Moogsoft Uses Deepfactor to Achieve Shift-Left Container Security

// About Moogsoft

Moogsoft, a pioneer of AIOps, helps ops teams collaborate, automate, and remediate. Designed to aggregate your entire monitoring and observability stack, Moogsoft streamlines your incident management lifecycle. Founded in 2012, Moogsoft has more than 140 customers worldwide including American Airlines, Fannie Mae, Fiserv, HCL Technologies, SAP SuccessFactors, and Verizon Media.

"The Moogsoft mainline product known as Moogsoft Cloud is primarily deployed through EKS, or Elastic Kubernetes Service, in AWS or Amazon Web Service infrastructure. We utilize a CI/CD pipeline to appropriately test, monitor, and deploy containers in an incremental fashion to ensure that the service is consistently up to date."

moogsoft

CUSTOMER:
Rex Steele,
Senior Security Engineer

INDUSTRY:
AIOps Software Solution

VIDEO:
https://www.deepfactor.io/moogsoft-uses-deepfactor-achieve-shift-left-container-security/

// Why Deepfactor: Providing an Integrated DevSecOps Approach with Unique Runtime Analysis and Usage Context

Moogsoft chose Deepfactor because of its integrated approach for software bill of materials (SBOM), software composition analysis (SCA), and runtime security. Deepfactor scans containers for vulnerabilities, detects vulnerable behaviors in running containers, and correlates SCA scan results with runtime analysis to both:

- Reduce alert fatigue by prioritizing CVEs that are in used packages.
- Burn down CVE debt intelligently by removing packages that aren't used.

> "Moogsoft engaged with the Deepfactor platform due to the diverse set of offerings that it enables us to engage with and implement into our pipeline process, particularly the deep inspection of the runtime and the various dependencies throughout our product. Deepfactor allows us to really get a fine-grained analysis of not only what was being used but how it was being used."

—REX STEELE
SENIOR SECURITY ENGINEER MOOGSOFT

// Understanding Supply Chain Risks Using SBOMs

Modern applications rely on open source and third-party software for a majority of their code base. Many of those software building blocks come with vulnerabilities and license risks that organizations must manage to avoid supply chain security incidents that can result in data breaches. Software Bill of Materials (SBOMs) improve supply chain security by maintaining inventories of software components and dependencies used to build and deliver applications.

Moogsoft used Deepfactor to produce, operationalize, and consume SBOMs as part of the software development lifecycle (SDLC). The Deepfactor portal produces SBOMs in industry-standard formats (SPDX, CycloneDX) and provides a searchable and filterable human-readable interface to help security teams quickly respond to zero-day vulnerabilities, developers fix vulnerabilities, and customers verify the supply chain security of their software.

"One of the most useful tools that we found within Deepfactor was the analysis of the SBOM, which enabled me to have meaningful conversations with my engineers and developers around what was being utilized in the product and what actually needed to be there. Then take that information and have conversations with our customers around why we had certain packages or dependencies within our product and the way that we were utilizing them."

// Shifting Left to Find Security Risks Before Production

To proactively address security risks, the Moogsoft security team decided they wanted to shift security left into their dev and test environments so they could identify security vulnerabilities and potential supply chain security issues before Moogsoft applications were shipped to production. By identifying security issues early and understanding their software supply chain, Moogsoft can reduce the risk of a vulnerability being exposed in production, lowering the total time required by engineering to address the issue, and accelerating release cycles by avoiding failed builds.

> "In resolving security issues, particularly those in a development state, the security team helps to manage the identification and facilitate the monitoring of the tickets as these are being processed in communications with the engineering and development teams to resolve these issues. Ideally, with the continuing shift to the left, the security team will help to facilitate the setup and continuation of tools, and enable the development and engineering teams to engage with these tools directly and resolve security issues without continuous oversight from the security team."
>
> **—REX STEELE**
> SENIOR SECURITY ENGINEER, MOOGSOFT

// Slimming Down Applications and Burning Down CVE Debt

Often, applications are built with additional packages that are downloaded with container images or open-source components. When applications have unnecessary components, it adds to the risk surface of the application, increases the time required to maintain the application, and can reduce performance or consume resources. Slimming down applications to only the required components reduces risk and can improve the application itself.

Deepfactor correlates SCA scan results with runtime analysis to identify vulnerabilities in both used and unused packages. When a vulnerability exists in a used package, it is assigned to a developer to be fixed or updated based on the criticality of the issue. If there is a vulnerability in a package that is not used, the engineering team can consider removing the package in the next build or switch to a different base image to eliminate the known vulnerability.

// Integrating Deepfactor into Security Reporting and Correlation

Deepfactor's variety of integrations with tools including Jira, Slack, and extensive REST APIs make it easy for security and engineering teams to consume the security alerts and information provided by Deepfactor.

In addition, Deepfactor offers an HTTPS webhook. Moogsoft used Deepfactor webhooks to notify their internal security dashboard when certain events occurred in Deepfactor. Using a webhook for integration meant that Moogsoft didn't have to periodically poll Deepfactor (via the REST APIs) to determine whether any changes had occurred in their security posture.

> "We were able to use the Deepfactor webhook to integrate into the Moogsoft AIOps platform, which we also utilized for internal purposes, specifically for security. With this, we were able to forward all alerts from the Deepfactor platform to our own platform, and then utilize that to help correlate against other alerts we were receiving from other security and monitoring tools. The Deepfactor development team was extraordinarily responsive and more than happy to work with us on configuring the webhook so that we could get the most value possible out of Deepfactor."

—REX STEELE
SENIOR SECURITY ENGINEER, MOOGSOFT

> **Deepfactor Recorded Demo:** This **short demo video** gives an overview of the Deepfactor Developer Security features and capabilities.

> **Deepfactor Personal Demo:** **Request a demo** so you can see how the Deepfactor developer security platform can help your team ensure secure code.

> **Deepfactor SaaS Free Trial:** Sign up for a **free trial** of Deepfactor SaaS.

{deepfactor}

Deepfactor is a developer security platform that enables security and engineering teams to quickly discover and resolve security vulnerabilities, supply chain risks, and compliance violations early in development and testing.
For more information, follow Deepfactor on **Twitter** or **LinkedIn** or **contact us**.