Inspide Gets Developers to Buy Into Security By Reducing Friction

inspide.

CUSTOMER:
Daniel Carrión, Chief Technology and Product Officer

INDUSTRY:
Geo-intelligence Applied to Mobility and Marketing

VIDEO:
https://www.deepfactor.io/inspide-gets-developers-to-buy-into-security-by-reducing-friction

Inspide provides geospatial data that connects cars and analyzes traffic data to improve fleet management and road safety. In 2020, Inspide expanded the scope of their platform to include telecommunications data, enabling Inspide to disrupt the omnichannel and outdoor digital advertising industries by enabling out-of-home advertisers to measure and target their consumer audiences.

// Building Security into a Cloud Native Application

Portall is a cloud-native technology hosted in AWS Frankfurt to ensure sensitive data remains in the European Union. The application is entirely containerized, uses the AWS Elastic Kubernetes Service, and has a backend written in Python. Inspide initially relied on penetration testing and the diligence of their developers to ensure the application was free of critical vulnerabilities. After moving to adding telecommunications data to their system, Inspide set out to implement DevSecOps practices to ensure that secure coding practices were applied consistently and that all code put in production was free of security vulnerabilities.

> "We had invested a lot in security from the point of view of the network or the site reliability engineers, but never from the software developer's perspective. Before Deepfactor, searching for vulnerabilities in our application was something that was done manually by each developer and it heavily depended on how strict those developers were at that moment in time. It was manual and it was inconsistent across all of our applications and services because it heavily depended on this individual developer."
>
> **–DANIEL CARRIÓN**
> CHIEF TECHNOLOGY AND PRODUCT OFFICER, INSPIDE

// Using Deepfactor to Automate DevSecOps

Inspide chose Deepfactor because of its ability to automate and accelerate the process of finding and fixing security vulnerabilities, supply chain security risks, and compliance issues early in development and testing. When developers add a container to their repository or check in code, they automatically get a slack message if there are any security risks present in any of their container images, application code, open-source components, or APIs.

According to Daniel, “Developers are happy with fixing things, but you have to make it easy for them. So one of the great things about Deepfactor is that as soon as someone uploads a Docker image to the repository, on our Slack channel they get all the alerts regarding the vulnerabilities that Deepfactor has found. That’s just one step, but it’s a very big step for them because they can very easily see what’s wrong with their image and fix it even before going beyond the deploying process.”

// Runtime Security Was Eye Opening

While Inspide uses all of the Deepfactor capabilities, the runtime security analysis was the most eye opening and provided a different perspective on security vulnerabilities and how their applications worked in practice. Vulnerabilities such as processes running as root, privilege escalation, secrets management, and remote code execution are difficult to detect and time-consuming to root cause without Deepfactor.

“We only looked at runtime in terms of performance analysis, but never in terms of security analysis, and that has changed,” said Daniel. “So with Deepfactor, the types of vulnerabilities that we’ve suddenly become aware of are the runtime ones. For instance, you could assess whether a process was going to be running as root or not by looking at your Docker file, but we would never really confirm that the process wasn’t running as root and that no other process were running as root.”

// Eliminating Friction to Get Developers to Buy into Security

Developers at Inspide have varying levels of security knowledge and desire to proactively seek out security vulnerabilities. The site reliability engineering team has a high degree of security knowledge but focuses on protecting the applications in production. The software developers had a wide range of security expertise but were willing to make the effort to fix vulnerabilities quickly when identified. Given the level of security at Inspide, some security measures can cause friction and context-switching that makes it challenging to get developers to buy into security initiatives. Inspide took the approach of automating the detection of vulnerabilities, while reducing friction by providing alert information in their existing tools such as Slack.

> “Suddenly, with Deepfactor, developers have a way for them to improve how they deal with security that doesn’t generate a lot of friction. Security has become a first-class citizen to developers as compared with security being a first-class citizen only for the paranoid SRE team. We’ve really seen an improvement after we started using DeepFactor.”
>
> —DANIEL CARRIÓN
> CHIEF TECHNOLOGY AND PRODUCT OFFICER, INSPIDE

// Preparing for Compliance and Certifications

Inspide has not yet gotten to the point where they need to meet stringent compliance or regulatory requirements. However, they anticipate the need to obtain certifications such as SOC 2 Type 2 and ISO 27001 that require audits of applications' security, development practices, and infrastructure. The ability for Deepfactor to give the engineering leadership and individual developers the compliance implications of each vulnerability puts Inspide in a position to proactively avoid any potential compliance issues as they prepare for future certifications.

> "We're a small company and so far we haven't really had to get any type of security certifications, but we know that eventually we will have to, and it's not really embedded in our culture to understand how all the certifications work, all the different certifications that we have, and how all these vulnerabilities are classified. And suddenly we have a tool that basically sheds a lot of light on top of all that and we are comfortable talking about SOC 2 Type 2 and other compliance requirements."
>
> **—DANIEL CARRIÓN**
> CHIEF TECHNOLOGY AND PRODUCT OFFICER, INSPIDE

Watch the full Inspide customer testimonial here >

For those interested in Deepfactor after learning about Inspide's success story, consider getting started with the following resources:

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

> **Buyer's Guide:**
The **Developer Security Buyer's Guide** outlines the top 5 areas to consider when evaluating developer security platforms.

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

{deepfactor}

Deepfactor is a developer security platform that enables 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**.