DXC Application Security



The DXC Application Security service helps organizations protect applications in their IT ecosystem against cybersecurity threats and helps maintain compliance.

Applications have proliferated to meet the growing requirement for seamless, secure and quick access to information. This has radically transformed how organizations operate and how they create new opportunities. Applications have now become a vehicle for information exchange.

Per regulatory requirements, organizations must exercise due care when developing, designing, selecting and using applications — to ensure compliance with security practices and to protect applications.

DXC's Application Security service, based on an adaptive, prevention-first framework, designs solutions that align with your specific technology environment and information security management framework. The service delivers tailored solutions that:

- **Enable visibility and transparency** of application security posture risk management in the IT ecosystem
- **Maximize and enhance security investments** by consolidating, standardizing and integrating application security into information security risk and compliance management strategy
- **Leverage automation** for application security practices, to be **in step with velocity requirements** and goals of modern applications
- **Provide risk-based continuous assessments** throughout code progression, based on a policy framework that helps discover issues early, allows adequate time for remediation and reduces security risk
- **Enable auditability** with proprietary frameworks based on industry standards, such as the U.S. National Institute of Standards and Technology Secure Software Development Framework (NIST-SSDF), Building Security In Maturity Model (BSIMM), Open Worldwide Application Security Project Software Assurance Maturity Model (OWASP SAMM) and the BSA Framework for Secure Software (BSAFSS)
- **Reduce remediation costs, security risks and liabilities** by providing a secure path from code to deployment

Key benefits

- Improves security through visibility into application security posture management
- Meets or exceeds response time requirements through intelligent automation
- Maximizes security investments through integration with existing issue management frameworks and information security frameworks
- Enhances compliance through continuous security assessments
- Enables auditability through industry standards framework
- Reduces post-deployment remediation costs, security risks and liabilities of applications

DXC Application Security (as a digital immune system) — in action

A leading global insurance company wanted to enhance the digital experience for its customers and employees. The company was seeking a solution/platform that would support opening its core market services to plug-and-play, mix-and-match services. This would benefit customers and end users through rapid deployment of new features and multichannel secure technology solutions.

DXC implemented a **digital immune system** (DIS) for the core platform to support rapid secure development and deployment for the insurance company's new, transformed market services.

With security integrated into the DevOps environment, the DIS delivered:

- Faster time to market — with automated digital assurance
- Cost savings — by identifying and fixing vulnerabilities early in the code progression pipeline (fixed more than 50% vulnerabilities over the past year by collaborating with app owners)
- Higher quality and more secure code as a result of guardrails for visibility and actions in the development pipeline
- Stronger collaboration through empowering stakeholders to collaborate effectively in a prevention-first culture
- Active support of apps team in migrating applications from on-premises to cloud while maintaining the apps' security posture

DXC Application Security — features

The DXC Application Security service includes the following key features:

- Adaptive solution tailored to fit each customer's technology ecosystem
- Automation and intelligence to transition from DevOps to DevSecOps
- Threat modeling to identify threats, attacks, vulnerabilities and countermeasures, so as to meet security objectives at early stage of SDLC
- Continuous security assessment of applications code, build and runtime environments, to identify potential security issues
- Risk prioritization to support remediation management and reporting

Capabilities

Based on an adaptive, prevention-first framework, DXC Application Security offers the flexibility to choose from standard or tailored services:

- Integrating security services into the development life cycle, via SAST/SCA, DAST and penetration testing
- API security — automated discovery, attack protection, posture management, threat detection, and fraud and bot security
- Application security architecture review and threat modeling at early stage of SDLC
- Security testing of packaged apps and SAP apps
- Mobile application security testing

Why DXC?

As a leading global IT services provider, DXC Technology is uniquely positioned to help weave cyber resilience into our customers' IT security, operations and culture. Leveraging the experience of thousands of cybersecurity professionals, we offer a wide range of security solutions to public and private organizations worldwide, incorporating best security practices.

Learn more at
dxc.com/security

Get the insights that matter.
dxc.com/optin

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**.

© 2024 DXC Technology Company. All rights reserved. DG_9255a-25 July 2024