Case Study

aqua

GitLab Uses Aqua Trivy to Provide Customers with Default DevSecOps Container Security

Background: GitLab's Complete DevOps Platform for Modern Software Pipelines

GitLab

GitLab has earned its position as one of the most prominent names in DevOps, providing a complete DevOps platform in a single application to support developers, engineers, and security teams as they focus on innovating and securing applications. GitLab empowers enterprises and small businesses by integrating and automating critical capabilities for development, testing, and deployment. Whether an organization is modernizing its SDLC or fully immersed in CI/CD methodologies, GitLab seeks to elevate the standard for secure DevOps without impeding agility or speed.

The Challenge: Find a Scanning Tool with the Best Ease-of-Use in CI Pipelines and Production Environments

GitLab is on a mission to provide top-notch security capabilities for its DevOps platform. This includes both scanning code before it is shipped to production as well as continuing to scan environments running in production. When GitLab set off to add production scanning capabilities to its offering, it wanted to find a scanning engine that could be used in the CI pipeline as well. To evaluate whether a new path forward could offer better customer value while lowering the work required of GitLab engineering teams, GitLab kicked off a research initiative to compare solutions that might replace its current default CI pipeline scanning tool.

"As far as our engineering time is involved, we can only realistically do tight integrations with a limited number of vendors and maintain those sustainably. We have to prioritize our time and resources around those that we feel like are really going to provide the most value for our customers. So typically, we do a research spike to compare solutions," explained Sam White, Senior Product Manager overseeing the security capabilities that serve GitLab customers in the Protect stage of GitLab.

Integrating open source solutions with its commercial capabilities allows GitLab to achieve the best use of its engineering teams' time. *"We try to leverage as much open source technology out there as we can. We certainly don't want to go reinvent the wheel,"* explained White. For GitLab, open source can help alleviate engineering cycles for other key projects.

"It also makes it possible for us to contribute upstream to those projects and to make those projects better," added White.

When evaluating potential vulnerability scanning solutions, White and the team considered a variety of options. As they refined their approach, they identified critical requirements for adoption.

GitLab's evaluation criteria for vulnerability management and container security solutions included:

- Update frequency of the scan engine
- Accuracy of vulnerability detection and identification
- Features and capabilities of the scanner
- Support for GitLab customer needs
- Support for offline, air-gapped environments
- Ability to scan containers running in production

This criteria helped White and team to establish the short list of candidate solutions, which included Aqua Trivy, to support vulnerability scanning throughout CI/CD pipelines.

> ***When we did compare Trivy, we found that we got really good results, and really timely vulnerability data back. It also had support for offline scanning and offline updates, which we had with our current scanner, and so it was important for us to maintain that capability.***
>
> **Sam White**
> **Senior Product Manager,**
> **GitLab**

The Solution: Aqua Trivy, the “Clear Winner” for DevOps Vulnerability Scanning

When evaluated against GitLab’s selection criteria, White and his team saw some clear reasons to select Aqua Trivy. *“When we did compare Trivy, we found that we got really good results, and really timely vulnerability data back. It also had support for offline scanning and offline updates, which we had with our current scanner, and so it was important for us to maintain that capability.”*

GitLab’s evaluation resulted in a list of key capabilities and benefits of incorporating Trivy into GitLab’s DevOps platform, including:

- Fast, accurate vulnerability data following a scan
- Offline support for air-gapped environments
- Simplified deployment and maintenance with a bundled vulnerability database
- Support for scanning distroless list images, which had been lacking in GitLab
- Built-in support for Aqua Starboard for future expansion to container scanning in production

“Trivy was a leader in the market as far as features, functionality, and capabilities,” White went on to summarize.

> ***“Trivy was a leader in the market as far as features, functionality, and capabilities.***
>
> **Sam White**
> **Senior Product Manager, GitLab**

Aqua Trivy and Aqua Starboard: Automating End-to-End Container Security by Default

The result of GitLab’s evaluation process was to implement Trivy as the default container vulnerability scanner for its Gold and Ultimate customers on version 14.0 and above. This scanning capability runs by default for customers using its DevOps lifecycle tool, Auto DevOps. Auto DevOps seeks to eliminate complexity by automating key aspects of pipeline configuration, integration, and testing.

GitLab has a much broader vision for its customers' security-by-default capabilities. White comments, *"In the containerized world, there are a lot of new concepts to learn. How does networking work? How do your firewall rules work? How do you even do scanning in this world where you've got containers spinning up and going down and things are a whole lot more ephemeral than they used to be? We're looking to help provide that easy button for users, where it's built-in by default."*

Based on this vision, one of the other benefits in choosing Aqua Trivy was its compatibility with Aqua Starboard, a sister open source solution that can run Aqua Trivy in production environments. Early in 2020, GitLab acknowledged an emerging trend for SecOps teams to require their own set of robust security controls to manage vulnerabilities for containers in production, and they needed a way to get risk information into the hands of developers for faster remediation, directly in their DevOps tools.

"Shift left doesn't end when you go into production, so you also need to shift right," says White. *"We need to find and fix container vulnerabilities earlier and also monitor production applications to make sure that those remain secure even after they're deployed."*

What White is looking to provide with Aqua Starboard includes:

- Automatic detection of running containers
- Installation into a Kubernetes cluster
- Container scanning on a schedule, on-demand,or automated as new containers start in the cluster

As GitLab pursues end-to-end container security risk visibility for GitLab users, White articulates a goal to combine Aqua Trivy and Aqua Starboard with other security capabilities in the GitLab portfolio. Doing so would evolve the standard for real-time protection against risks in production. *"Where we really see this headed is: Trivy finds a vulnerability in production [with Starboard]. We then take a look at what that vulnerability is, the nature of it, and we actually... take all of that data and eventually start tying that into our production capabilities around firewall protection and IDS/IPS, to help provide for real-time mitigations or compensating controls to protect things real-time in production. This buys the developers needed time so they are able to go and vet a more formal fix."*

> ***Shift left doesn't end when you go into production, so you also need to shift right. We need to find and fix container vulnerabilities earlier and also monitor production applications to make sure that those remain secure even after they're deployed.***
>
> **Sam White**
> **Senior Product Manager,**
> **GitLab**

The Relationship:
GitLab and Aqua Innovate DevOps Security

GitLab emphasizes strong relationships with its partners and its customers, and values the community support of its end-to-end DevOps platform.

For GitLab, open source is synonymous with innovation. While the GitLab team derives great benefit from community contributions, they pride themselves on giving back. *"When we see an enhancement or we hear a need from our customers that's shared by the Trivy product as well, we can push that upstream into the open source project and make that available for anyone and everyone who's using Trivy, regardless of whether or not they're using GitLab,"* explained White. *"And so, again, that partnership and close collaboration is probably just one other thing that really stood out to us during the selection process that was the icing on the cake."*

> *That partnership and close collaboration is probably just one other thing that really stood out to us during the selection process that was the icing on the cake.*
>
> **Sam White**
> **Senior Product Manager,**
> **GitLab**

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they are deployed. Aqua customers are among the world's largest enterprises in financial services, software, media, manufacturing and retail, with implementations across a broad range of cloud providers and modern technology stacks spanning containers, serverless functions, and cloud VMs.

aquasec.com
contact@aquasec.com
@AquaSecTeam
in/Aqua Security