ActioNews

FALL 2019
THE NEWSLETTER OF ACTIONET

Turning VISION into ACTION®

PRESIDENT'S NOTE

Dear Friends,

In June 2019, ActioNet was named to The Washington Post Top Workplaces 2019 for the Sixth Year in a Row, and the Washington Technology Top 100 for the Seventh Year in a Row! Our commitment to our ActioNeters, our Customers and our Community remains stronger than ever.

In this issue of ActioNews, we would like to share with you how we integrate Contact Center as a Service and our DevSecOps Core Services Offerings.

Happy Autumn!

Ashley W. Chen
Chairman & CEO

IN THIS ISSUE

Contact Centers as a Service 2
ActioNet 2019 Summer Picnics. 3

DevSecOps Unleashed

By Nate Avery, Solutions Architect

DevSecOps joins security into the traditional DevOps model. DevOps represents a blending of Developer and Operations teams, culture, and toolsets. As the two teams work closely together, the overall system becomes more stable and supportable. Operations and developers share a code repository and deployment pipeline that makes code and infrastructure deployments consistent, reliable, and repeatable. With the integration of Security teams into the equation, we can expand the practice to become DevSecOps. DevSecOps brings security into the process at the earliest stages, which avoids potentially costly fixes and re-work later in the application development process. Leveraging security standards and practices for code facilitate the participation in a full Continuous Integration / Continuous Deployment (CI/CD) Pipeline alongside application and infrastructure code. Just as DevOps breaks down silos between Dev and Ops, DevSecOps breaks down the barriers between those groups and Security.

> "DevSecOps brings security into the process at the earliest stages, which avoids potentially costly fixes and re-work later in the development process."

A typical CI/CD pipeline is comprised of a few key elements:

1. Code Repository
2. Build Engine
3. Deployment Automation Engine
4. Artifact repository

From these basic building blocks, the pipeline extension support comes from a variety of security tools.

continued on page 4

ActioNews, the newsletter of ActioNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActioNews is published quarterly (March, June, September, and December) as a service to its staff, customers, and potential customers.

ActioNews Staff

Lead Designer

Lynda D. Pitman

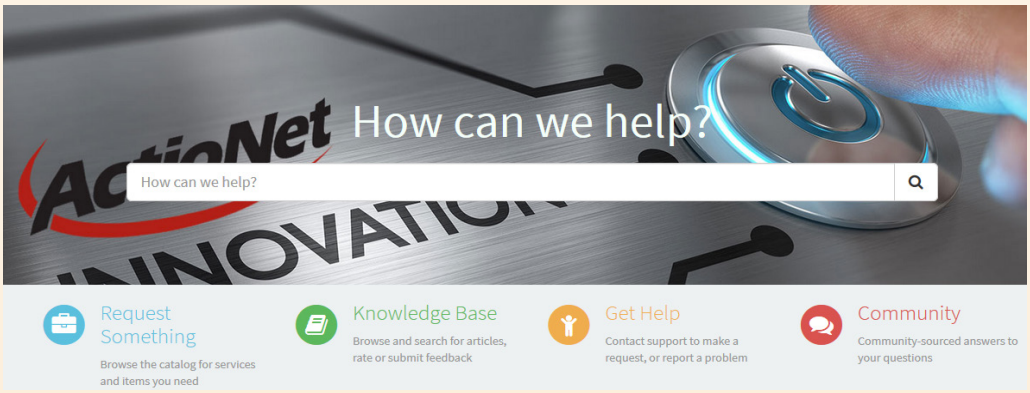
Contributing Authors

Nate Avery
Eric Chasteen

"ActioNet has increased efficiency through cost reductions with returns on investment of over $500K annually . . ."

