# Security orchestration leader Demisto secures its AWS-based container pipeline and SaaS offering with Aqua Security

## Customer Overview

Demisto is a leading Security Orchestration, Automation, and Response (SOAR) platform that helps security teams accelerate incident response, standardize and scale processes, and learn from each incident while working together. It combines security orchestration and automation, incident management, and interactive investigation to help security teams meet these challenges and best leverage existing and new security investments.

## The Challenge

As a security software vendor serving security professionals, Demisto must adhere to the strictest security best practices when it comes to how its own software is developed and deployed. Demisto's engineering chose to use Docker containers as a key component of its agile development process. It was important for the engineering team to vet the container images it uses, ensure that they don't contain vulnerabilities, embedded secrets or malware, and that they are configured to run according to best practices. The team also had to be able to be sure that only approved images can be used in production, and get alerted on any new vulnerabilities that may have gone undiscovered previously, but are in use within packages used in its application.

## The Aqua Solution

In late 2017, after vetting several solutions, Demisto chose the Aqua Container Security Platform to secure its container image development pipeline and runtime environments. Aqua was easy to integrated into Demisto's CI pipeline and image registries, where images are automatically scanned using the latest vulnerability data. Demisto was then able to create image assurance policies that control the flow of images from development into production based on various factors that constitute acceptable risk – for example, no images with high severity vulnerabilities can be deployed.

By using the Aqua platform, Demisto is able to integrate security into its container-based development pipeline, and at every stage from image build to container deployment and runtime:

- Scanning CI/CD builds for known vulnerabilities, embedded secrets, malware and open-source licensing issues
- Continuously scanning image registries for newly discovered vulnerabilities
- Image assurance policies that enable the use of trusted images and prevent risky or unknown images from running
- Runtime security policies that use a whitelisting approach to enforce least-privilege behavior on containers
- Real-time monitoring and audit events of any suspicious container activity, new vulnerabilities, host login attempts, and more.

Aqua was also chosen for its compatibility and tight integration with key AWS services that are in constant used by Demisto.

## AWS Services Leveraged

Demisto uses multiple AWS services across two main areas. The bulk of its engineering infrastructure is done on AWS, using Amazon EC2, Amazon ECS and ECR, and auxiliary services such as AWS S3 and CloudWatch. Additionally, Demisto runs a hosted service for its customers, that runs on AWS and leverages AWS ALB.

Aqua's platform integrates with Amazon ECR (Elastic Container Registry) to facilitate image vulnerability scanning and is deployed using Amazon ECS to protect container workloads.

## Customer Benefits

By using the Aqua platform, Demisto is able to secure its container-based development pipeline, leveraging automation to reap the benefits of agile development without introducing unnecessary risk.

Additionally, Demisto has gained visibility into its container stack from development to runtime, keeping tabs on security issues as they emerge:

- Ensuring that security and compliance best practices are continuously applied and enforced
- Preventing and monitoring unauthorized access to its containerized environment
- Identifying issues early in the development cycle to ensure fast remediation and avoiding security incidents in production