Penetration Testing Services

Stay ahead of threats with DXC Technology, a leader in Cyber Resiliency Services

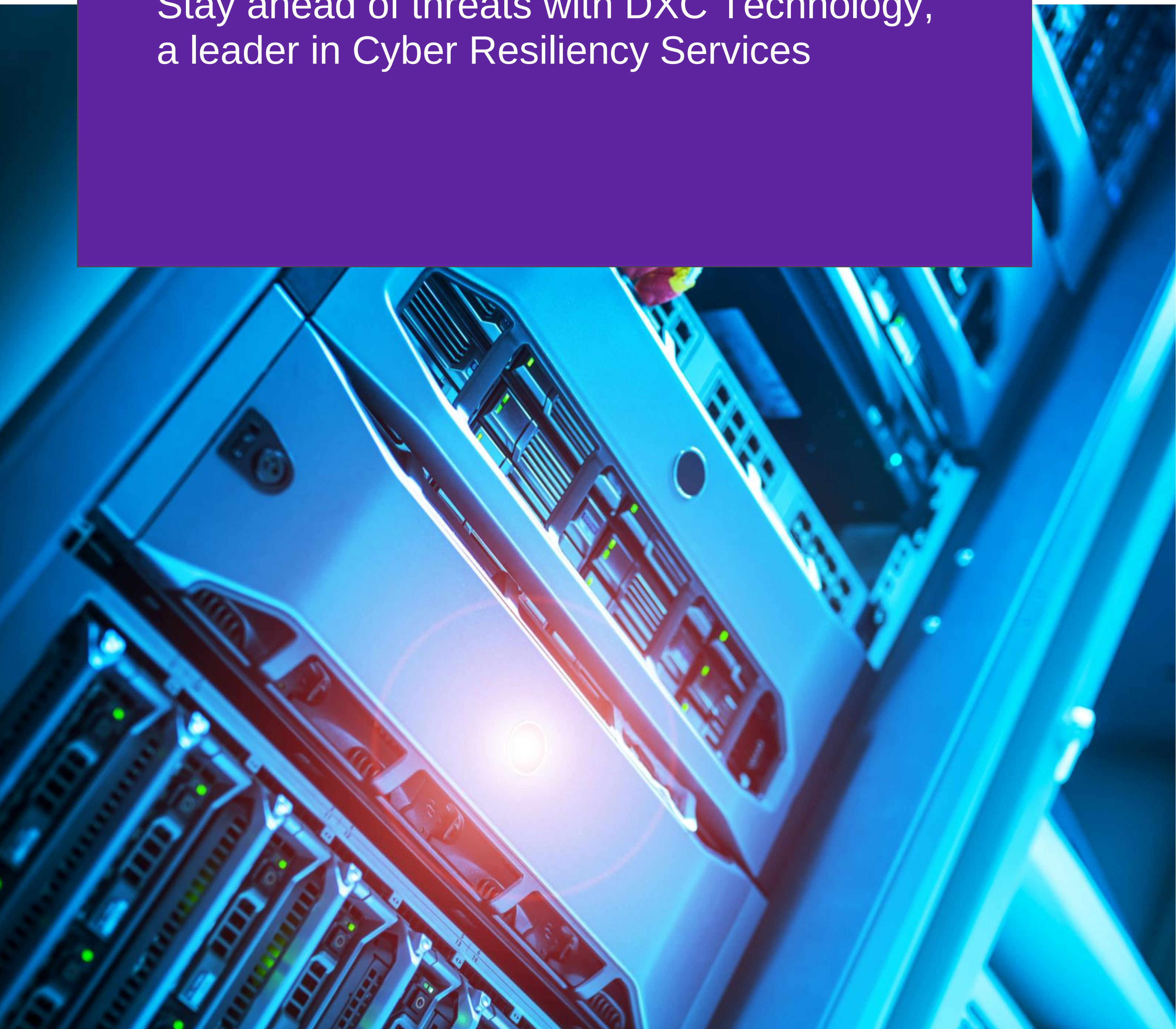


Table of contents

Background

Organisations are increasingly concerned about cybersecurity attacks, both on their organisations and in their industry. Cybersecurity attacks exploit weaknesses in an organisation's applications and underlying infrastructure.

