COLORADO

Governor's Office of Information Technology

DevSecOps: Securing Applications & Ensuring Quality

CATEGORY:

Enterprise IT Management Initiatives

STATE:

Colorado

PROJECT INITIATION DATE:

May 1, 2019

PROJECT END DATE:

June 30, 2019

NASCIO STATE IT RECOGNITION AWARDS

Brandi Wildfang Simmons | Chief Communications Officer
brandi.simmons@state.co.us | 303.764.6897

Executive Summary

Colorado's Governor's Office of Information Technology (OIT) provides technology services and solutions for executive branch agencies and offices of the Governor. Work to update legacy systems and implement new solutions is continuous throughout the year. The DevSecOps program brings operations and development together with security functions via an Agile development team. It was established in 2017 with the primary goal of creating a culture and practice of collaborative, repeatable, sustainable, quality deployments of technology services and products. But in its inaugural year, without any dedicated resources or funding for tools, the program struggled to gain traction across the many OIT teams located around the state, often within the agencies they serve. The teams often operated in silos within those agencies, creating a lack of efficiency in solution implementation.

The DevSecOps program was officially launched in 2019 with executive sponsorship and limited staff with the charter to evolve siloed behaviors into innovative, collaborative practices that consistently deliver desired and predictable customer outcomes through a faster solution implementation methodology. The initiative, **Azure DevOps MVP Implementation,** focused on procuring and configuring the Azure DevOps toolset to create a secured single repository for all Colorado state code with an automated, continuous integration and continuous delivery (CI/CD) template. The minimum viable product (MVP) implementation focused on creating automation, a self-service onboarding toolset for code migration, and CI/CD standardized practices with a goal of steadily increasing automation and security practices across OIT teams. In essence, it was a maturing of OIT's DevSecOps program to provide the tools and path forward to secure applications and ensure quality application development across the agencies and offices that OIT serves.

The result is a repeatable, automated process that is greatly improving OIT's delivery cycle and Cloud offerings enabling better utilization of analytics and team collaboration. All measurements, from the number of users to the number of tracked work items, have increased significantly and continue to do so in 2020. As an example, security scans increased 40% by the end of 2019 and are trending upward. Dozens of teams have created efficient processes through the DevSecOps program, increasing the security and timeliness of IT deliverables to our agency customers.

Project Narrative

Concept

Adding or changing new technology products and websites for the State of Colorado is often a highly manual process without automated, enforceable quality and security gates. Errors found when performing security reviews at the end of a project after the majority of development was completed resulted in launch delays and increased costs.

In one instance, two years of development to modernize a system had taken place before a single code security scan. When the pre-go-live security scan was performed it detected more than 10,000 vulnerabilities, which required mitigation and caused the delay of multiple releases. This impact to the customer resulted in low satisfaction with OIT, prevented development/deployment teams and the supplying vendor from moving on to other priorities, and frustrations ran high. The outcome emphasized the need to modernize solution and delivery at every touch point—improving efficiency, decreasing overhead, and supporting rapid value delivery to achieve OIT's goal of customer delight by exceeding expectations.

The DevSecOps program was already focused on a strategy of ***Securing Applications and Ensuring Quality*** and followed these general guiding principles:

- Risk and errors are reduced by injecting quality, security, and standards upfront to make each step more consistent and repeatable.
- Changes are broken into smaller increments that make them easier to track, verify, roll back, and troubleshoot.
- Faster feedback loops and delivery enable greater alignment with business objectives.
- Increased collaboration and cohesion among OIT teams, with more time spent innovating and building new solutions, leads to increased employee satisfaction and engagement.

The program identified several issues that stood in the way of implementing these principles for improved service delivery and security, including:

- Development and operations teams working in isolation across 17 state agencies.
- Separate tools, processes, and practices among teams of the same and different specialties but who worked in different locations created silos, isolation, and disunity.
- Disparate, unmanaged, and insecure solutions for code storage, password management, and development workflows resulted in no coherent method to protect and organize state intellectual property.
- Programmatic and systematically enforced standards or controls had not been established for quality assurance testing, user acceptance testing (UAT), change management, environments, performance, code quality and security (Veracode) scans, or the security of many state assets.
- Advanced security practices were lacking from design to delivery.

