MEND

Mend Helps A Large Financial Firm Address Spring4Shell in Hours

About The Company

A large investment research firm that provides analytics and governance tools to institutional investors and hedge funds. Approximately half of their 4000 employees are involved in some way with either software development or IT operations. There are a total of 60 people on the cyber security team, including 3 people who are responsible for application security.

The Challenge

Before the Spring4Shell announcement
In 2020, the company decided to adopt modern DevOps methodologies across all their business units to improve speed of application delivery, quality and reliability. Around the same time, the security team chose to standardize on Mend SCA for open source software security. By early 2022, Mend application security tools, including Mend SCA and Mend Renovate, were deployed across thousands of software projects spanning hundreds of repositories.

The Executive Director of Cyber Security knew that a good security program encompasses people, process and technology. He built his company's application security program on three main pillars:

· **People**: "You need empathy for what the developers' lives are like. We give our developers the information and the tools that they need to do their jobs, and we ensure that each DevOps team has a security SME. The goal should be familiarity, not mastery."

· **Process**: The Executive Director of Cyber Security knew that communication of software vulnerabilities has to take place at DevOps speed. To achieve that, his team integrated Mend SCA with the company's Jira ticketing system. For the few development teams that were not using Jira, they set up Mend to trigger a daily email report.

· **Technology**: The company uses automation to trigger real-time testing with Mend SCA and Mend Renovate. This is designed to reduce friction and to "industrialize" the process as much as possible. According to the Executive Director of Cyber Security: "It is not reasonable to expect developers to constantly be working with separate security tools. So we try to make Mend as invisible as possible. Thanks to Mend's various integrations and automations, we have been able to accomplish this."

The Mend Solution

Day Zero
On March 31, 2022, CVE-2022-22965, also known as the Spring4Shell vulnerability, was announced. This caused Mend SCA to send alerts via Jira or email to all software developers working at the financial software firm whose projects were impacted.

The Executive Director of Cyber Security explains: "For us, March 31 was not an emergency. We had refined our Zero Day processes just three months before, thanks to the Log4j drill. So everyone knew what to do. We had situational awareness within just a few hours. That was key! We knew which applications were priorities to address. Our IT staff applied mitigations to all the applications that needed them, and our developers were already working on applying the fixes."

Many developers relied on Mend Renovate to automate the pull requests to fix their vulnerable dependencies. Teams that had implemented automated testing did very well, whereas teams that were not as far along on their DevOps journey and had less automation took a bit longer.

> *"It is not reasonable to expect developers to constantly be working with separate security tools. So we try to make Mend as invisible as possible. Thanks to Mend's various integrations and automations, we have been able to accomplish this."*

The Results

According to The Executive Director of Cyber Security, "With Mend in place, and with the automation that we had designed, our developers were able to turn everything around in a matter of hours. After that, it was just another day."

Related Resources

Learn more at www.mend.io