methods
AN ALTEN COMPANY

Penetration Testing

To gain insights into potential threats to your network, it's essential to simulate a realistic attack scenario in a controlled environment. This approach enables you to accurately identify the risks that your company faces from determined intruders. In doing this you can assess your vulnerability to potential compromises and take proactive steps to address them before malicious hackers can exploit and harm your assets.

Service Offering

Method's Penetration Testing Services team offers a range of comprehensive engagements, including network, application, wireless, social engineering, IoT, Red Team, and specialised assessments. These services are designed to assess the security posture of your organisation's critical systems and infrastructure effectively.

Assess, evaluate, and identify security weaknesses by simulating real-world attacks on your organisation through:

Web Application Penetration Testing

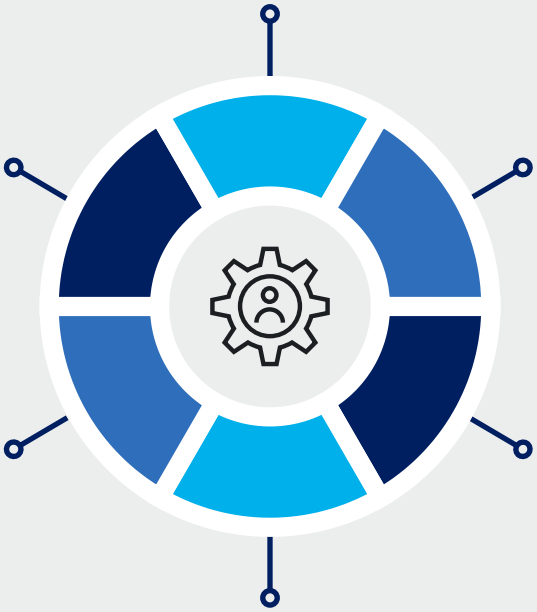
Identifying security risks including the OWASP Top 10 and business logic security flaws

Red Team Testing

Custom-designed tests for your organisation working alongside mature security programmes in order to test all controls and layers

PCI DSS Compliance

Ensuring you are going beyond just meeting compliance standards and that your payment systems are secure end-to-end



Network and Infrastructure Penetration Testing

External and Internal networks will be investigated including reviews of Active Directory

Cloud Penetration Testing Services

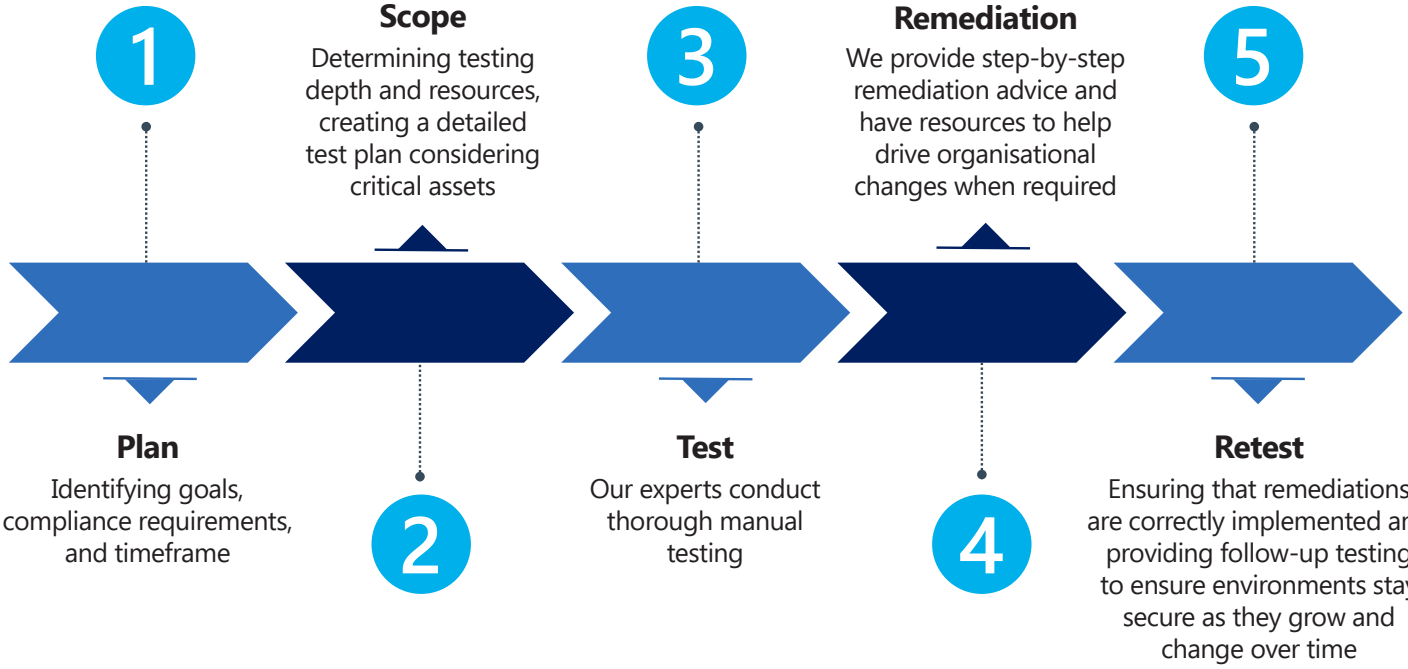
We specialise in cloud technologies including testing of AWS, GCP, and Azure infrastructure along with SaaS applications

