DXC.technology

Offering Overview

Solving the severe, pervasive applications security problem

DXC Comprehensive Applications Threat Analysis (CATA) service

Avoid security defects from the start with industry-leading ROI

Insights

- 70%-90% of successful security breaches are directed at the application layer.
- Find and fix vulnerabilities early in the lifecycle; it dramatically reduces lifecycle and maintenance costs (30×[1] to 100×[2] according to NIST).[3]
- Avoid regulatory compliance penalties, costly security-related downtime, and breach disclosure remediation costs to you and your customers with CATA.

The primary information technology cyber threat is changing from successful attacks against the network or infrastructure to attacks against applications. At the same time, the blurring of the boundary between work and personal devices, and the customers' demand for ubiquitous services, is rapidly expanding the number and locations of applications that organizations must secure. Enterprises must still deliver services from old applications (apps) that were not designed for this new threat environment, as well as provide services via new applications that put a premium on the users' experience over security. With these new threats and user profiles, Enterprises need to rethink how they address applications security.

Security quality exposes app and systems to substantial risks and rework

IT departments are under ever-increasing security requirements pressure from regulatory compliance and heightened threats that exploit undiscovered security defects.

Most applications miss or insufficiently address the underlying security requirements resulting from standards and governance sources such as Federal Information Security Management Act (FIMSA), National Institute of Standards and Technology (NIST), and Payment Card Industry-Data Security Standards (PCI-DSS).

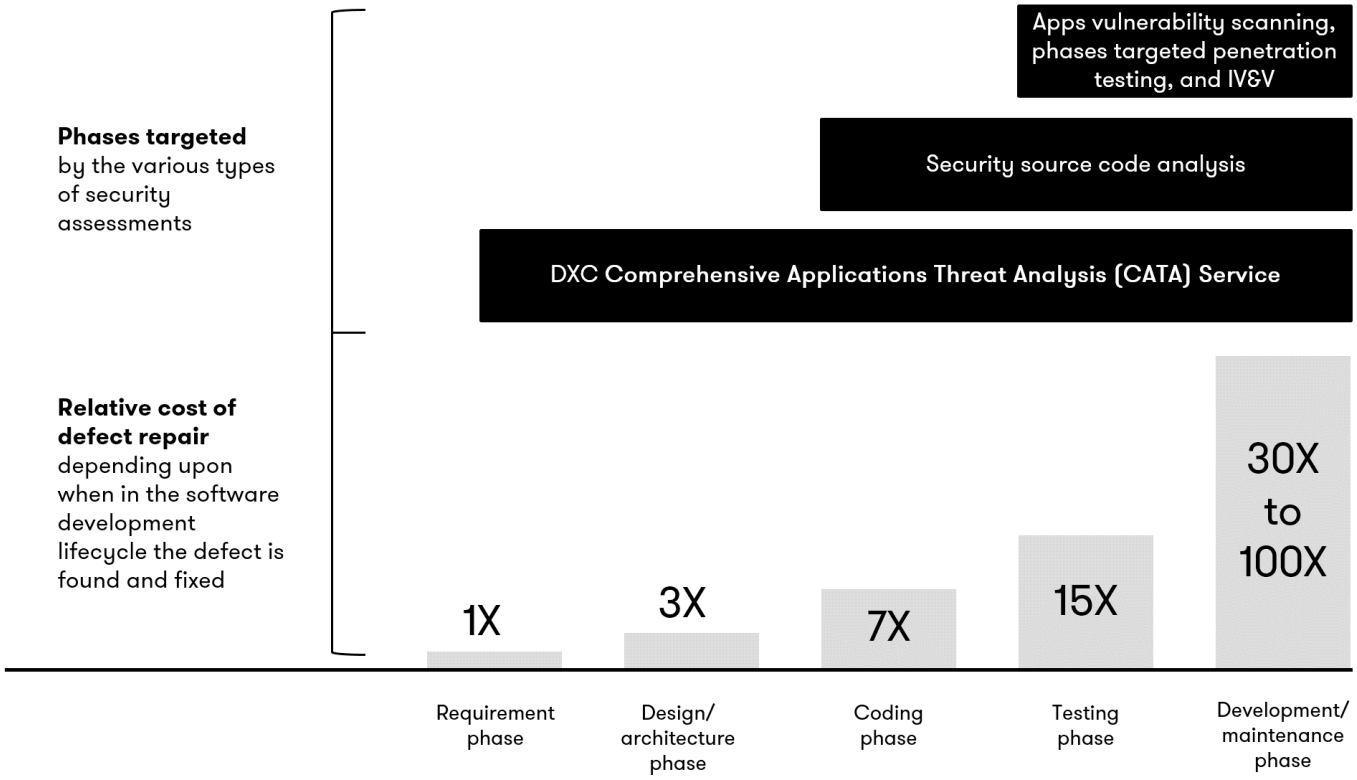
The severity of the applications' security issue continues to grow as networks become more secure, causing adversaries and criminals to refocus on the more vulnerable target—the applications. To demonstrate the pervasiveness of these security vulnerabilities:

- The US National Vulnerability Database (NVD) is currently populated with more than 80,000 separate vulnerabilities and exploits, which represents only a fraction of the problem.
- DXC Technology and other industry research estimate that the number of undiscovered security defects is at least 20 times the number reported, so per NVD, security vulnerabilities could number 1.6 million or more.