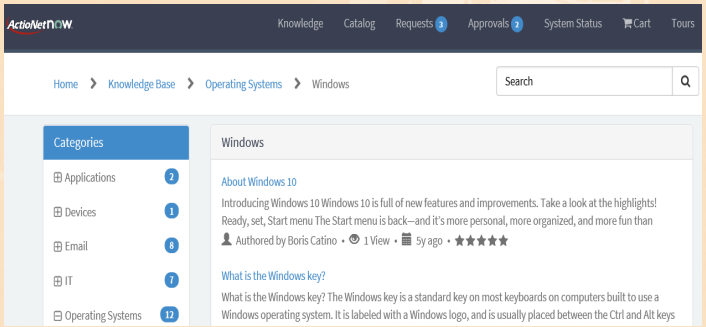
Contact Center as a Service

By Eric Chasteen, Solution Architect



ActioNet continues to develop innovative, cost effective, and secure IT Service Management (ITSM) Solutions for Federal Agencies to effectively deliver on their mission 24/7. Our ActioNet Innovation Center (AIC) is built upon our 21 years of experience, past performance, process maturity, and technology vendor partnerships to offer the Next Generation hosted multi-tenant Service Center services through our Contact Center as a Service (CCaaS). Our solution is based on industry recognized ITIL, ISO 20000 (for ITSM), ISO 27000 (Security), and ISO 9000 (Quality) Certifications; cloud-based hosting, quality management, easy onboarding, and low risk transition.

ActioNet's CCaaS provides secure hosted managed services comprised of subscription-based support of multiple IT Mission related needs and is available through multiple Federal contract vehicles. We provide prompt, courteous, and personalized services using pre-configured workflows that are easily tailorable to agency needs. Support services include software, hardware, network, telecommunications, mobile, and daily operations request fulfillment, incident and problem management, training, accessible knowledge, and advanced engineering services. End users can engage our CCaaS as their single-point-of-contact through multiple channels including phone, E-mail, web, mobile, chat, and remote access.



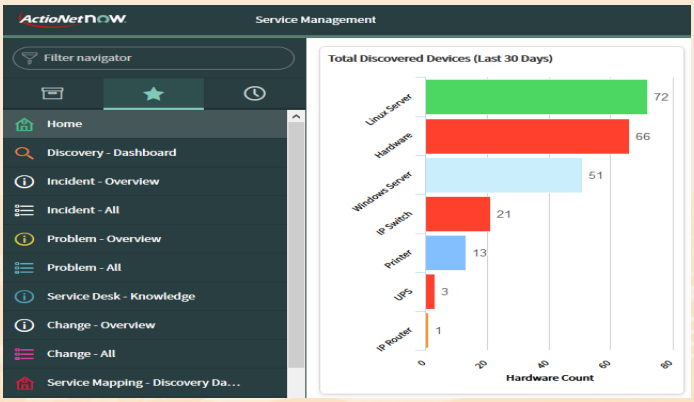
ActioNet, as our customers' Most Trusted Innogrator™ leverages and wide variety of technology partners including ServiceNow, Remedy, Cisco, RightAnswers, and Beyond Trust. This eliminates the need for Agencies to worry about purchasing, licensing, support and maintenance of ITSM systems, reduces IT footprint, and eliminates complex maintenance. ActioNet has increased efficiency through cost reductions with returns on investment of over $500K annually by eliminating expensive and obsolete on-premise hosted ITSM systems.

ActioNet's customer service portal offers end users the ability to browse and request their personalized service catalog of items, search knowledge articles to answer frequently asked questions, get help, report a problem, or connect with specified communities of interest to answer how-to questions related to agency processes, commercial or government off-the-shelf applications, and product services. We can configure and maintain your customer service portal to streamline your fulfillment processes, automate manual steps, and enable touchless transactions securely and accessible at any time, from anywhere, or on any device. This can result in 30–40% of your tickets per month diverted from Service Desk calls to direct routing, approval and fulfillment by service providers using our customer service portal.

