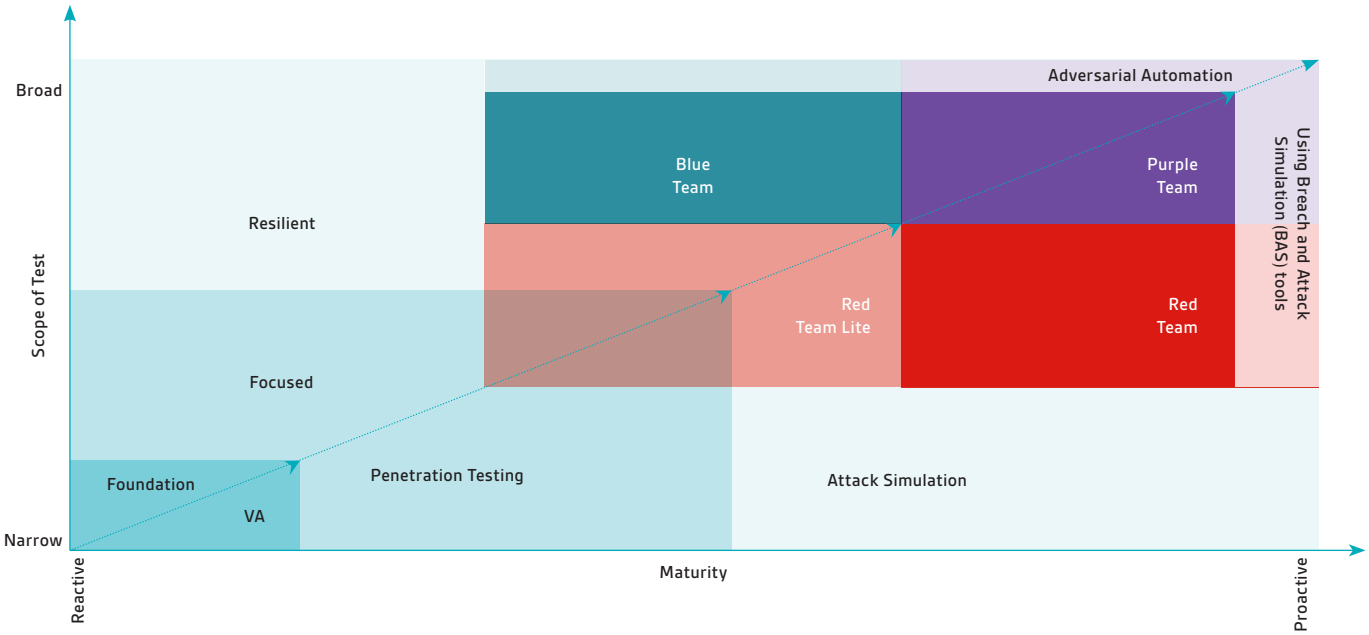
The BSI Security Testing Maturity Framework

The BSI Security Testing Maturity Framework will identify the most effective security testing level for your company dependent upon the maturity of your security operations, team and the risk appetite of the organization.

Security Testing Maturity Framework



Foundation Level – Vulnerability Assessment

The foundation maturity level is designed for organizations that are looking to establish their security capability. It is the first step on the journey to improving your information security maturity and creates the initial technical baseline from which to build on your security program.

The Vulnerability Assessment (VA) scan is an automated test that assesses your internal IT networks and perimeter for potential and actual vulnerabilities. Each vulnerability is reviewed independently of one another. The scope focuses on running many automated tests (breadth) rather than manually probing how far they can get into the network (depth). Exploitation is not typically involved with VA assessments; however, issue verification would be carried out.The VA approach can also be used to support the compliance requirements such as PCI.

Focused Level – Penetration Testing

This maturity level is designed for organizations with a growing security capability and are looking to identify and achieve security improvements. This should also align with the organisation's risk appetite.

The scope of a penetration test is typically defined at a specific business function, focusing on a specific set of well-defined technical assets. Penetration Testing uses a mixture of manual and automated techniques to find vulnerabilities. Each vulnerability is fully assessed with exploitation performed to determine the full impact, however, often vulnerabilities are chained together to have a greater impact. Traditional penetration testing techniques would include network level testing (internal and external), web application, API, mobile application or even social engineering.

This style of penetration testing has traditionally been the defacto choice of security testing.

Resilient Level – Attack Simulation

This maturity level is designed for organizations with a fully grown, established security function who are looking for holistic assurances across their business with regards to their security posture.

The scope of testing for the attack simulation approach is significantly widened and does not focus solely on specific assets or business function. It rather focuses on the whole organization across multiple information security domains.

The intended outcome of the attack simulation approach provides an organization with a strategic view to their:

- **susceptibility to be compromised by real world adversaries**
- **ability to prevent, detect, respond and recover from an attack**

To achieve this, an attack simulation mimics the Tactics, Techniques and Procedures (TTPs) of real-world adversaries and focuses on the elements within the cyber kill-chain.

Attack simulation assessments provide clients with realistic, intelligence-led testing, designed to realistically test organisation's ability to identify and respond to a real cyber-attack. Depending on the nature of the assessment, we can provide a layered service, which can include:

- Red team testing (offensive assessments), attacking the whole organisation across multiple domains
- Blue team testing (defensive assessments), coaching and assessing response team activities versus best practice
- Purple team testing (offensive and defensive), with one team performing the offensive attacks and the other team assessing and coaching the organisation's ability to respond

bsi.

...making excellence a habit.™