[1] http://nist.gov/director/planning/upload/report02-3.pdf, table 5-1, and table 1-5

[2] "Industrial Software Metrics: a Top 10 List"csse.usc.edu/csse/TECHRPTS/1987/usccse87-503/usccse87-503.pdf

[3] http://nist.gov/director/planning/upload/report02-3.pdf, table 5-1, and table 1-5



Unaddressed vulnerabilities can cause financial and operational risks

Security vulnerability costs include:

- Rework—Up to 100 times or more for development costs
- Noncompliance penalties—up to $1 million USD per incident for PCI-DSS alone[4] Planned and unplanned downtime due to security patching and incidents— ~$700,000 per hour average[5]
- Breach disclosure costs—$5.4 million per breach on average[6]

Industry expectations are such that when security defects are found after an application has been released, they are fixed and published in security bulletins. These releases generate negative publicity and damage to an organization's reputation.

The root cause of these vulnerabilities usually occurs early in the application development lifecycle—because of imprecise and incomplete security requirements, lack of security "fault-tolerant" architecture, or flawed designs. Since these are the fundamental building blocks of an application, they can't be fixed through purely reactive measures, such as security code scans, penetration testing, and other implementation and test activities. However, reactive or no security methodology is the norm across much of the IT industry. Studies have shown return on investment (ROI) results ranging from 30 times to 880 times better[7] with early lifecycle defect detection, compared to later discovery. DXC Comprehensive Applications Threat Analysis (CATA) service provides the proactive means to avoid these defects from the start with industry-leading ROI.

[4] http://pcidsscompliance.net/overview/fines-for-non-compliance, 5 major PCI vendors * $200K penalty each.

[5] Mean total from Table 3 of 2013 Cost of Data Center Outages by Ponemon Institute, http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf

[6] Ponemon 2013 Cost of Data Breach Study: Global Analysis, http://www.ponemon. org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

[7] nist.gov/director/planning/upload/report02-3.pdf, table 1-5

The DXC CATA service

CATA can be applied at any point in the application lifecycle, from new development projects to systems currently in production. While the greatest ROI is achieved by analyzing new projects from the earliest phases of the lifecycle, significant value is obtained by understanding the security readiness of existing applications already in use by the enterprise.

The CATA findings report includes recommendations for identifying deficiencies that can be addressed for existing applications to migrate security vulnerabilities that already exist. DXC developed this proprietary, highly efficient, and effective security vulnerability assessment service to greatly reduce the problem of undiscovered security defects. With conventional applications development methods, only a fraction of vulnerabilities are discovered and fixed before release into production—many are discovered and corrected at a high cost after the fact.

The CATA service provides two capabilities:

Security Requirements Gap Analysis, which identifies often-missed or incompletely addressed security requirements and controls for deploying applications in compliance with common standards such as recommended security controls for:

- Federal Information Systems and Organizations (NIST Special Publication 800-53)
- Health Insurance Portability and Accountability Act (HIPAA)
- PCI-DSS
- Gramm-Leach Bliley U.S. Law (GLB) and others

Architecture and Design Threat Analysis, which provides an architecture-level review, includes a deeper look into the security properties of underlying components, and delivers in-depth recommendations for mitigating elevated risk areas. This review helps enable resilient designs that greatly reduce the likelihood and severity of vulnerabilities, despite inevitable coding defects that may be present in any non-trivial application or system.

The assessment also functions as an independent validation and verification (IV&V) of security requirements and architectural security resilience for any applications development projects.

Benefits of the CATA service

- Enables architecting "secure-by-design"applications by starting with a Security Quality Assessment
- Provides a low-cost, steady-state security quality assessment and improvement approach that can be applied throughout the development lifecycle, minimizing or eliminating rework costs
- Leverages the same superior quality methodology DXC optimized and applied hundreds of times over several years to assess and achieve high-security assurance in our own applications
- Delivers expertise and a superior methodology that gives reviewed applications a much higher security assurance than the industry norm
- Uses a Security Quality Assessment as an IV&V, even when conducted post-release, to validate security quality
- Leverages the expertise of DXC security consultants holding multiple security certifications to include CISSP, CISM, CAP, CSSLP, CISA and others.

Learn more at www.dxc.technology/gov

For more information
Contact your DXC account representative or email: cybersecurity@dxc.com.
www.dxc.technology