VERACODE

YOUR JOURNEY TO AN

ADVANCED APPLICATION SECURITY PROGRAM

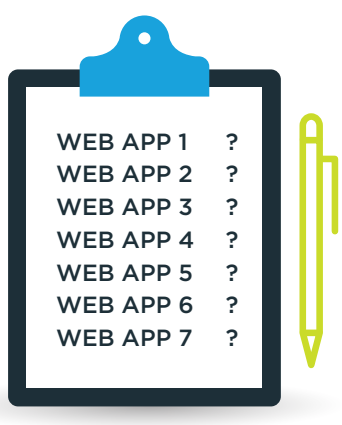
There are an established series of stages most organizations progress through when developing an application security program. Wherever the organization begins its application security journey, the goal should be to mature over time to have an advanced program.

01. Reactive Stage

GOAL: Satisfy requirements

- Mostly manual testing of critical apps
- Remediation of most severe vulnerabilities

Most organizations don't even know how many web applications they have. Veracode recently worked with a global media and technology company that had 100 percent more apps than the company thought.



02. Baseline Stage

GOAL: Understand risk, mitigate vulnerabilities

- Develop accurate view of current state: Use a maturity assessment, such as Open SAMM.
- Gain complete visibility and control over web perimeter: Run a discovery scan of the web perimeter.
- Use a combination of assessment techniques, such as static analysis (SAST) and dynamic analysis (DAST).

03. Expanded Stage

GOAL: Manage risk, lower costs

- Partner with development and DevOps: Ensure assessment protocols do not disrupt the development lifecycle.
- Set goals, and metrics for measuring success.

30x more expensive to fix a vulnerability during post-production than during earlier stages.

ACCORDING TO THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

04. Advanced Stage

GOAL: Reduce risk, accelerate business

- Scale to assess all internally developed apps in SDLC.
- Remediate all vulnerabilities.
- Protect apps in production: Identify and block threats in real-time with runtime protection.
- Create inventory of all components and their versions used in development: Yields an easy way to update a component to the latest version if a vulnerability is discovered.
- Set policies and protocols for purchasing secure apps: Require third-party software to adhere to the same standards as internally developed software.
- Measure and iterate.

ACCORDING TO VERACODE'S ANALYSIS OF

5,300+

Enterprise applications uploaded to its platform over a two month period

24

Known vulnerabilities found in EACH application due to components

For more details on this application security journey, see our new guide, *From Ad Hoc to Advanced Application Security: Your Path to a Mature AppSec Program.*

VERACODE