Open Standards & Open Collaboration:

Enabling Faster Application Delivery in the Intelligence Community with DevOps

redhat.

govloop

INDUSTRY PERSPECTIVE

EXECUTIVE SUMMARY

Today, government agencies, and particularly the intelligence community, face challenges from all directions. Adversaries are not only using technology to attack, but these attacks are increasing and constantly evolving; nation states are using sophisticated cyberattacks to breach government systems; terrorists and criminals are attacking infrastructure; and global ransomware damage costs are predicted to exceed $5 billion in 2017.

The situation for the U.S. intelligence community (IC) and the people and information they are protecting is dire. They must have a quicker response to threats, keep up with changing requirements for user needs and create a rapid development of capability. The landscape today is a multidomain battlefield: the enemy is innovating quickly using cyber as a weapon, and so the IC must innovate ever faster to stay ahead.

But there are numerous challenges to this innovation in the IC. First, legacy IT and infrastructure can often get in the way of digital transformation and innovation in the IC.

To advance, the intelligence community needs to take lessons from the development and innovation at Uber, Facebook, Google, and other innovative private-sector companies. But for the IC and other government agencies it is not always prudent to start fresh with private-sector-style innovations; rather it is critical to identify when to refresh legacy apps and when to start new. The IC is in a bimodal practice and as such must evaluate people, processes and technology to identify the most effective systems deliver quicker response to threats, keep up with changing requirements for user needs and create a rapid development of capability for team development. Modernization in infrastructure and application development processes can enable faster delivery of mission applications, and the ability to quickly respond to new threats and changing requirements.

That's where Red Hat, a leading provider of open source solutions and a central player in the digital transformation effort in the intelligence community, comes in. GovLoop sat down with Red Hat's **Toan Do**, Director of National Security Programs, and **Nick Sabine**, Solution Architect, to understand how leveraging automation and application development through approaches like DevOps can help IC member agencies as they address the challenges and opportunities of innovating faster through digital transformations to meet mission need.

OVERCOMING THE CURRENT CULTURE OF THE IC WITH DEVOPS

Every day that the IC spends time maintaining legacy systems is another day of incurring technical debt. Today, prosecution of war has changed to be more agile and nimble; the tools to support the warfighter needs to change as well. But the current approach to culture and technology in the IC can make these needed changes difficult. The IC expends too much effort, money and time supporting legacy apps and not leveraging new technology, as well as holding onto rigid waterfall development practices. Additionally, policy and legal requirements often prevent information sharing, leading to an IC that is today a culture of silos.

"Our customers say they are facing four challenges in IC culture," said Sabine. "Optimizing existing, traditional resources so they can continue to add value; integrating old and new systems, resources, and practices; adding and managing the cloud infrastructure that's appropriate for their needs; and building the modern apps and solutions that will take them further."

As a community, the IC needs to innovate rapidly to meet the rising and constantly changing demands for capabilities. This requires new ways of thinking, including technology, process, and culture. Deployment-centric application platforms and DevOps initiatives can drive benefits for the intelligence community in their digital transformation journey.

DevOps is an approach to culture, automation, and platform design to provide better mission value and responsiveness. The goal is to increase the speed and flexibility with which new features and services are delivered. DevOps applies open source principles and practices to culture, automation, and platform design, delivering increased business value and responsiveness through rapid, iterative, and high-quality IT service delivery, helping to connect different IT environments.

Legacy applications in the IC represent significant investment and are critical to ongoing mission operations. But as the technical baselines of these applications age, they can be a challenge to maintain in terms of security best practices, and they present significant roadblocks to migration into modern DevOps process.

"Red Hat sees the contributions that come from lots of people working together and improving successes," said Sabine. "In the IC, applying that means working together, reducing stovepipes, being more nimble and agile and using DevOps."

There are three components of the DevOps journey:

1. **Instilling a culture of collaboration:** DevOps is as much a cultural shift as it is implementing processes and tools.
2. **Automating to improve application delivery:** Automating your existing processes and applications lets you deliver software faster and reclaim time for new innovation. Automation helps your smartest people do the most important things by automating repetitive and mundane tasks. It is the fastest way to ROI.
3. **Building a dynamic software-defined platform:** Infrastructure platforms are rapidly evolving to dynamic, programmable platforms that can help you migrate to modern cloud and container-based applications.

"DevOps is the bridge between 'mode 1' organizations like the intelligence community that have more legacy infrastructure, and 'mode 2' or more advanced innovators," said Sabine.

DevOps represents the opportunity for the intelligence community to increase their pace by broadly embracing open source culture to invigorate software development's role as an engine for increasing the delivery of applications. DevOps increases the speed and flexibility with which new features and services are delivered. Automation and more agile and iterative development, deployment, updates, and operations also improve quality and security.

DevOps will allow the intelligence community to embrace a "go fast" mode of IT while not only maintaining, but incrementally modernizing their classic IT with its slower and more tightly controlled rate of change management.

Linking these classic IT and cloud-native IT modes is key to sharing the rich set of data and applications on which the IC depends and making them accessible throughout the entire IT environment.

