accepted and successful. Typically, the involvement and drive for such an assessment comes from the senior management within an organization to provide assurances that the organization is as resilient to attack as expected or to independently highlight the impact an organization's current security posture and its security budget, could have on the business.

Additionally, there would typically need to be buy-in from other areas of the organization too, including HR due to the people element of the testing and also the legal team, to ensure that the testing is above board and does not break any laws or contracts that the organization is bound to.

Other than the above, the remainder of the organization is typically unaware of the engagement to ensure the realistic nature of the testing is upheld.

Within a red teaming engagement, there are a number of different levels of testing, each of which are intended to represent the types and levels of attack an organization may face, dependent on their risk profile.

Enhancing your penetration testing regime
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (IE)
Email: cyber@bsigroup.com

Case Study

As an example of the value a red team assessment will bring, the BSI attack simulation team conducted a red team exercise against a financial institution that wanted to assess their prevention, detection, and response capabilities against the threat of a sophisticated outside attacker motivated by financial gains.

BSI's red team were tasked with the objective to gain authorized access to the financial institution's internal network and applications. As the external perimeter of the organization appeared to have been securely hardened, BSI's red team targeted the organization's employees through social engineering attacks, mimicking the methodology and approach of a realistic attack against the organization.

The contact information of the organization's employees was harvested through reconnaissance exercises and targeted social engineering attacks were performed against relevant employees, with the attacks emerging from BSI's dedicated phishing server.

These phishing attacks appeared to emerge from the organization's support and service desk functions, with links to a BSI controlled transparent reverse proxy. Victims of this attack were tricked into submitting their credentials to BSI's controlled proxy, which were then forwarded to the relevant, authentic portals, making the attack appear benign.

Once this phase of the exercise was completed, it was possible for BSI's red team to gain unauthorized access to the organization's cloud hosted applications and VPN portals using the compromised credentials, achieving the objective of the exercise.

Upon completion of this exercise, it was evident that even though the external perimeter of the organization was securely hardened, it was still possible to gain access to the internal network through targeted social engineering attacks against employees. Highlighting scope for improvement in employee security awareness training, and inadequate detection and prevention controls on the users' devices.

In addition, one of the main outcomes of the exercises highlighted that even though multiple detection and response solutions were deployed, the red team's activities went undetected. After thorough investigation, it was discovered that some of the security solutions deployed on the network had been misconfigured, whist others were not fine-tuned to the organizations expected security baseline, reducing the likelihood of detecting and alerting anomalous behaviour. In one case, one of the tools was configured properly, however an exception to all internal VLANs was applied, rendering the tool ineffective.

This is something encountered on a regular basis during red team and purple team exercises, an organization would have a lot of tools in place to detect and respond to breaches and threats, however these are often not utilized properly and therefore, offer a false sense of security.

