Case Study: Employing DevOps in Classified Environments

Organizations of all sizes are increasingly deploying Development Operations (DevOps) tools to enhance productivity, streamline workflows, reduce time to market, deliver better quality software, and minimize costs associated with the software development lifecycle. Deploying and utilizing open-source and enterprise DevOps tools in classified environments where access to the internet is restricted, additional security certifications are required and cleared DevOps engineers are needed adds a level of complexity that many are unwilling to tackle. This case study describes Ascolta's experience in using the latest DevOps tools successfully in support of a U.S. Air Force contract on Secret and Top Secret Department of Defense (DoD) networks.

Why DevOps?

Before we tackle the challenges associated with deploying DevOps solutions in classified environments, let's establish why DevOps is important in these environments in the first place. With a team composed of cross-functional members working in collaboration, DevOps organizations can deliver with maximum speed, functionality, and innovation. The Technical benefits include improved infrastructure, security, continuous delivery, less complexity, and faster resolution of problems. Cultural benefits include happier, more productive teams, higher employee engagement, and greater professional development opportunities. Finally, the mission and operational benefits include faster delivery of features, more stable and scalable operating environments, improved communication and collaboration and more time to innovate rather than fix and maintain.

The Challenges

As in most problems, the solution involves aspects of people, processes and technology. Let's examine the challenges and solutions associated with each.

People:

Organizations trying to implement DevOps solutions face problems of finding, training and keeping skilled DevOps engineers; finding DevOps Engineers with active DoD clearances is even harder. According to a March 2019 Federal News Network story about 103,000 federal employees and contractors are waiting for an initial background investigation. In industry alone, 37,000 people are waiting for a secret clearance, and 25,000 are waiting for a top secret clearance. In general, expect a confidential or secret clearance to take between *one to three months* and a top-secret clearance to take between *four to eight months.* However, some individuals have been waiting for their top secret/sensitive compartmented information (TS/SCI) clearances for more than a year. Workers that

already possess a clearance are difficult to find and more expensive to hire.

In addition to an active security clearance the DoD in many cases, based on individual Service or Agency, requires that engineers that access – hands on keyboard – classified computer systems meet the requirements established in DoD Manual 8570.01-M, *Information Assurance Workforce Improvement Program for Information Assurance Technical (IAT) personnel*. Generally, this entails the individual maintaining an IAT level II status which requires initial training, an IA baseline certification (i.e. Security +, CCNA Security, GICSP, etc.), and annual continuous education.

Anecdotally, out of a pool of 100 qualified DevOps engineers maybe ten either have a clearance or are clearable. Of those ten remaining, two have the required IA qualifications, and if you're lucky, one of them is looking for a new job and fits your budget.

How to overcome these challenges: In most cases involving classified contracts, the production data is classified, the software is not. Uncleared DevOps engineers can be utilized to build and test solutions, and a smaller number of cleared DevOps engineers can deploy and configure them on classified networks. To solve this problem for our Air Force customer Ascolta maintains a mix of TS/SCI cleared Developers and DevOps engineers on staff with the requisite IAT training. Our matrixed staffing approach allowed us to assign personnel where needed and transition smoothly between unclassified development environments to classified operational environments.

Processes:

Most process challenges associated with employing DevOps in classified environments are not unique to the classification level of the system. What is unique are the processes involved with introducing tooling and software to classified environments. It is industry best practice to ensure that software installed on our networks has been thoroughly vetted, scanned and tested for security vulnerabilities before being deployed and made operational. The DoD doesn't view this as a best practice, but as a hard and fast requirement.

DoD Instruction 8510.01, *DoD Risk Management Framework (RMF) for DoD Information Technology (IT)* establishes the requirements for all DoD Information Systems and Platform IT to implement security controls derived from the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53A, *Security and Privacy Controls for Federal Information Systems and Organizations*. Software must be granted some form of an authority to operate (ATO) before it can be installed on DoD systems. The ATO can come in the form of an interim authority to test (IATT) or operate (IATO) for systems under development. If being developed under a system with an existing ATO, a system can be granted a certificate to field.

