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.

1

STEP ONE

The Reactive Stage

Goal: Satisfy requirements

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

2

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

STEP TWO

The 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.
- 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.
- Use a combination of assessment techniques, such as static analysis (SAST) and dynamic analysis (DAST).

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.

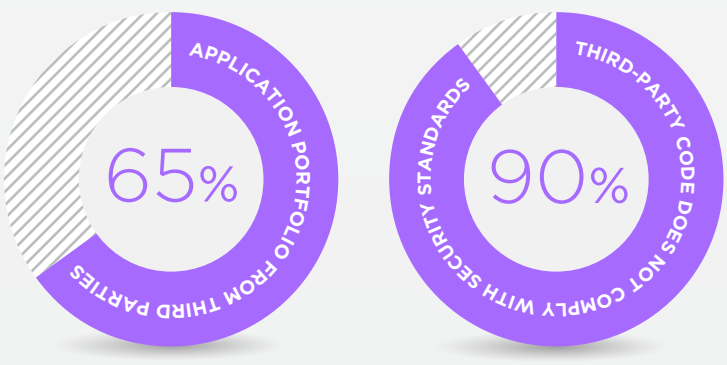
3

STEP THREE

The Expanded Stage

Goal: Manage risk, lower costs

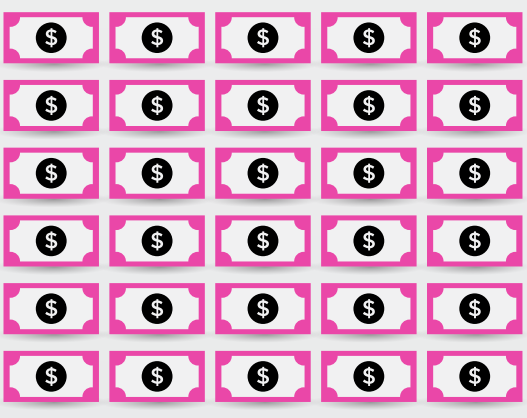
- Set policies and protocols for purchasing secure apps: Require third-party software to adhere to the same standards as internally developed software.
- Protect critical apps.
- Partner with development and dev/ops: Ensure assessment protocols do not disrupt the development lifecycle.
- Set goals, and metrics for measuring success.



ACCORDING TO QUOCIRCA AND A RECENT VERACODE STATE OF SOFTWARE SECURITY REPORT

Sixty-five percent of a typical enterprise application portfolio comes from third parties. Yet ninety percent of third-party code does not comply with enterprise security standards such as the OWASP Top 10.

4



STEP FOUR

The 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.
- Measure and iterate.

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

30x

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

For tips on explaining this application security journey to others in your organization, see our new eBook, *Top 6 Tips for Explaining Why Your Application Security Journey Is Just Beginning.*

VERACODE