DXC's Security Defense services improve security by identifying and assessing security threats and weaknesses that enable attackers to cause damage through data theft and by gaining access to valuable intellectual property (IP).

The Penetration Testing Service Catalogue allows customers to engage in effective security testing with DXC Technology.

Introduction

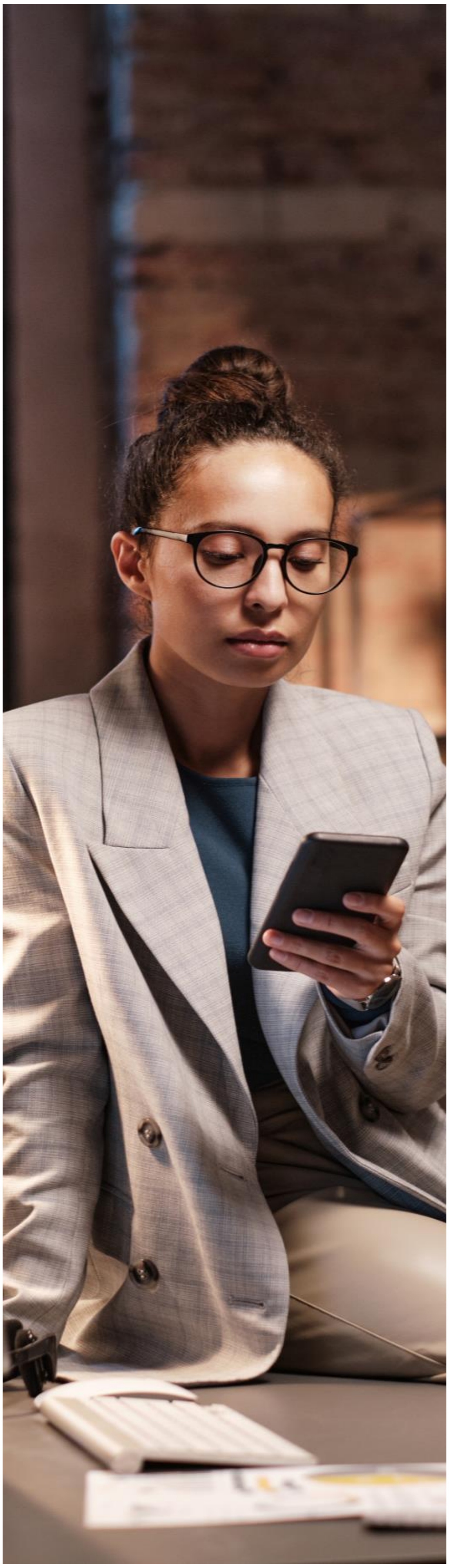
Defend against today's cyber threat landscape with a recognised leader in cyber resilience services.

As enterprises adapt to changing business models, security is now top of mind to protect and grow business with confidence.

DXC's Cyber Defence team manages mission-critical systems for thousands of large organisations worldwide with a key focus of understanding cyberattacks and how they occur. Quite often, the biggest enemy is the enemy within: highly complex, poorly implemented and/or poorly maintained IT environments.

As cyberattacks become more common and sophisticated, the best way to stay protected is to act before the adversary does. In order to stay protected, organisations can complete penetration testing, vulnerability scanning and management, social engineering, and cyberattack simulations. This allows organisations to identify points of weakness in their environments and how to address them.

Our services are delivered globally with expert teams who employ an industry-aligned, business-led approach. DXC's Cyber Defence team engages quickly to improve organisation's security by identifying and assessing security threats and weaknesses that could enable attackers to steal data, gain access to intellectual property (IP), or damage the business.



Web Application Penetration Testing

Web applications typically represent the most exposed portion of an organisation's infrastructure and often store critical data. This means that web applications are the most heavily targeted asset by threat actors, and breaches can have an immense financial and reputational impact on your company. Penetration testing identifies exploitable weaknesses in web applications, assisting in the remediation of vulnerabilities that hardens the application against attacks.

