CHEAT SHEET

Scaling risk-based AppSec programs

Scaling a risk-based AppSec isn't something that happens overnight — it's an iterative process that evolves alongside the business as an organization grows.

snyk

01 Make a full asset inventory

Build a full inventory of the assets in your application environment. Assets include:

- Source code
- Dependencies
- Container images
- Services
- Endpoints
- Hosts
- Mobile apps
- Developer teams and more

Once the inventory of assets is complete, they should be classified by business criticality. This process can be simplified with the use of application security posture management (ASPM) with its core capability of prioritizing assets based on business-criticality.

02 Identify and measure coverage gaps

Carry out an assessment of your current tooling and services by running a comparison of different combinations of solutions and resulting issues.

- Are there any gaps in coverage? Overlaps?
- Do these gaps/overlaps affect business-critical assets?
- Can you quantify the tools' impact in terms of real risk?

03 Automate as much as possible

- Start by automating your vulnerability scanning and reporting processes to speed up the identification and remediation of issues.
- As your organization scales, automation should include workflows across your engineering and security teams which will allow you to ensure that risk thresholds are not being crossed and policies are being met.

04 Enable developers to succeed

Engineering is the most important stakeholder in reaching a mature, robust AppSec program. To bring them into the program:

- Give developers a prioritized list of security issues — not a to-do list without context.
- Show how their fixes reduce real risk and their impact on the business.
- Give developers security tools that are designed to integrate seamlessly into existing tools and workflows.

05 Celebrate loudly, widely, and clearly!

Build trust and collaboration with engineering by celebrating accomplishments and clearly communicating their value across the org.

- Create reward systems.
- Communicate successes across the entire org (including the C-suite, explaining the impact that it brings.
- Make clear the cost-saving and/or value-adding aspects of each success.

06 Report out to stakeholders

Regularly report on the progress and effectiveness of your AppSec program to build executive trust and buy-in.

- Identify business risk and quantify risk reduction.
- Demonstrate how your team is able to adjust strategies based on data-driven insights.
- Show why scaling your program is business-critical.

Find out how Snyk enables AppSec teams to build, manage, and scale their programs with ASPM.

Learn about ASPM