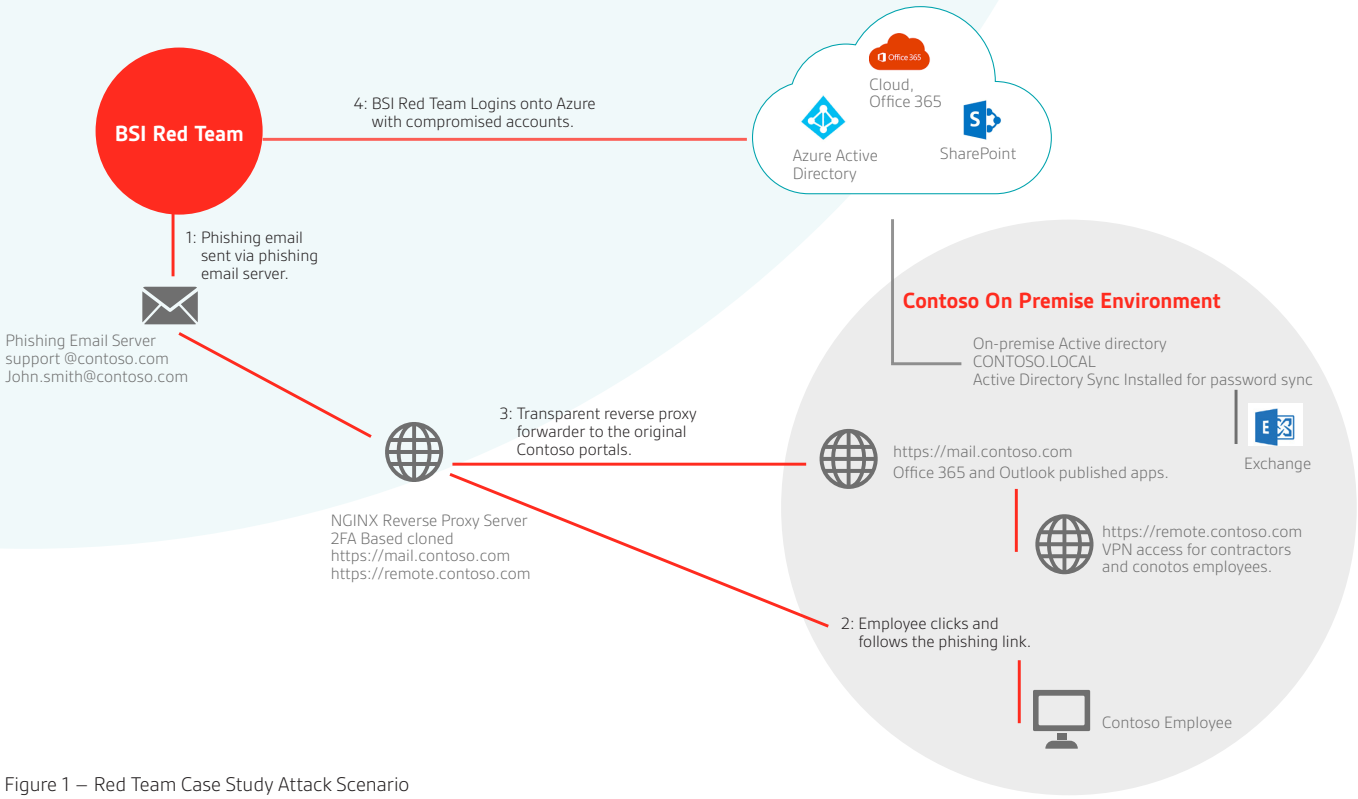


Figure 1 – Red Team Case Study Attack Scenario

Red and Blue – Purple team

Another high value adding exercise that can be done on its own or after a red team assessment is what is called a "purple team" exercise. This is a highly collaborative exercise in which both the red and blue teams work together closely to exchange knowledge, identify gaps and assess the current detection and response capabilities of the organization.

Prior to the commencement of a purple team exercise, a set of scenarios and TTPs to form the basis of the purple team exercise are agreed upon. This can be the output of a threat modelling, a table-top, or a red team exercise. Once agreed, both teams will sit together to commence the exercise during which the red team will go through the list of tactics and techniques one by one and work closely with the blue team to measure, fine-tune, and develop the organization's detection and response capability of each technique.

While traditionally both the red and blue teams have been operating separately and communicating through findings reports, this exercise gives the blue team practical exposure and insight into the operations of a red team.

What type of testing fits my organization?

Security testing requirements for organizations depend on their current security posture and maturity level. BSI has developed the Security Testing Maturity Framework, Figure 2 below, to aid organizations in assessing their current maturity level and the most effective security testing level.

Foundation

Vulnerability Assessments: Utilizing tools and techniques which are designed to identify and classify vulnerabilities before applying consultant knowledge to verify identified vulnerabilities and apply context for prioritization

Focused

Penetration Testing: using manual testing techniques along with some automated processes and tools to assess the security posture and identify any security vulnerabilities which may be present in specific assets, for example, networks, web applications, mobile applications and internet of things devices

Resilient

Attack Simulation Assessments:

Red Team testing (offensive assessments), attacking the whole organization across multiple domains (people, process and technology)

Blue Team testing (defensive assessments), coaching and assessing response team activities versus best practice or organizational key performance indicators (KPIs)

Purple Team testing (offensive and defensive), with one team performing offensive attacks whilst assessing, and in some cases coaching, the defensive teams' ability to respond to the attacks.