- Customer experience across the organization is inconsistent and outcomes are unpredictable.

The Azure DevOps MVP initiative addressed these issues by assembling all of OIT's code in one place in the Azure DevOps toolset and steadily increased automation and security practices across OIT teams. The desired result was to increase efficiency, security, and quality across the technology and service delivery lifecycle by shifting "left" security and quality so they would be automatically addressed earlier in the solution delivery process and lead to increased efficiencies through automation and cultural changes.

Part of the shift left process began in 2015 with OIT's Application Security program and the purchase of a secure code analysis tool to help shift securing applications to an earlier position in the development lifecycle. The initial adoption of the tool by development teams was only moderate as depicted in the graph below. With the implementation of the Azure DevSecOps MVP initiative to enable secure code analysis scans to run automatically, adoption steadily rose as applications started regular automatic scanning.

Flaw Resolution Activity

To increase awareness and encourage adoption of the DevSecOps strategy, Azure DevOps toolset, and the larger culture and practices, a change management and communication strategy was adopted. The strategy includes the use of a website; a wiki; dashboards and kanban boards of progress; a monthly email newsletter with helpful information like DevOps terms explained, ideas and progress; frequent large group presentations and training; a monthly community of practice sharing session; and a monthly meeting with DevSecOps champions. For adoption of specific technical practices, like migrating code, security scanning and gating releases, a self-service approach was taken. By focusing on the quick delivery of onboarding guides, templates, a sandbox environment, short demos and Q&A sessions, teams were given resources that allowed them to implement changes gradually alongside their existing feature and fix backlogs.

Once the initiative was implemented, the program began measuring success in adoption counts, number of flaws found and mitigated, number of scans, number of code sets secured, and number of code sets automated.

Significance

The Azure DevOps toolset is a self-service model that has resulted in many benefits for OIT development teams. It is a configuration designed for collaboration and extensive communication and outreach. It has allowed dozens of teams across OIT to improve their processes, efficiencies and security.

Addressing Priorities and Pain Points

One benefit was the ability to allow teams to address their greatest pain points first. This increased efficiencies, allowing teams to choose to focus on plan, build, test, secure, deploy, provision, and/or monitor aspects of the services delivery lifecycle, instead of a top down, linear approach to change.

Agile Adoption

Implementing Azure DevOps, which includes many collaboration and automation options, has jump-started Agile adoption as users are now able to start implementing Agile framework organization and workflow practices as part of their day-to-day tasks.

Increased Security

A focus of the initiative was to shift security earlier in the production process by scanning applications earlier and more often instead of as an afterthought. By adding automated scanning and approval gates, security and quality are now a requirement in the implementation process and not a post-implementation approval step. Security has also been increased through Identity and Access Management (IAM) integration and central management of code and assets, as well as through easy-to-setup automated static security scans and quality checks that run regularly or automatically when a change is made to the application code.

Improved Collaboration

Heightened collaboration, communication, and reusability of already created assets, along with consistency through automation, has allowed teams to accomplish tasks faster and therefore deliver high value items to the customer earlier. With planning and technical builds of the product in the same place, in collaboration with the customer, transparency and visibility have been elevated, thus increasing trust with our customers. Consistent processes and tooling, combined with an open format, has allowed for expanded collaboration and visibility across different teams, roles, and disciplines in the organization, enabling more conversations around innovation and idea sharing.

Strategic Alignment

The Azure DevOps toolset is a software as a service cloud solution, following OIT's Cloud First policy and reducing our infrastructure footprint. It aligns with many of NASCIO's top priorities, including cloud solutions, legacy application modernization, data analytics, and security enhancement tools, to name a few. The initiative directly supports OIT's strategic goals of increasing organizational efficiency, transparency and customer satisfaction, and the critical goal of evaluating and improving statewide cybersecurity practices. An additional OIT priority is to expand virtual access to government services anytime and anywhere. This will be delivered as integrations are increased

by accessibility tools automatically scanning changes as soon as they can be tested.