ActioNet provides efficient caller management through our Automatic Call Distribution (ACD) System to quickly distribute incoming phone calls to appropriate customer service agents for immediate, courteous and personalized service based on need, skills required, and tailored routing menus. Our Interactive Voice Response (IVR) engine shares collected customer data enabling effective routing, handling and reporting under one platform. We can customize menus of predefined actions, greetings, communications, transfers, prompts, and sub-menus. Our customer service agents and advance engineering support teams can securely access end-user environments remotely using our hosted Beyond Trust remote access tools. We have lowered agency end-user support costs by 15-20% by enabling hosted remote access tools that reduce costly travel, desk-side, or on-site support. We are incorporating Artificial Intelligence (AI) and machine learning, enabling agent intelligence to handle higher volumes of requests at lower cost, reduce resolution time, and minimize error rates through automating categorization and assignment of requests and issues.

We provide extensible IT Operations Management (ITOM) that includes 24/7 expert monitoring, automated event driven alerts, and critical incident management of storage, network and computing services using ServiceNow, Remedy, and SolarWinds. End user and infrastructure hardware, software, telecommunications, and network configuration items are maintained using our asset management lifecycle, and managing configuration of key technical services with their underpinning infrastructure to ensure reliability, availability and security. Our ITOM services are tightly integrated with ITSM into a single platform to manage incidents, problems, and changes.

Our customers can trust and rely on our effective and efficient delivery of services by leveraging our ISO Certified Quality Management System (QMS) and weekly and monthly personalized reporting, dashboards and service reviews. We also maintain daily operational reviews with clients to ensure transparent visibility into the overall health of their IT environment. We maintain and manage Service Level Agreements, Operational Level Agreements, and Key Performance Indicators in coordination with our vendors and customers through integrated reports and dashboards. Call metrics include calls presented, calls handled, abandoned, average speed to answer, and average talk time. Ticket metrics include incidents, requests, and problems reported, response times, and resolution times. Performance metrics along required performance agreements are closely monitored and managed and we constantly look for continual service improvement to strive for Service Delivery Excellence and the best Customer Experience. For more information, please contact us at https://www.actionet.com/contact-us/.



ActioNet 2019 Summer Picnics

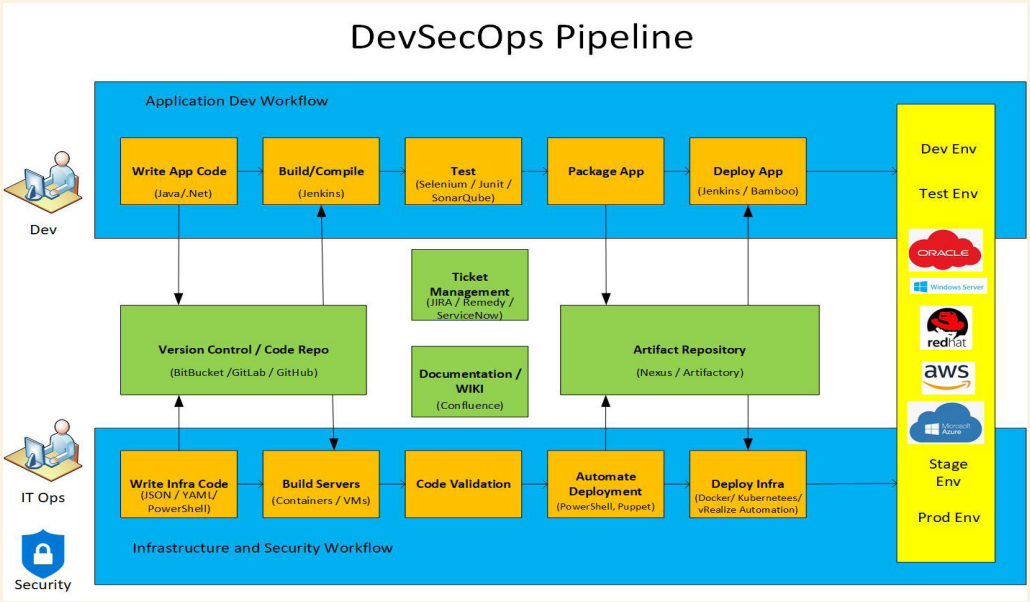
"Our customers can trust and rely on our effective and efficient delivery of services by leveraging our ISO Certified Quality Managment System (QMS) and weekly and monthly personalized reporting and dashboards and service reviews. "

