BSI Attack Simulation Services

Our Attack Simulation Services are a series of complementary, advanced services designed and delivered by our global offensive and defensive security teams. These services are intended to highlight an organizations' susceptibility to compromise from real-world attacks, by accurately simulating the Tactics, Techniques and Tools (TTPs) of the most likely adversaries. The Attack Simulation Services are also well placed to help an organization determine how well prepared they are to prevent, detect, respond and recover from an attack.

Red Team Star Flow

Our Attack Simulation Services comprise of a combination of offensive, defensive and table-top based activities to provide a holistic approach to Attack Simulation assessments.

Offensive – Red Team

Our Red Team performs all offensive based activities within the Attack Simulation Services. The offensive assessments are defined into three, distinct levels:

- Red Team Lite
- Red Team Standard
- Red Team Plus

With Red Team Lite and Red Team standard assessments, the complexity of the engagement can be reduced, and the levels of knowledge provided to the red team (grey box) increased. To provide increased value to the assessment, certain phases of the assessment can be "staged" to provide access, or entry points to the internal network for example.

A Red Team Plus engagement is our full in-depth attack simulation engagement considering all phases of the cyber kill-chain and encompassing detailed threat intelligence to enhance the assessment. All domains of security are in-scope, including IT assets, physical assets and your employees.

Hybrid – Purple Team

Our Purple Team encompasses both offensive (Red) and defensive (Blue) consulting capability to provide a highly targeted and educational assessment for organizations and their internal teams. The assessment is usually performed in full sight in a collaborative manner. The Red Team is utilized on a purple team assessment, their actions being used to "coach" the internal blue team by assessing against a specific test plan to determine the blue team's capability to prevent, detect, respond and recover to an attack.

Cyber Readiness

Our Cyber Readiness assessment takes a deep-dive view of your organizations' level of preparedness. By reviewing and benchmarking Incident Response plans, policies and playbooks along with performing threat modelling exercises and table-top exercises to "dry-run" specific compromise scenarios. We're able to determine the level of Cyber Readiness within an organization, from the technical staff who would be on the front-line all the way up the to the executive level, understanding how well the organizations' customers security and reputation are protected. A Cyber Readiness assessment from BSI encompasses both members from the Red Team and also from wider information governance teams.

Credentials

Our highly skilled and experienced global consulting team comprises of team members from a multitude of backgrounds and industry qualifications. With consultants headquartered out of cybersecurity hubs in Ireland, UK, the US and the wider Europe, BSI is well placed to provide high quality Attack Simulation assessments to our clients. Our team maintains extensive industry qualifications, including CREST (CCSAS, CCT-INF, CCT-APP), Tiger (SST), Cyber Scheme (CSTL), Offensive Security (OSCP and OSWP), SANS (GWAPT and GPEN) and extensive academic qualifications including Masters and PhD.

CREST

CREST STAR

bsi.

...making excellence a habit.™