Impact

The implementation of the enterprise-wide IT management initiative Azure DevOps MVP has allowed OIT to steadily transform and experience technological advances in cloud, analytics, security, collaboration, and identity and access management. It has led to a dramatic increase in the adoption of tools and methodologies across OIT as well as within individual teams. From the project's May 2019 implementation until December 2019 we have seen and continue to see double-digit growth in each of the categories below,

- 317 users were added to Azure DevOps, along with 90 teams and project kanban boards,
- 314 shared documents,
- 7,305 distinct work items tracked,
- 173 automated quality builds,
- 70 automated releases, and
- 262 code bases migrated to a secure platform.

As the chart below shows, the numbers have only doubled since between December 2019 and June 2020.

As of December 31, 2019:

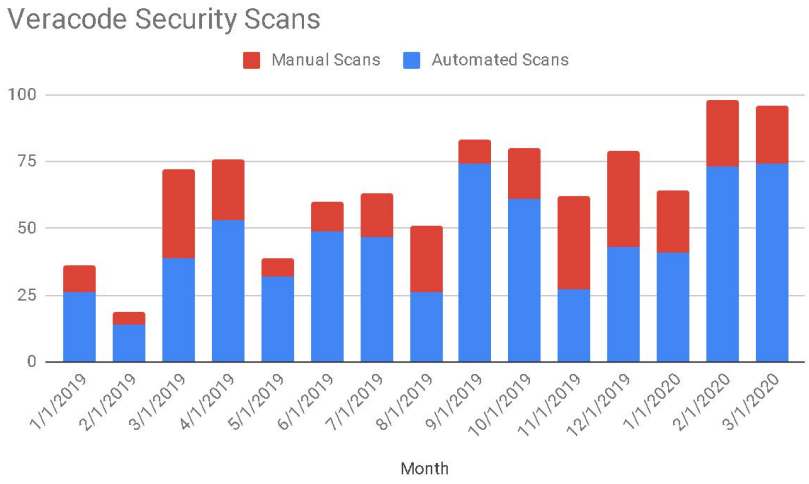
Users	Projects	Teams/ Board	Repos	Wikis	Work Items	Pipelines	Releases
317	25	90	262	314	7,305	173	70

As of June 2020:

Users	Projects	Kanban Boards	Repos	Wikis	Work Items	Pipelines	Releases
549	28	183	533	669	19,132	318	177
⇧ 73%		⇧ 103%	⇧ 103%	⇧ 113%	⇧ 161%	⇧ 83%	⇧153%

This continuous integration and delivery engine has allowed us to create automated provisioning and deprovisioning options as we increase our vast cloud offerings. By consolidating traditionally separate components of the plan, build, and deliver processes into a single platform, we have

increased our ability to utilize analytics to greatly improve our delivery cycle. We automated security analysis scans to execute whenever a change is made and automated recurring scans on unchanged code.



A central code repository allowed us to securely control assets by connecting customers with greater visibility into the delivery process to find areas for improvement. A task tracking and team work management platform that includes assignment, history, discussion sections, following, tagging, linking, descriptions, associations and customizable attributes and notifications increased collaboration even over the last few months when the majority of staff are working remotely due to the COVID-19 pandemic.

As one OIT senior developer explained, "Introducing Azure DevOps into our toolset has saved a tremendous amount of time. There is total transparency of every aspect of the project. It opens up communication between business and tech and allows us to be more Agile in our approach to software development."

As the DevSecOps mindset, tools, and processes have spread across OIT, teams now have greater opportunities to not only improve security in their applications, but to analyze, improve, and automate many of their processes. Cycle time, lead time, deployment speed, deployment frequency, velocity, and work burndown are now generated automatically, freeing teams from what is generally seen as exhausting, repetitive, and manual work. By automating processes, early and often, we are not only ensuring quality and security through reduction of manual errors and inclusion of regular scanning, but we free up people - our greatest resource - to focus on innovative solutions and delivering value to customers.