Duration: 5 days to 4 weeks

Mobile Application Penetration Testing

Mobile applications regularly house critical data about company customers, employees, or assets. The security of these applications is often neglected by many businesses. This combination of high-value data and low-security integrity has made mobile applications an increasingly attractive target for cybercriminals. DXC offers penetration testing solutions to assist in identifying weaknesses in mobile applications and provides advice on remediation strategies that harden your application against threat actors.

Duration: 5 days to 3 weeks

Source Code Review

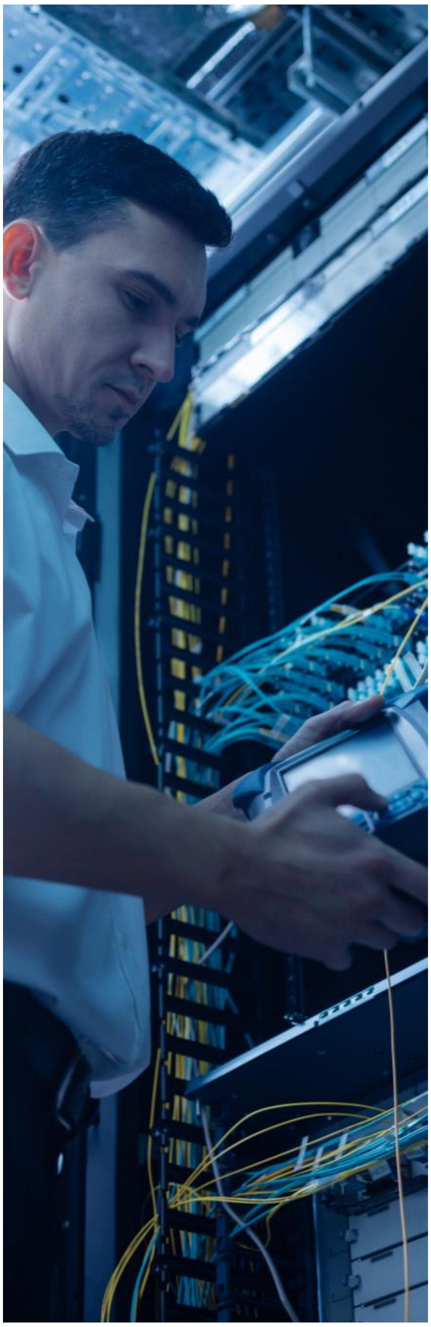
Source code review (White-box penetration testing) is an audit of an organisation's code-base for any exploitable design flaws. This style of testing offers a more comprehensive solution for security, as it allows the tester to identify and provide remediation advice for subtle vulnerabilities that can be missed in a pure black-box test.

Duration: 5 days to 4 weeks

Cloud Assessments

As more organisations are turning to the cloud for their information services, the unique risks presented by these environments necessitate a careful approach to ensure all services are securely configured. Misconfigured cloud services are one of the top causes of data breaches. Our Security Testing Team can be engaged to review and analyse your cloud environment to ensure best practice is being implemented.

Duration: 5 days to 2 weeks



Internal & External Network Penetration Testing

A network is one of the organisation's most critical assets. The exploitation of a network often results in the complete compromise of company data with subsequent devastating consequences, such as the installation of ransomware across company property. An external penetration test, conducted from public internet, aims to penetrate the network's perimeter and gain access to an internal network segment. In contrast, an internal penetration test, conducted from the internal network segment, is from the perspective of an assumed breach. It ensures that any internal threats are limited in their ability to access and extend their control over company assets further through lateral or vertical movement.

Duration: 5 days to 4 weeks

Wireless Penetration Testing

A wireless penetration test is aimed at detecting and exploiting vulnerabilities in security controls employed with the use of wireless technologies. This includes the standards that support wireless technologies, access points, security protocols and clients.

