Architecture Risk Analysis

Find and remediate weaknesses in your design before they are exploited.

Identify flaws within a system's design to improve your security posture

Half of the software defects that create security problems are flaws in a system's design. Simply scanning software for security bugs within lines of code or penetration testing applications ignores half the problems that leave an organization vulnerable to attack.

Remediate problems early in your SDLC

By performing security early in the software development life cycle (SDLC), you can avoid the costly rework of addressing security defects found later in the SDLC. Most importantly, finding and remediating security problems earlier in the SDLC is less expensive, less invasive, and less time-consuming than waiting until code is written or QA tests are performed.

Get a clear picture of your risks

In an architecture risk analysis (ARA), Black Duck® experts produce a list of technical risks found in your software, and then provide recommendations on the methods, tools, and strategies for mitigating them. We'll also help you understand the related business risks and provide proper mitigation advice to reduce risk to an acceptable level.

Uncover weaknesses in your design

An ARA also reviews your application design in depth to look for weaknesses that might allow attacks to succeed. These design deficiencies are found by analyzing the system's major software components, trust zones, assets, security controls, asset flows, and threat agents. An ARA can discover whether any of your security controls can be bypassed, are weak, or are the wrong controls for what you're trying to achieve.

You'll walk away with a comprehensive list of system options for removing risk completely or mitigating risk to an acceptable level for your business.

How an ARA works

An architecture risk analysis consists of four essential steps.

1. Analyze business context

   We conduct interviews to gather and analyze information to better understand the security risks that impact the business goals of the system.

2. Create a threat model

   We identify major components, assets, threat agents, and security controls that exist in the system, and then create a diagram to capture these entities and the relationships between them.

3. Conduct a risk analysis

   We identify software-based risks and prioritize them according to business impact (e.g., unauthorized access to data or service availability). Activities that comprise our analysis include

   - **Known attack analysis.** We draw from a set of known attack patterns to model subsystem and application behavior for the components in the system being reviewed.
   - **System-specific attack analysis.** We evaluate the foundations of system architecture as it relates to well-established security principles. We also look for unspecified software behaviors with little independent impact that may combine to create critical vulnerabilities.
   - **Dependency analysis.** We focus on peeling back the layers of the software in the platform to understand the security risks introduced or mitigated by each layer.

4. Provide mitigation advice

   At the end of each assessment, we conduct a call with the appropriate development team to review each vulnerability identified during the assessment, answer any questions that the team might have around each vulnerability, and discuss mitigation/remediation strategies.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. August 2024