Cyber Security Wrap Around Solutions

SECURITY TESTING

- Web Apps
- Web Services
- Mobile Apps
- Vulnerability Assessments
- Internal Infrastructure
- External Infrastructure
- Cyber Essential Accreditations
- Firewall Reviews
- Build Reviews
- Phishing
- Cloud / O365
- Code Reviews
- Database Reviews
- ITHC
- SSO
- SAML
- VPN
- Thick Client Testing
- Wireless Testing

All above have detailed questionnaire to asess your unique requirements which we then analysed to give you the best quality testing experience.

CYBER SECURITY (SSWAS)

Comprehensive Cybersecurity:

Our cybersecurity services are designed to safeguard your business against evolving threats with a comprehensive approach tailored to industries such as finance, education, and healthcare. Our team of certified Ethical Hackers and expert penetration testers conduct rigorous assessments across your web applications, web services, and mobile devices, identifying vulnerabilities before they can be exploited. We offer in-depth vulnerability assessments, covering both internal and external infrastructure, and provide Cyber Essentials certification support to ensure compliance. Our services include detailed firewall, cloud, O365, build, and code reviews, along with specialized assessments such as phishing simulations, wireless testing, and thick client testing.

We also conduct social engineering exercises, database security reviews, break assessments, and test secure access methods like SSO, SAML, and VPN. With a disciplined, proactive approach, we provide the highest level of security, helping you mitigate risks and fortify your infrastructure against cyberattacks.

Our Pre-Sales Cyber Security team plays a crucial role in understanding and assessing the security needs of each client before initiating vulnerability testing. The team engages with clients through a set of carefully designed and unique questionnaires aimed at gathering comprehensive information about their IT infrastructure. These questionnaires cover critical aspects such as hardware, software, network configurations, cloud deployments, and security policies. By obtaining detailed insights into the client's environment, we ensure that our vulnerability testing is tailored to their specific needs and covers all areas of concern, including legacy systems, third-party integrations, and cloud infrastructures.

Once we have gathered the necessary information, our team performs in-depth vulnerability assessments across all areas of the IT infrastructure. This includes on-premises systems, data centers, and network configurations, as well as cloud environments like AWS, Azure, or hybrid clouds. The objective is to identify potential vulnerabilities that could expose the organization to security breaches, data leaks, or operational risks. Whether it's scanning for outdated software, insecure configurations, or potential entry points in the cloud, we provide a thorough and comprehensive assessment that leaves no stone unturned.

The questionnaires not only help in scoping the assessment but also enable our Pre-Sales team to align the testing with the client's security goals. This approach allows us to deliver customised recommendations that address specific pain points and potential threats in their infrastructure. By involving our clients early in the process, we ensure that the resulting security strategy is aligned with their business objectives, compliance requirements, and future growth plans.

Following the assessment, we provide a detailed report highlighting the vulnerabilities uncovered, along with actionable recommendations for mitigation. Our team works closely with the client to prioritise and address these findings, ensuring that their IT and cloud infrastructure is fortified against current and emerging threats. Through this proactive approach, our Pre-Sales Cyber Security team ensures that clients are well-prepared to secure their digital assets while maintaining operational efficiency.

ADSINET LTD
technology
consulting