Duration: 3 days to 2 weeks

Vulnerability Assessment

A vulnerability assessment is where your digital assets are scanned to search for known vulnerabilities. This differs from a penetration test as no vulnerabilities are exploited, and the scope is generally wider and aims to identify and classify all vulnerabilities across the network or systems. Vulnerability assessments have many benefits, including validating vulnerability management, ensuring best practice is being followed and that the latest patches are being applied whilst keeping up with the current threat landscape. It can also be used to locate potential rogue devices on your network that are not authorised, alongside suspicious new local users on devices and hardware.

Duration: 3 days to 2 weeks

ICS & OT Penetration Testing

Operational Technology (OT) networks and Internet of Things (IoT) offer a unique challenge for businesses. With the continued blurred boundary of OT and IT networks, these networks are exposed to increasing threats of attack. DXC's Security testing team has real work experience, industry knowledge and expertise in performing assessments and penetration tests against production OT networks. These assessments allow for a greater understanding of threats and risks within environments and can be tailored to risk assessments, vulnerability assessments, and passive and realistic simulations of attacks on these sensitive networks and devices.

Duration: 5 days to 4 weeks

Social Engineering Assessments

Breaches of confidential information often arise from low-tech attacks, where employees are manipulated into divulging sensitive information or providing access to malicious actors unwittingly. Security testing offers a wide range of social engineering services that utilise these tactics. DXC can measure your employees susceptibility to these attacks, providing guidance on where to focus security awareness education efforts that will reduce the likelihood of these attacks succeeding. We can tailor a testing program that suits the threat model of your organisation through electronic methods such as e-mail, voice and SMS phishing and physical methods such as tailgating, USB drops.

Duration: 3 days to 2 weeks

OSINT Assessments

Open Source Intelligence (OSINT) assessments provide visibility to your organisations publicly accessible data. This information allows you to prevent opportunistic attacks and reduce the attack surface of your network perimeter. This makes it harder for threat actors to achieve a foothold in your organisation. If your employees have been the victim of a public data breach, this knowledge can be used to notify them that their account has been compromised and educate them on the dangers of password reuse to help in securing your environment.

Duration: 3 days to 2 weeks

Physical Penetration Testing

A physical penetration test evaluates the physical security systems in place to expose any potential gaps in controls. Many organisations focus on cybersecurity at the expense of their physical security. By identifying gaps in physical security that undermine other security controls, security testing can help your organisation better protect systems, data, equipment, and other digital assets from unauthorised access.

Duration: 3 days to 2 weeks

Red Team Testing

DXC's approach to Red Team engagements provides a highly targeted and specialised simulation of a real-world attack against your organisation. This tests your organisations ability to detect and respond to an incident while also identifying areas for development or practice. Our Red Team operation creates custom tools, malware, and exploits to avoid detection by your organisations security team as we work towards the specific target objectives. Red Team Testing is generally recommended for organisations that have a certain level of security maturity, however, organisations that wish to test their security team's detection and response capabilities or organisations that have unique testing objectives also benefit from these type of engagements.

Duration: 2 weeks to multiple months

Elham Ghourbandi
Head of Client Security Delivery
eghourbandi@dxc.com

Sean Thompson
APAC Lead Penetration Tester
sean.thompson3@dxc.com

Why DXC Technology?

Broad Expertise and Specialisation.

Our security professionals balance broad expertise with specialisation where you need it.

Rooted in Experience.

Our ethical hackers, inspectors, auditors, systems and software engineers, systems architects, policy experts, trainers, and experts in certification and accreditation bring deep commercial and federal sector experience.

Highly Trained and Industry Certified.

The professionals on DXC's security team are certified in multiple specialised industry areas, with expertise in federal and commercial regulatory compliance requirements.

Technology Compliance Leadership.

DXC is a technology compliance leader with security laboratories in the United States, Europe and Australia that offer advanced security technologies worldwide.

Robust Network.

Our robust network provides an unrivaled capability to research, develop, test and deploy the most advanced security configurations for compliance within regulatory guidelines.

Industry Best Practices.

Our security team follows industry-validated best practices together with an in-depth understanding of security and regulatory requirements.

DXC Technology
dxc.com

About DXC Technology
DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at DXC.com.