Strengthen the supply chain with Software Delivery Shield

So far, you've learned about the software supply chain and how to secure it. The software supply chain includes the people, processes, and tools that play a part in software development. You've also learned about the supply chain levels for software artifacts (SLSA) that outline standards and controls that enhance the integrity of artifacts. Because the supply chain encompasses nearly every aspect of software development, it's important for cloud security professionals to understand the different security considerations organizations should take to defend their supply chain. There are several tools and services that cloud security professionals can use to help manage software supply chain security.

In this reading, you'll learn about Software Delivery Shield (SDS), a Google Cloud service that helps secure the supply chain, and all its components.

Software Delivery Shield

SDS is a fully managed solution that strengthens software supply chain security in each stage of the software development lifecycle.

Software Delivery Shield is a combination of:

- Google's best practices for securing software development
- Dashboards in the Google Cloud console that alert to the security health of resources
- A comparison of your supply chain security to SLSA's guidelines

The combination of these offerings enables customers to quickly assess security concerns that affect their applications.

SDS features

SDS offers many features to strengthen an organization's supply chain. First, part of SDS includes Cloud Workstations, a fully managed service that enables developers to securely access development environments directly from a web browser. Cloud Workstations reduces issues caused by locally stored code, configuration inconsistencies, and code and privacy risks. Storing code in the cloud and using shared repositories improves visibility into source code changes.

Second, SDS automatically generates a software bill of materials (SBOMs), which is a machine-readable list of each piece of software and its components involved in the supply chain. Readily available access to an SBOM provides organizations with a thorough overview of how their software supply chain adheres to security best practices and compliance requirements.

Assured Open Source Software (OSS) is another feature of SDS. Assured OSS improves the supply chain's security by incorporating the same open-source software that Google uses for software dependencies. Organizations can take advantage of trusted OSS packages, explanations of SBOM components, and regularly scanned and improved packages.

SDS supports shifting left

An important part of SDS is that it reinforces the concept of shifting left. Shifting left means implementing security checks and practices at the earliest phase of software development. With this practice in mind, SDS not only hardens your security posture, but also strengthens the DevSecOps workflow.

SDS supports shifting left by helping to secure continuous integration and continuous delivery (CI/CD) pipelines. Cloud security professionals can bolster security by using suggested identity and access management (IAM) policies, virtual private cloud (VPC) guidance, and cloud-native development environments. These practices provide more granular control over resources while also providing a central location to manage IAM and VPCs. And, incorporating these practices align with SLSA guidance to secure artifacts. Implementing these guidelines helps enforce security at different stages of the CI/CD pipeline, which facilitates efficient software updates and deployments.

Key takeaways

The software supply chain has many elements that are crucial to secure. Software Delivery Shield is a service that can help organizations improve security of the supply chain's components. SDS supports shifting left in security by integrating best practices and trusted software packages throughout the software pipeline. As a cloud security professional, you'll use these types of services and tools to secure your organization's software supply chain.