Security Testing Maturity Framework

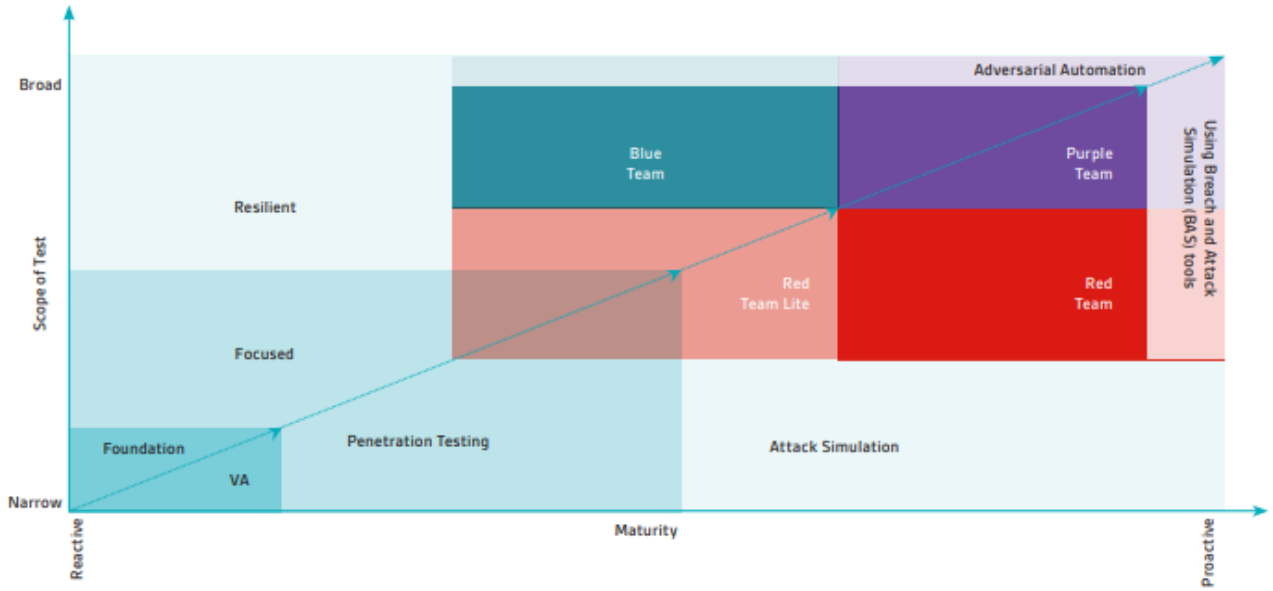


Figure 2 – BSI Security Testing Maturity Framework

Conclusion

The penetration test, which has been a focal point of the cybersecurity industry for many years, is a tried-and-tested method for understanding the security posture of assets. However, there are limitations to this approach, as penetration testing determines the security posture of a particular asset, not the organization. Therefore, in recent years conducting periodic attack simulation exercises have become the norm, for security mature organizations, in conjunction with traditional penetration testing.

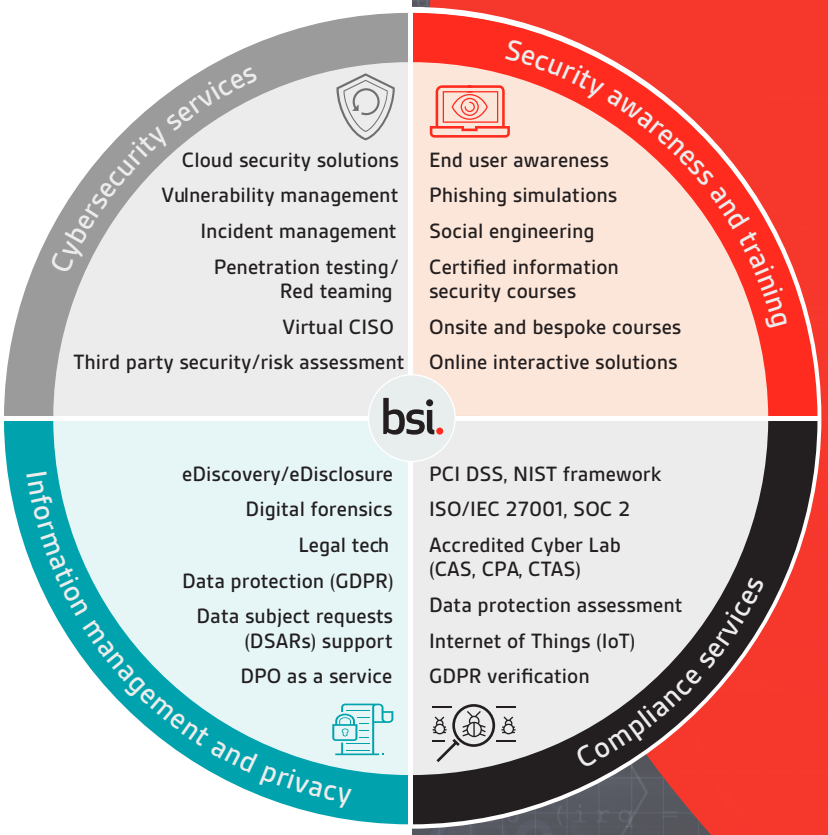
This whitepaper has explored two attack simulation testing types which can add a real-world element to organizations' penetration testing efforts; objective-oriented penetration testing and red teaming. Both types of assessment offer an advancement over standard penetration testing as they reflect realistic attack scenarios and therefore allow organizations to better understand their cybersecurity weaknesses. Also, by shifting the focus of the test to pre-defined and agreed objectives, the testing can then encompass the many different domains of cyber and information security across the organization.

Planning and delivering an objective based penetration test or red teaming engagement, an organization can gain a greater understanding and appreciation of the likelihood of a successful compromise, the types of adversary they may face, and how well they are equipped to respond to and deal with such an incident. Additionally, an organization can conduct Cyber Readiness assessments like table-top and threat modelling exercises to be better equipped and maximise the value and insights gained from a red team engagement.

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, and consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Consultancy Services include:



Our expertise is accredited by:

Find out more

IE/International
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us

bsi.