Regardless of the approval path, documented prior approval is required which can be a lengthy and resource intensive process. Once granted approval to be installed, a continuous monitoring program must be utilized to ensure security controls remain effective and software changes don't introduce new vulnerabilities.

In addition to security requirements, utilizing templated environments, tool chains and workflows is a foundation of DevOps methodology and critical when deploying code across multiple classification networks. The mantra, "workflows, not technologies" encourages focus on the mission objective and uses the best current technology available to solve the problem. If the workflow is correct, new and improved technologies can continue to be leveraged as they emerge.

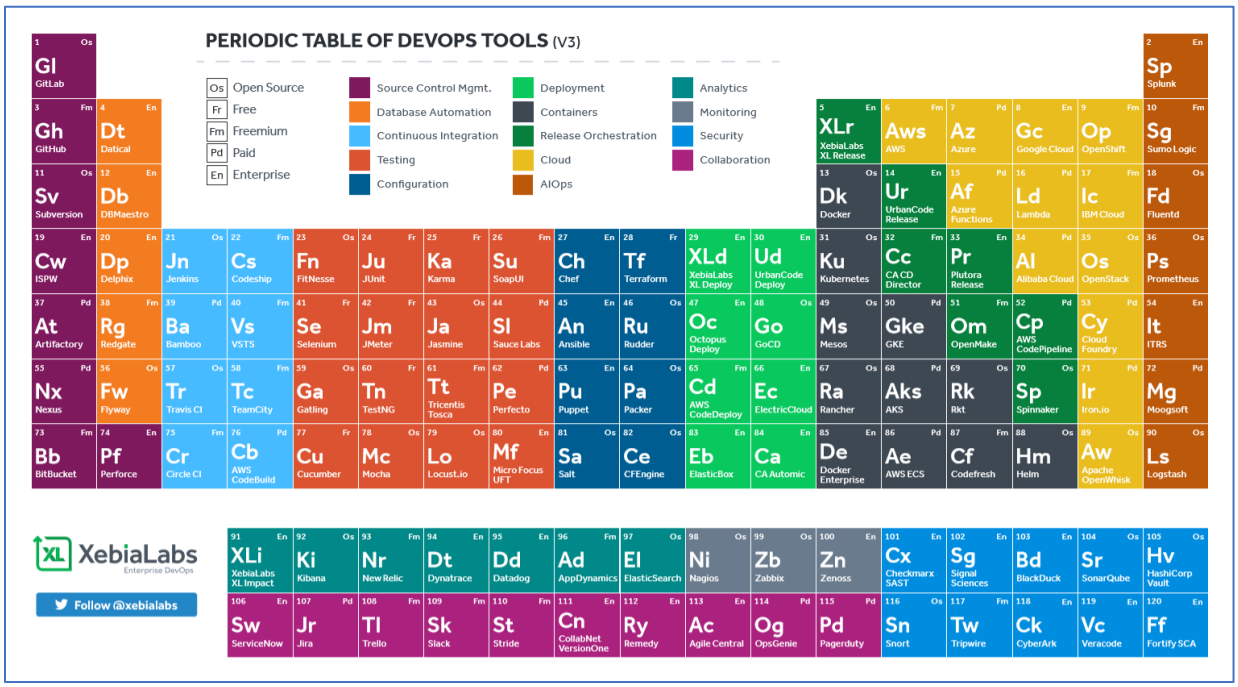
How to overcome these challenges: As mentioned above, the data is classified but the systems are not. Build low; promote to high and ensure tools and software are available at all classification levels. Ascolta has a proven track record of successfully navigating the RMF process by obtaining certificates to field and ATOs for third party tools and software. Our full-stack development team brings expertise in architecture, development, integration and delivery and is underpinned by a strong security focus. Ascolta's development philosophy allowed for development of a sound continuous integration/continuous delivery pipeline. Additionally, by utilizing templated environments, tool chains and workflows we were able to seamlessly deploy solutions developed in our unclassified Customer Integration Lab (CIL) to Air Force test environments and ultimately deploy to classified weapons systems.

Technology:

DevOps tools are available in a range of offerings from open source to enterprise licenses, XebiaLabs has created a periodic table of DevOps tools, shown on the next page, that nicely lists and categorizes some of the technology available to DevOps engineers today.