- Founded in 1998, 1000+ ActioNeters in 40+ States
  - Overall Customer Retention Rate > 98%
  - Annualized Professional Staff Retention Rate > 92%
- CMMI®-DEV Level 3 Externally Assessed
- CMMI®-SVC Level 3 Externally Assessed
- HDI Certified Support Center
- ISO 20000 (ITSM), ISO 27000 (Information Security) and ISO 9000 (Quality) Registered
- GWAC and IDIQ Contract Vehicles!
  - **GSA Alliant 2**
  - **GSA IT Schedule 70**
  - **NIH CIO-SP3 SB OTSB**
  - **NIH CIO-SP3 8a OTSB**
  - **GSA PSS**
  - **DISA Encore III**
  - **Air Force NETCENTS-2**
  - **ARMY ITES-3S**
  - **HHS SPARC**
  - **NAVY Seaport-NxG**
  - **NRC GLINDA**
  - **US Courts JMAS IV**
- "92 out of 100" Rating from Open Ratings
- "Exceeds Customer Expectations" from D&B
- "5A1" the Highest Financial Rating from D&B
- Certified Earned Value Management (EVM) System
- DoD Top Secret Facility Clearance with Secret Safeguarding Capability

ActioNet, Inc.
2600 Park Tower Drive
Suite 1000
Vienna, VA 22180
PHONE 703-204-0090
FAX 703-204-4782
info@actionet.com
www.actionet.com

DevSecOps Unleashed

continued from page 1



QA testing tools like Selenium are often the first tools added. By looking for errors in the way the applications perform, system engineers can detect how a malicious actor might attempt to compromise a system.

Code analysis tools from vendors such as CAST are a growing set of tools that be called upon to validate the security of code. CAST code analysis views the code and the dependencies to ensure that the code is clean and free of defects.

The key to integrating any tools into DevSecOps is to leverage automation. The goal should be to reduce the reliance upon making changes via Graphical User Interfaces (GUIs). Steps defined as GUI clicks are converted to the equivalent code in Desired State Configuration tools such as PowerShell, Puppet, Terraform, etc. Desired State Configuration tools are an important component in security by enforcing various configuration standards. Agency baselines like DISA STIGs and NIST checklists can be applied in this manner. Moreover, desired state configuration tools combat system drift by resetting configurations at a set time interval. Included in the pipeline are security scans and validations in the form of code. This is done by building interfaces that query the Application Programming Interfaces (APIs) of the security tools.

In the event that a particular security tool does not offer native integration, it may be necessary to tie the tool to your CI/CD pipeline via custom API integrations.

REST APIs enable data exchange between applications. Data interchange usually occurs in a format such as JavaScript Object Notation (JSON).

All of the practices come together to provide improved customer outcomes.

1. Easier to sync changes between test /dev/staging and prod environments
2. Fewer human errors during deployments; by scripting the steps, humans can't click the wrong item in a GUI
3. Scripted Deployments tie into overall automation efforts meaning fewer (if any) staff need to be available for deployments. This reduces the need for employee overtime requests and therefore better budget projections

DevSecOps symbolizes a shift in traditional IT thinking and practices. Where we used to build systems and applications then scan them at the end, we can now automatically scan the code closer to when it is written, recommending errors be corrected before going into production. This is key for Federal Government customers who must achieve and maintain Authority to Operate (ATO) for their applications. The ATO process is often expensive and time consuming. DevSecOps practices go a long way to reducing the risk and cost in achieving ATOs through codified security practices that are tightly coupled and integrated into the development process.