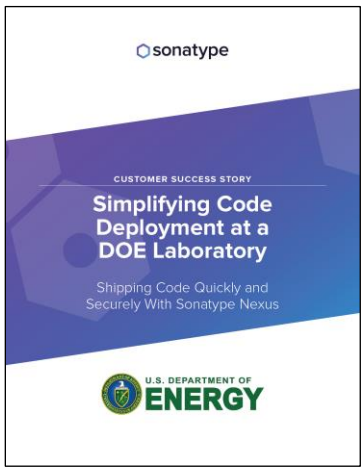
carahsoft.



Simplifying Code Deployment at a DOE Laboratory

Shipping Code Quickly and Securely with Sonatype Nexus

Thank you for downloading this customer success story. Carahsoft represents proven DevSecOps solutions, delivering agencies the innovative solutions needed for every phase of the DevOps and DevSecOps lifecycles and with security built-in every step of the way. These solutions provide support for collaborative planning, rapid code builds, iterative testing, rapid release, optimized deployment and ongoing monitoring that continuously feeds into the next wave of planning.

Carahsoft combines extensive knowledge of the technologies we provide with a thorough understanding of the government procurement process to analyze needs, provide configuration support, simplify the ordering process, and offer special government pricing. Speak to a Carahsoft representative today about achieving your DevSecOps objectives.

For more information, contact Carahsoft or our reseller partners:
carah.io/solve/devsecops |devsecops@carahsoft.com | (703) 871-8570

sonatype

CUSTOMER SUCCESS STORY

Simplifying Code Deployment at a DOE Laboratory

Shipping Code Quickly and Securely With Sonatype Nexus

U.S. DEPARTMENT OF ENERGY

No matter what industry you work in, it's a challenge to ship code quickly. Every business needs to verify that code does what it says and doesn't break anything. That need goes up to a whole different level when you're dealing with nuclear weapons. That's the reality for a DOE Laboratory and its Program Manager (PM).

Struggling to Ship

The teams supporting the DOE Laboratory found that they would write some code, but the lengthy security process would make shipping that code challenging. As the PM notes "It became an issue that nearly shut the organization down. Our security teams were on approval cycles that sometimes took as long as six months."

"It became an issue that nearly shut the organization down. Our security teams were on approval cycles that sometimes took as long as six months."

— PROJECT MANAGER FOR A U.S. DEPARTMENT OF ENERGY LABORATORY

For a developer, looking at a code approval timeline of six months is excruciating. Receiving feedback that some bit of code you wrote months ago didn't pass security reviews requires an extremely costly context switch. Then, the new code would need to re-enter the security pipeline, sometimes taking weeks or months for new approvals.

Shifting Security Left

The PM knew that he needed to decrease the time between writing code and evaluating it for vulnerabilities. He also knew that it would need to meet the stringent quality requirements demanded by a laboratory studying nuclear energy.

That's where Sonatype's Nexus Platform came in. By using Nexus, teams were able to verify the security and quality of the libraries they were integrating into their code before they shipped it. They were able to prove Nexus' quality to the security evaluators within the organization, which meant a reduction in the level of scrutiny applied to new code. Nexus helped carry the load for security engineers so those engineers could focus on finding more obscure vulnerabilities and leave the easy stuff to the Nexus software.

Nexus helped carry the load for security engineers so those engineers could focus on finding more obscure vulnerabilities and leave the easy stuff to the Nexus software.

The end result was that some security reviews went from taking weeks down to just a few hours. Teams enjoyed a reduced time to ship, which meant that they could deliver more critical features to research teams.

Proving Value From Day One

While developers acutely felt the challenges presented by these long security checkpoints, the PM knew that he couldn't change everything all at once. "I can see why it took us so long in our government environment," he noted. "Because if I had told the people on my team that we were

doing all this... and we were starting on day one and in a couple of months, here's where we needed to be — they all would have quit."

Instead of trying to turn over every leaf at once, the PM took a more measured approach. He looked at each piece of the process he wanted to introduce and added them one by one. Then, he gave each tool some time and space to work and to let the team acclimate to them. This approach meant that the group learned to see how the tool would help their workflow once they'd gotten used to the new system.

As each tool was added, the PM would sit down with a team and ask them what kind of results they saw with their changed workflow. The responses were always positive.

By introducing the tools to teams and letting them see the value, the manager found leaders who would share how much value they saw with other teams. Instead of a top-down mandate, this became a grassroots effort.

Cultivating Leaders Within Teams

Some of the changes hit home with certain developers more than others, though. "I had one or two developers who really, really became DevSecOps practitioners. The story started getting out within our organization and within our group," the PM shares. By introducing the tools to teams and letting them see the value, the manager found leaders who would share how much value they saw with other teams. Instead of a top-down mandate, this became a grassroots effort.

Those evangelists spread the good news of DevSecOps to the rest of the organization. Before long, teams were coming to the PM with extra money in their budgets, asking him to scale his work up to their group, too. What had started small grew rapidly because it provided so much value to the teams who picked it up.

Fitting In, Not Running Over

As the DevSecOps mentality spread throughout the organization, the PM noticed another major benefit of Sonatype. When he'd originally introduced these changes, it was just to one team. He knew how the tools would integrate with their workflow.

Once other teams started scaling up DevSecOps work, he found that they weren't working the same way as the team he'd started with. He anticipated that this would lead to challenges—that different workflows would feel clunky integrating with Sonatype tools to provide value.

Instead, the opposite was true. There was no need to worry about those integration touch points. Developers were able to configure Nexus integrations with the other technologies in their stack themselves. "They designed and set all that up themselves because I wanted them to be comfortable with it," the PM explains. "We had a meeting in our DevSecOps community a couple months ago. Different teams are actually working with their source code and the repositories and the way they're merging and branching and they're releasing and all that. There are five or six different ways that teams are doing it."

sonatype

Each Team With Their Own Pace

Because the PM was able to connect teams with the Sonatype Nexus Exchange, they were able to connect with plugins to suit their specific workflows. This meant that each team found that integrating with Sonatype didn't mean upending their entire workflow. And because each group was able to configure their installation themselves, they felt greater ownership over the final product. Adding Sonatype Nexus meant a new step in their workflow, sure. But that step demonstrated value quickly and didn't upend the way that the team worked.

The end result was a product that, once installed, quietly and unobtrusively helped development teams ship higher quality, more secure code. Other teams, noticing the benefits hopped on the train, and quickly found themselves right at home with Nexus in their workflows, too.

Sonatype Nexus: Transforming How a DOE Laboratory Ships Code

The PM isn't someone who went out and got fancy training in DevSecOps. "I went down the path of self-teaching. Without that, I wouldn't be where I am today. I'm not a developer, but I know that with the right tools, I can make development easier for our developers," he explained.

In using the Sonatype Nexus Platform, the PM built a new process that identified security issues and code problems earlier than ever before. Because the tool was reliable and comprehensive, that meant his teams could cut down on the time code needed for security reviews. That decreased cycle boosted his team's productivity and made developers happier. Those happier developers shared their success stories with other groups, and from there the changes flourished. Because Nexus was so easy to integrate with various tools and workflows, each of those teams found value quickly and easily.

While there were some unique challenges working with nuclear research labs, the solutions the PM found fit the organization's mission needs. DevSecOps provided a framework that simplified their code deployment and delivered on just that, using Sonatype Nexus. Now consider, how could Sonatype help your business?

Visit www.sonatype.com/customer-success to see how other customers automate open source security.

sonatype

Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype's Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit Sonatype.com, or connect with us on Facebook, Twitter, or LinkedIn.

Headquarters
8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place, Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com