ca technologies | VERACODE

Getting Started with

APPLICATION SECURITY

77% of applications have at least one vulnerability on initial scan.

CA VERACODE STATE OF SOFTWARE SECURITY REPORT

We are increasingly seeing cyberattackers targeting the application layer. Yet as companies of all sizes and in all industries build, buy, and download more applications than ever before, application security can become a daunting project. However, the application security market has matured to the point that security professionals can follow an established series of action plans to build and scale a program. Where many companies fall down is that they focus on technology and tools to help them secure their applications rather than developing a strategy and program. The simplest framework centers around five basic steps: identification of vulnerabilities, assessment of risk, fixing flaws, learning from mistakes, and better managing future development processes.

Getting buy-in from executives and developers is a critical part of a successful AppSec program.

Find out ***Everything You Need to Know About Getting Application Security Buy-In***

Phase 1

Pilot a program — start small to demonstrate value

The first step toward moving from a reactive program to an advanced program is to create a strategic road map.

STEP 1: MATURITY ASSESSMENTS

Conduct a maturity assessment based on industry-standard frameworks such as OpenSAMM.

STEP 2: DISCOVERY OF THE WEB PERIMETER

Most enterprises don't even know how many public-facing applications they have.

STEP 3: ASSESS MOST CRITICAL VULNERABILITIES

Begin by prioritizing the five to 20 most business-critical applications.

STEP 4: REPORT ON SUCCESS AND OUTLINE NEXT PHASES

Prepare a report that includes detailed information on what was discovered during the pilot phase and describe next steps for further reducing risk.

Find out everything you need to know about application security policies.

LEARN MORE

Phase 2

Set policies and metrics

The organization must first determine what metrics the company wants to use to measure the success of the program and the security posture of applications.

Learn more about how to integrate security into DevOps.

LEARN MORE

Phase 3

Scale to assess all legacy applications and integrate in the SDLC

The most scalable and practical way to ensure all applications built by an organization are assessed for security is to create an assessment process that is integrated into the software development lifecycle.

Note: Don't neglect developer training, a key component of SDLC integration. Learn more.

Find out more about software composition analysis.

LEARN MORE

Phase 4

Create a strategy for assessing third-party components

The most critical aspect of component security is setting policies and standards for what is acceptable to use and tracking the use of components.

Get all the details on these steps in our *Ultimate Guide to Getting Started with Application Security*.

GET THE GUIDE NOW

ca technologies | VERACODE