SNYK CHEATSHEET

5 STEPS TO PRIORITIZE BASED ON RISK WITH SNYK

Keeping up with security can feel like a juggling act, but Snyk makes it easier by helping you focus on what matters.

Follow these five steps to protect your most important application assets and prioritize issues based on the actual risk to your organization.

01

Discover your apps

Before you can start securing your assets, you need to know what assets you have. Integrate Snyk with your SCMs, IDPs, Service Catalogs, and runtime tools to build a complete inventory of your application assets: repos, containers, packages, developer teams, and more. This is your foundation for making informed prioritization and ownership decisions with Snyk.

02

Classify based on importance

Not all these assets are created equal. Use Snyk's policies to classify them automatically based on their importance to your business. For example, your "A" assets might be customer-facing apps or anything with sensitive data, while "B" assets are less business-critical. Similarly, you can use policies to add additional tags that help you better identify assets automatically. Knowing what's important lets you prioritize where to focus first.

03

Manage security coverage

Now that you've got a handle on your software, you can use Snyk to ensure your most important assets are getting scanned for issues (and to identify those that are not). Create policies that define what needs to be scanned, how often, and by which Snyk tool — Snyk Open Source, Snyk Code, Snyk Container, or Snyk IaC. If something's missing, set up notifications to keep you in the know and prepared for the next zero-day vulnerability or incident.

04

Prioritize risk

With Snyk securing your business-critical assets, you're ready to focus on the risks that matter most. Filter your inventory to target specific application assets, such as 'A' assets or those with designated owners. Once you've identified a key asset, the asset view shows issue categories detected by Snyk. From there, the Issues page allows you to prioritize critical problems using Snyk's Risk Score, which factors in exploit maturity, reachability, and more. Runtime context helps you further refine your prioritization with additional factors — such as whether an issue is deployed, loaded into memory, or publicly accessible — allowing you to address the most urgent risks.

05

Provide developers with prioritization and fix context

Great! Now that you better understand your apps and their risks, you and the responsible teams can find and prioritize the issues and vulnerabilities that pose the most significant risks, but the job's not done — you still need to fix the issues. Snyk not only helps find the issues, but it also makes sure your developers have all the info they need to take swift action. Use Snyk's evidence graph to share clear prioritization context behind each issue so they know exactly what to fix and why it's important, with actionable fix advice to reduce risks to your organization. This saves time and helps them address the most critical vulnerabilities first.

Ready to refine your risk prioritization?

BOOK A LIVE DEMO

You know the path to protecting your critical application assets, but you don't have to do it alone.
Book a demo with our security experts to see how Snyk can help you build and enact a custom risk-based prioritization plan.

snyk