ACCELERATING DEVOPS AND APPLICATION DEVELOPMENT WITH OPENSHIFT

With pressure to modernize legacy systems, do more with less, meet mandates, and keep up with new innovations, the IC needs to turn to DevOps for help. By employing a comprehensive platform for operationalizing containers, Red Hat OpenShift enables IC IT organizations to efficiently implement DevOps and reduce conflicts between development and operations teams. Containers and DevOps practices give developers the freedom to work on applications while operations can focus on the infrastructure. Red Hat provides container-focused solutions that give intelligence community IT the infrastructure, platform, and control needed to deliver on their mission with security and stability. **Below are the primary IT initiatives that Red Hat OpenShift targets:**

Accelerate application delivery with agile and DevOps methodologies: OpenShift offers a common platform for development and operations teams to ensure consistency and standardization of application components, eliminate configuration errors, automate deployment and controlled rollout of new capabilities into production, and rollback in the event of a failure. For environments with a high degree of security and regulatory requirements, additional capabilities are provided to enforce policies and role-based access control.

Modernize application architectures toward microservices: OpenShift provides a common platform for cloud-native, microservices applications alongside the existing traditional and stateful applications. Broad choice of application frameworks, programming languages, and developer tools enables customers to prototype innovative applications more quickly.

Adopt a consistent application platform for hybrid cloud deployments: IT organizations that want to decouple application dependencies from the underlying infrastructure, like the intelligence community must, are adopting container technology as a way to migrate and deploy applications across multiple cloud environments and datacenter footprints. OpenShift provides a consistent application development and deployment platform, regardless of the underlying infrastructure, and provides operations teams with a scalable, secure, and enterprise-grade application platform and unified container and cloud management capabilities.

One recent example is a modernization effort in which Red Hat consulting engineers and partners migrated a legacy FORTRAN application into a Red Hat containerized deployment within a cloud-based OpenShift platform. This accomplishment brought an application with significant maintenance burden and inflexible deployment requirements into a cloud-enabled, secure platform where automation and hybrid cloud management practices can be applied to secure, standardize, and optimize application runtimes.

RED HAT OPEN SOURCE HELPS ICITE INNOVATION

At its core, open standards and open source software are about flexibility, portability, integration and innovation. Relatedly, the biggest digital transformation effort to hit the U.S. intelligence community is under way: the Intelligence Community (IC) Information Technology Enterprise, or ICITE initiative, which aims to create a common IT workshop for all 16 IC agencies.

Ultimately, ICITE is all about innovation, which explains why open standards and open-source solutions are fundamentally embedded into the ICITE vision and architecture. OpenShift Container Platform is prevalent in the IC. This allows application portability across agencies instead of silos. And Red Hat open source solutions were among the first to be included on the ICITE blanket purchase agreement in 2004.

Predicting a continuing imperative to innovate, Do predicted intelligence agencies will increasingly be compelled to move away from proprietary solutions. "If you make everybody choose a proprietary solution, you're always going to be beholden to the vendor of a particular software package," Do said. "There's a lot of innovation that can occur in communities, and scoping the influence of that innovation to a single software vendor limits who can contribute good ideas and who can enable creative solutions. When we look at open source within the IT community, it's the open standards that enable quicker innovation, more agility, more creative solutions, and ultimately, who can build better applications."

One salient example of how the IC values and uses open-standard, open-source technology is Security Enhanced Linux (SELinux), a series of security modifications to the popular Linux operating system (OS) kernel. SELinux was developed and offered to the open source community by the National Security Agency in conjunction with Red Hat in 2000. SELinux enables the Linux OS —a popular operating system for physical and virtual servers, containers and Android smartphones — to support strict security access controls, including the Defense Department's mandatory access controls. Built in collaboration between Red Hat, the NSA, and large number of members from the open source community, SELinux addresses the hard problem of implementing policy enforcement for mandatory access controls.

The development of SELinux technology illustrates how powerful the combination of open standards and open source software can be in driving continuous innovation. "Red Hat is the steward to lead the community," Do said. "SELinux was a collaborative effort with the intelligence community that has helped industry."

The application of SELinux to container technology was an unintended consequence of the development work that went into SELinux at the time, but has exemplified the value of applying technology in new and innovative ways.

STAYING SECURE AND COMPLIANT

Red Hat products are accredited and certified to meet government compliance standards, including the Common Criteria, FIPS 140-2, STIG, and more listed here

- **COMMON CRITERIA**
- **FIPS 140-2**
- **Secure Technical Implementation Guidelines (STIG)**
- **Criminal Justice Information Services (CJIS)**
- **US Government Configuration Baseline (USGCB)**
- **USGV6 (DOD IPv6)**
- **USGv6 TESTED PRODUCT LIST**
- **SECTION 508**
- **US ARMY CERTIFICATE OF NETWORTHINESS**
- **FISMA**
- **FedRAMP**
- **NISPOM CHAPTER 8**

CONCLUSION

The pace of mission need in the intelligence community is only increasing, and budgetary pressure requires capabilities to be developed more efficiently. Waterfall development practices that have been the hallmark of government development programs for decades simply cannot keep pace with ever-changing requirements. The IC is responding, but digital transformation is not a destination; it's a culture of open innovation and a sharp focus on mission capability. If done correctly, modern application development practices such as DevOps can lead to higher code quality, quicker development cycles and better flexibility in the face of changing requirements.

By modernizing its integration strategy and architecture, the IC will unlock the key to digital transformation. The right integration strategy can help intelligence communities become a connected enterprise and thrive in today's increasingly complex and demanding threat environment.

ABOUT RED HAT

Red Hat® is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux® and middleware technologies. Today, Red Hat is at the forefront of open source software development for enterprise IT, with a broad portfolio of products and services for commercial markets. That vision for developing better software is a reality, as CIOs and IT departments around the world rely on Red Hat to deliver solutions that meet their business needs. Solutions that provide technology leadership, performance, security, and unmatched value to more than 90 percent of Fortune 500 companies. Learn more here.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross- government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop