DEVSECOPS FOR A U.S. AIR FORCE CYBER WEAPON SYSTEM

Increasing delivery speed by a factor of six by compressing idea-to-production times

BUILDING A DEVSECOPS OPERATIONS MODEL

When the U.S. Air Force (USAF) wanted to streamline operations at a key defensive cyber weapon system, it turned to Technica to help it bridge the divides — both technological and human — that stood between the status quo and improved operability.

To get there, Technica implemented DevSecOps (DSO) practices for its USAF customer, Cyberspace Vulnerability Assessment/Hunter (CVA/H) weapon system, achieving multiple successes in the first year of deployment (2020) including instituting Continuous Integration, Continuous Delivery (CICD) practices, meeting NIST 800-53 compliance hurdles, and overcoming technical debt associated with previous releases. Technica's work for USAF on this deployment centered on helping it build a culture that fostered strong relationships and allowed for the incorporation of Agile practices.

Putting it even more simply, where there previously had been DevOps ***and*** Security, there is now **DevSecOps**. Two separate entities were combined into one cohesive whole, resulting in a stronger, more resilient cybersecurity stance.

Let's take a look at what it took to get there.

DEVOPS AND SEC: ALLIES SOMETIMES WORKING AT CROSS PURPOSES

At its heart, the challenge revolved around what might be called a "cultural divide" between DevOps and Security teams. In summary:

- **Developers want the tools they develop to be *faster*, go *farther*, do *more*. Their focus is on features and functionality. As they see it, security often inhibits the innovation and agility they strive to bring to life.**
- **On their side of the equation, security teams will tell you they value innovation and agility just as much as DevOps, but not at the expense of protection and compliance. For them, mitigating risk is *always* job #1.**

The resulting disconnect — of two equally important assets working at what is sometimes cross purposes — serves no one and can even jeopardize the mission. A transformation was needed.

The path forward could be found in helping its CVA/H client build a new operational model — one that bridged the unique needs and perspectives of DevOps and Security and, in doing so, created a **DevSecOps** culture.

Technica®

TIME FOR TRANSFORMATION: RELATIONSHIPS DRIVE RESULTS

Step one was building the foundation for a culture that could foster strong, cooperative relationships and incorporate Agile practices. Central to this transformation was the idea that security is not a retrofit, nor an impediment to innovation and agility.

By incorporating security early in the development process, it is possible to expose and remediate weaknesses soon enough that developers can address them without having to sacrifice features and functionality. However, when security concerns are not addressed until near the end of the development arc, conflicts may arise, with functionalities being dropped to meet security compliance requirements. Technica developed a set of standards to guide transformation:

- **Mutually agreed-upon definitions of security roles and responsibilities**
- **Shared goals, metrics, and targets between DevOps and Security teams**
- **Shared knowledge base linked to feedback and expanded skill sets**
- **Visibility into vulnerabilities, configurations, and compliance failures before application deployment**
- **Investment in security education and tools for the DevOps teams**
- **Security tools to empower DevOps teams to own the security posture of applications**

With these considerations in mind, and moving in tandem with its CVA/H community, Technica worked to foster an environment in which DevOps and Security teams were equipped with the organizational assets they needed to create a cohesive DevSecOps operational model.

In practice, the trust and rapport achieved from frequent engagement and collaboration between DevOps and Security teams have resulted in cost savings, improved operations, and diminished security risk.

DEVSECOPS: DEFINING ROLES

However, getting there required drilling down on the way Technica's USAF customer had been defining and deploying its team assets.

Like most organizations, development work had been divided among functional teams. Under this model, each team completes a task and then passes it to the next. There was little communication between the groups—the problem being that communications, however well intended, can result in confusion and conflict and, thereby, slow delivery, or introduce vulnerability into final products. In the simplest terms:

- **Development builds, and deploys new capabilities**
- **Testers test and return to Dev or pass to security**
- **Security verifies compliance and risk mitigation standards before returning to Dev or passing to Ops**
- **Ops deploys**

From a high level, it's easy to understand how and why this model came to be. However, with shorter delivery timeframes, waiting until the last minute to ensure an application is safe to deploy disrupts the entire delivery lifecycle. It's just not a sustainable model of operation.

A DevSecOps operational model was the answer.

DevSecOps places security policies into the workflow from the beginning of the lifecycle, resulting in a more robust, efficient, and resilient process. Building compliance controls into the release pipeline, coupled with an automated approach to find and resolve bugs, increase deployment efficiency and consistency with a lower risk of security flaws. Vulnerabilities decrease and velocity increases resulting in a better, more secure product faster.

IMPLEMENTATION: MAKING IT HAPPEN

Process Improvements. Technica's DevSecOps implementation began with a value-stream mapping process, based on a firm understanding of the customer's goals. Then, taking USAF's short and long-term objectives into consideration, flowcharts were created for existing process steps and assessed for their value in achieving those goals. Addressing bottlenecks and nonessential activities resulted in:

- **Enhanced workflows**
- **Shorter feedback loops**
- **Increased sharing of best security and deployment practices shared across all teams**

Resolving and eliminating inefficiencies in the software delivery lifecycle led to faster cycle time, with less wait time between steps and re-work.

Help Evolve the Culture. Technica's goal was to shift the USAF Defensive Cyber Operations process from a traditional Waterfall model to an Agile approach aligned with DevSecOps.

Three previously independent programs—feature development, product delivery, and sustaining fielded systems—merged into a unified work structure. As part of that, Technica partnered with the USAF to institute the Scaled Agile Framework (SAFe) as the structural process model. Embracing Agile mindsets enabled streamlining work processes while encouraging creativity. The teams adopted more collaborative mechanisms.

In addition to faster delivery of new features, Technica relied on our sprint methodology to respond to other immediate and critical challenges:

- **Maintaining development pace while establishing a new facility**
- **Paying off technical debt while developing code**
- **Ensuring all features met NIST 800-53 compliance requirements**

Creating a Thriving Work Environment. Technica shifted seamlessly to a new model with new personnel from three contracts being rolled into one, operating from no central facility for the first nine months, and, on top of that, the rise of the COVID-10 pandemic. Even with these challenging dynamics, Technica is proud that two full releases were completed during this timeframe.

Operating from temporary workspaces drove work on a distributed basis, which served to prepare us for the realities of the pandemic crisis when it emerged. For example, collaboration processes and tools were already in place to support:

- **Standup meetings**
- **Customer demonstrations**
- **Planning and retrospective sessions**
- **Information sharing**
- **Remote access to test and development environments**

Staffing retention, execution pace, and productivity remained steady during the Technica transformation to a "new normal."

Improved Standards. Technica adapted the inherited codebase to our quality standards. In transferring the code, we established a suitable software development pipeline, created a production gate process, and began implementing telemetry across the enterprise. These processes required a functional lab to run Dev, Test and Prod environments to succeed.

The Technica team scoped and scaled code development sections based on event-driven processes to move forward. The integrated test team members documented the results, contributing to shared learning. Building through the existing codebase helped define how to configure the pipeline processes. This knowledge facilitated a change from Jenkins to GitLab for increased scalability. The DevSecOps approach of "No Heroes" instills shared responsibilities so that every team learns from each other.

Technica®

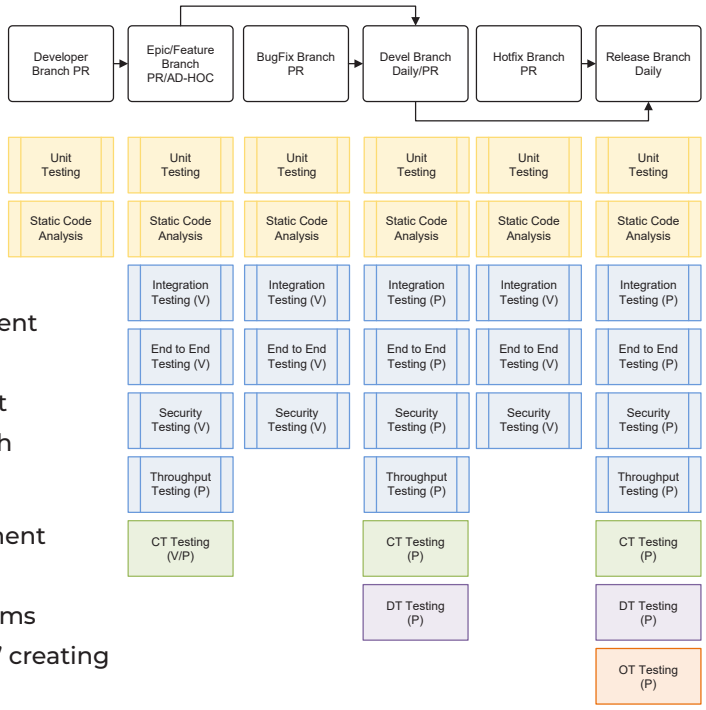
Compliance and Transparency. The requirement to achieve NIST 800-53 compliance was necessary to obtain an ATO. DevSecOps emphasizes increased transparency and integrated delivery, so the Technica teams shifted security practices accordingly.

A code quality checker was implemented at the beginning of the pipeline, and vulnerability scans were added at the end for each section of code.

Each security expert was assigned to at least one development team, coordinated as a central security team, and managed cybersecurity policy requirements. After the first Agile sprint iteration, the System Integration Lab (SIL) team merged with the security team for daily coordination as a shared service.

This collaboration created full visibility from initial development to delivery to increase the ability to document government compliance areas. These baseline successes allowed the teams to continue planning to implement "telemetry everywhere," creating continuous monitoring across the entire value stream.

Testing for Compliance



RESULTS: DEVSECOPS IMPLEMENTATION SUCCESS

Knowing the value of DevSecOps and recognizing the cultural change required, the Technica team achieved multiple successes during the first year supporting the CVA/H operational community:

- **Transformed Waterfall culture to DevSecOps culture**
- **Delivered 6x faster than previous program**
- **Implemented Hybrid Development Facility during the COVID-19 pandemic**

In the first year, Technica delivered four software releases within twelve months. Contrast this with a previous release occurring only twice in three years! Technica increased the delivery speed by a factor of six by shortening the time from idea to production.

IN CONCLUSION: FIND A WAY OR MAKE ONE

Technica delivers innovative services and products to solve our customer's unique challenges. At Technica, our vision is to "find a way or make one," driven by our core values of promoting change and building knowledge and skills. We continue to improve overall customer effectiveness through innovative approaches that blend new practices and proven experience to prepare for the next challenge.

031221