State Government Rolls Out a Scalable Application Security Program in One Year

State of Missouri scales AppSec program to 365 applications and 14 agencies.

PROFILE

Company
State of Missouri

Industry
Government

Location
Jefferson City, MO

HIGHLIGHTS

- Ramped up AppSec program to reduce risk for 360+ applications in 14 state agencies
- 18,000 flaws fixed in first 8 months and 28,000 flaws fixed in the first year
- 132,000 flaws fixed and 10,700 flaws mitigated since April 2014
- Developers embrace feedback from scans and consultation calls

SUMMARY

Amid rising data breaches in recent years at governments from the local, state and federal level, the Governor, Legislature and the CIO of the State of Missouri all recognized cybersecurity as the state's top IT priority, including application security testing. With Veracode's cloud-based service and policy-based approach, the state launched a comprehensive application security program, fixing over 28,000 flaws in the first year alone, and scaled to 360+ applications within three years.

THE CHALLENGE

Preventing Data Breaches and Ensuring Compliance

Amid rising concerns about data breaches affecting millions of taxpayers, with full support from all branches of the Missouri Legislature, the State of Missouri CIO established cybersecurity as the number one IT priority. Application security testing became a significant focus of the cybersecurity initiative, alongside security training for developers and end users, and implementation of data loss prevention tools.

Although the state had an existing tools-based approach to application security testing, only one of 14 state agencies with IT departments administered through the Office of Administration Information Technology Services Division (ITSD) was thoroughly using the scanning software. Nikki Veit PMP, GSSP-NET, came on board in 2011, and now manages the application development (AppDev) security oversight team.

When Nikki started, the existing application security solution was used only sporadically, and it was running on a Windows XP workstation that needed to be upgraded. As Nikki waited for an upgrade, she scanned one application using static analysis. After four hours of scouring 1,200 vulnerabilities, she discovered that every single one proved to be a false positive. "At this rate there was no way we could make developers use this." Nikki said. "It would just be a waste of time. We needed a better way." Nikki got the OK to find a better application security solution.

THE SOLUTION

Veracode Application Security Platform and Services

Nikki's team evaluated application security testing solutions, ultimately selecting Veracode for its comprehensive offerings and services-based approach. "We looked at the Gartner Magic Quadrant and identified other tools that would fit our environment," Nikki said. After a proof of concept with Veracode, "we were scanning that same day or the next day," Nikki said. "It was really easy."

ca technologies | VERACODE

"In the first eight months, we had 18,000 flaws fixed. It was just phenomenal."

Nikki Veit

Since April 2014,
THE PROGRAM HAS SCALED TO...

365 applications

4,500 scans

132,500 flaws fixed

10,756 flaws mitigated

With an initial goal to implement a program for 100 applications in the first six months, Nikki began onboarding development teams across the 14 consolidated agencies, starting with a single application for each team. The teams made progress much faster than expected, and the program had expanded to assessing 150 applications, fixing 18,000 flaws in eight months and 28,000 flaws in the first year alone.

Getting Started

In partnership with the state's cybersecurity team, Nikki established a group to determine security policy. The AppDev security oversight team is responsible for setting standards and security policies, and driving AppDev security initiatives. A Veracode Customer Success Manager helped the AppDev security team implement a centralized, policy-based program with consistent policies, metrics and reporting.

"When we first started scanning, there were a lot of noncompliant applications," Nikki said. "But [Veracode] was really easy to use, and developers were able to go in and scan early and often. In the first eight months, we had 18,000 flaws fixed. It was just phenomenal."

In the first year, the teams used Veracode's recommended policies based on business criticality of applications. Using Veracode's comprehensive reporting, the AppDev security oversight team provides regular reports to upper management. "This lets us know where to praise and where to invest more time," Nikki said.

Expanding the Program

Within a year, the AppDev security oversight team determined that the development teams were doing well, with many applications becoming compliant, but they could do even better. The oversight team wanted to require higher scores to be compliant. To transition the teams to higher scores, development teams were invited to participate, but within a year the stricter policy would become a requirement. With comprehensive policy compliance reporting, Nikki's team can quickly review reports to see where the flaws are and review how to mitigate those flaws in AppDev meetings.

In the second year of the program, the AppDev security oversight team decided to expand the program to non-consolidated agencies, and two more agencies have since joined the program. "The platform makes it simple to add other teams to our account," Nikki said.

Nikki continues to look for ways to improve the security posture and automate application security. Some of the development teams have taken the initiative to create scripts that automatically uploads binaries to Veracode whenever they do a build. In 2017, the AppDev teams plan to start integrating automated scan processes with Team Foundation Server. "Veracode APIs make it easy for our AppDev groups to take the tool and run with it," Nikki said.

The AppDev security oversight team has begun integrating security requirements as part of the RFP (Request for Proposal) and PAQ (Project Assessment Quote) processes. New software products must be compliant with internal policies. "Now we have a way to ensure code that we purchase meets our same internal standards," Nikki said.

"When I talk to people about Veracode, I talk about the ease of use and the rollout. As compared to on premise options, the startup time is in minutes. And it's easy to use by the developers because it makes it easy to fix the flaws. It's been a huge success."

Nikki Veit

THE RESULT

AppSec That Works for Developers and Security

Veracode's ease-of-use helps ensure that developers buy into the program, and Veracode APIs for decentralized scanning puts a lot of control into the developer's hands. Once a developer has access, they can use Veracode right within their developer environment and scan as often as they want. "The plugins that work with the IDEs make scanning and reviewing even easier," Nikki said.

Some developers are using Veracode Developer Sandbox for scanning pre-production applications against the policy to get feedback without setting off reporting or alerts. Some developers like to use it when they're not ready to publish yet," Nikki said.

To provide training and support for developers, each agency has a security lead to ensure their teams are following security best practices. These security leaders received specialized security training in the first year of implementing the program. Each year, additional team members receive the specialized training. In 2016, all developers received general security training that covered the OWASP Top 10.

The AppDev teams can also lean on Veracode expertise to answer their toughest questions and review the results of their scans on consultation calls with Veracode experts. Although at first some developers can be a little intimidated about showcasing the flaws in their code, they quickly begin to embrace the idea of openness with their code. "I see [consultation calls] as a great opportunity for our team to increase their knowledge in security, which has been awesome," Nikki said.

WHY VERACODE

Nikki said Veracode was the best choice for an applications security solution, for ease of use and quick rollout. Nikki pointed out a host of other reasons why the State of Missouri has had such success with Veracode.

- No infrastructure to manage
- Monthly updates to the Veracode Application Security Platform
- APIs to enable developers to scan their own code
- Consultation calls for developers
- Fast scan results for most applications
- Low false-positive rate
- Ease of implementation and adding applications
- Comprehensive compliance reporting

"As compared to on premise options, the startup time is in minutes," Nikki said. "And it's easy to use by the developers because it makes it easy to fix the flaws. It's been a huge success."

CONTACT US

Learn more at WWW.VERACODE.COM on the Veracode blog and on Twitter.

Veracode, CA Technologies' application security business, is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets – whether that's software they make, buy or sell. Veracode serves over a thousand customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks and more than 20 of the Forbes 100 Most Valuable Brands.

ca technologies | VERACODE