Operational Technology (OT) Testing Services

Identifying weaknesses and ensuring implemented security controls are effective

Pentest Lifecycle

We give expert independent and tailored advice, working towards cyber security that is:



Key Service Features

We utilise well-defined and industry-standard methodologies (such as OWASP, PTES, CREST, and NIST SP 800-115) to conduct the penetration testing process systematically and thoroughly.

Employing a combination of manual and automated testing techniques to identify vulnerabilities efficiently, while also uncovering more complex issues that automated tools may miss.

Providing detailed and actionable reports outlining the findings of penetration testing, including identified vulnerabilities, their severity levels, potential exploitation scenarios, and recommendations for remediation.

Guidance and support to the organisation in remediating identified vulnerabilities, including recommendations for patches, configuration changes, and security best practices.

Open communication and collaboration throughout the testing process, ensuring that their specific concerns, constraints, and objectives are addressed effectively.

Follow-up penetration testing engagements to validate the effectiveness of remediation efforts and ensure that previously identified vulnerabilities have been adequately addressed.

Ensures you are compliant with relevant industry standards, regulations, and guidelines, such as PCI DSS, GDPR, etc., based on your specific requirements.

Maintaining strict confidentiality and data protection measures to safeguard sensitive information discovered during the penetration testing process.

Key Service Benefits

Identifying vulnerabilities and weaknesses in the organisation's systems, networks, and applications before malicious actors can exploit them. By proactively uncovering these vulnerabilities, organisations can take corrective actions to mitigate potential risks.

Reducing your exposure to cyber threats and minimising the likelihood of successful cyber attacks. This risk reduction can help protect sensitive data, intellectual property, and other critical assets.

Penetration testing raises awareness among employees and stakeholders about cyber security risks and the importance of maintaining a strong security posture. It helps foster a culture of security within the organisation and encourages proactive security practices.

By simulating real-world attack scenarios, penetration testing helps organisations improve their incident response capabilities. It allows them to test their detection and response mechanisms, as well as their ability to contain and mitigate cyber attacks effectively.

Identifying and mitigating vulnerabilities through penetration testing can help ensure business continuity by minimising the impact of potential cyber incidents. By addressing security weaknesses proactively, organisations can reduce downtime, financial losses, and reputational damage.

A successful cyber attack can severely damage an organisation's reputation and erode customer trust. Penetration testing helps organisations identify and address security vulnerabilities before they can be exploited, thereby safeguarding their reputation, and maintaining customer confidence.

Early addressing of security vulnerabilities via penetration testing can save costs by preventing potential data breaches, fines, legal fees, and other expenses linked to cyber attacks. Proactive security investments are often more economical than managing post-incident fallout.

Regular penetration testing showcases a commitment to cyber security, giving organisations a competitive edge. It boosts credibility and trust with customers, partners, and stakeholders, leading to increased business opportunities and market differentiation.

An iterative process that allows organisations to continuously improve their security posture over time. By conducting regular tests, organisations can identify emerging threats and vulnerabilities and adapt their security measures accordingly.