Tool stacks such as the HashiCorp product suite consisting of Terraform, Vault, Consul and Nomad provide an integrated suite of solutions that work together nicely and are cleared for use on DoD classified networks. Terraform Enterprise provides workspaces, modules, and other powerful constructs for teams to package infrastructure as code into reusable modules enabling developers to quickly provision in a self-service fashion. Likewise, policy-as-code and logging enable organizations to secure, govern, and audit their entire deployment. Vault tightly controls access to secrets and encryption keys by authenticating against trusted sources of identity such as Active Directory, LDAP, Kubernetes, CloudFoundry, and cloud platforms. It also enables fine grained authorization of which users and applications are permitted access to secrets and keys. Consul provides a multi-cloud service networking platform to connect and secure services across any runtime platform and public or private cloud. Nomad is an easy-to-use and

flexible cluster scheduler that enables an organization to automate the deployment of any application on any infrastructure at any scale.



Available at xebialabs.com

The ability to develop and test solutions outside of classified networks is greatly enhanced by commercial cloud service providers (CSP) that provide secure cloud environments that meet FedRAMP (Federal Risk and Authorization Management Program) requirements for protecting classified information. The DoD utilizes Information Impact Levels (IL) that consider the potential impact should the confidentiality or the integrity of the information be compromised. There are four levels (note that IL-1 was merged with IL-2 and IL-3 was merged with IL-4):

- IL-2: Non-Controlled Unclassified Information or publicly releasable information;
- IL-4: Controlled Unclassified Information;
- IL-5: Controlled Unclassified Information with additional protections for National Security Systems; and
- IL-6: Classified Information up to secret.

Notable CSPs that offer secure clouds (as of April 2019) are Amazon Web Services (AWS) Secret Region at IL-6, IBM Cloud Managed Services for Government (CMSG) at IL-5, and Microsoft Azure DoD at IL-5. The ability to create and package software builds with tools in these clouds allows developers to efficiently and cost effectively develop and package code for delivery on production servers wherever they may reside.

How to overcome these issues: The periodic table of DevOps tools shows there are

numerous solutions available. Selecting those that work well together and are available and acceptable for use in classified environments is critical. Ascolta utilized our experience building and maintaining secure cloud-based environments for the Air Force by providing an unclassified but secure CIL in AWS GovCloud as a staging and testing platform for integrating and moving code to classified systems. Having the ability to engineer outside of sensitive classified information facilities (SCIF) in a secure cloud environment reduced the number of cleared DevOps engineers required. Our status as a HashiCorp system integration partner with expertise in their full tool suite provided the underpinnings for the construction of a seamless, functional and secure DevOps environment allowing rapid code integration, testing and deployment.

Conclusion

Reducing the time from concept to capability is becoming increasingly critical in both the public sector and within the IC/DoD. The DevOps paradigm is to deploy small increments to get quick feedback, determine where problems exist in the environment, and identify what should be fixed. DevOps includes all the stakeholders involved in a project from beginning to end, including development and operations personnel, program managers, acquisition staff, and security and quality engineers and others as needed. Developers can also build their applications with a technology stack with DevOps in mind. This process can be automated further to simplify moving applications across environments. This capability is applicable in the defense space where multiple applications must be packaged together to deploy to a classified environment and ultimately to the warfighter.

There are many advantages of being platform and technology agnostic and avoiding vendor lock-in. All these tools can be mixed and matched, and there is some overlap among them. The selected tools should not drive your mission; they only exist to support your workflows, not the other way around.

DevOps is a movement that has gained traction for good reason, it demands a keen understanding of best practices and the tools to support them. DevOps continues to bring value to the commercial space and there is no doubt that it can do the same for the classified government space.

Ascolta's Software Development and DevOps teams have delivered real-world solutions to solve highly complex mission requirements by working closely with our Air Force clients to select the best toolset, design the architecture, write code to integrate disparate algorithms, data sets and technologies where necessary and deliver that solution into a codified, hardened and tested environment. We have worked with clients to deploy solutions, work through the ATO process, and provide user training to ensure mission success. DevOps in classified environments is possible and has been proven to greatly increase speed to deployment, security and functionality.