ActioNews

FALL 2024
THE NEWSLETTER OF ACTIONET

Turning VISION into ACTION®

## CHAIRMAN'S NOTE

Dear Friends,

October is Cybersecurity Awareness Month. The theme this year is "Secure Our World" with a focus on improving Cybersecurity best practices and defense against enhanced phishing schemes, which have taken the form of fake QR codes, AI-generated deepfakes and conversational scams with AI Chatbots. We must all up our game with improved awareness and verification of sources, also leveraging AI to fight these enhanced threats.

We also cover DevSecOps from a Program Management and Security perspective. This approach is about more than just security, it's about Mission Assurance. Automating the security process creates efficiencies and maintains rapid development.

We will continue to work with our Customers and Partners to meet Mission Objectives as integrated teams focused on delivering value with enhanced security.

**Ashley W. Chen**
Founder & CEO

## IN THIS ISSUE



# Leading the Charge:
# The Strategic Importance of DevSecOps in Program Management

**By Joseph Maville, Program Manager**

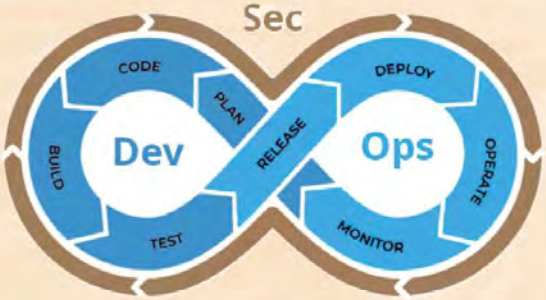
As a Marine and now a Program Manager at ActioNet, I've led teams through complex, high-stakes projects where precision and security are paramount. In both military and corporate environments, success often depends on our ability to adapt, innovate, and stay ahead of threats. Today, in software development and IT, that means embracing DevSecOps.

## What is DevSecOps?

DevSecOps—Development, Security, and Operations is not just a buzzword. It is a strategic approach that ensures security is embedded into every phase of the development lifecycle, rather than being an afterthought. In a world where cyber threats are increasingly sophisticated, this proactive stance on security is crucial.

## The Program Manager's Perspective

For Program Managers, delivering successful outcomes means not only meeting deadlines and objectives but also ensuring that the software we produce is secure and reliable. DevSecOps plays a critical role in this by integrating security early in the development process, thus mitigating risks and preventing costly breaches.




This approach is about more than just security, it's about mission assurance. Drawing from my military background, I understand the importance of ensuring that all systems function as intended, even under adverse conditions. DevSecOps supports this by making security a fundamental part of our development efforts, enhancing the resilience of our solutions.

Operational efficiency is another key benefit. By automating routine security processes, DevSecOps allows us to maintain the pace of modern development without sacrificing safety. This balance between speed and security is essential in today's fast-paced technological landscape.

## Leading in a DevSecOps Environment

Leading in a DevSecOps environment requires a shift in mindset, one that emphasizes collaboration, continuous learning, and adaptability. Just as in the military, where every team member has a role in the success of the mission, DevSecOps thrives on seamless collaboration between development, security, and operations teams. Breaking down silos and encouraging open communication is crucial to fostering a culture of teamwork and security.

Continued on page 2


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

**Karen Tepera**

Contributing Authors

**Joseph Maville**
**Sandra Montiel**



**"Leading in a DevSecOps environment requires a shift in mindset, one that emphasizes collaboration, continuous learning, and adaptability."**

## DevSecOps continued from page 1

Continuous improvement is also vital. In both combat and corporate settings, there's no room for complacency. The iterative nature of DevSecOps means we must constantly learn, adapt, and refine our processes to stay ahead of challenges.

Leadership by example remains a core principle. In the Marines, leading by example is essential, and this holds true in the context of DevSecOps. As leaders, we must be engaged with the process, understand the tools and methods being used, and show a commitment to security. When teams see that security is a priority for their leaders, it becomes a priority for them as well.

### Practical Insights for Implementation

Implementing DevSecOps effectively begins with involving security teams early in the project. Their input during the planning phase can help identify potential vulnerabilities before they escalate. Automation of security checks is another crucial step, ensuring that security standards are consistently applied across all projects.

Regular training and drills are essential to keep teams prepared and updated on the latest security practices and tools. Measuring the effectiveness of these efforts is also important metrics like the number of vulnerabilities detected early or the time it takes to address a security issue provide valuable insights and highlight areas for improvement.

### Conclusion: A Strategic Advantage

As I settle into my role at ActioNet, I'm excited about the opportunities to leverage DevSecOps to deliver even greater value to our clients. The principles of DevSecOps align closely with the leadership qualities I honed in the Marine Corps: discipline, attention to detail, and a relentless focus on the mission. By adopting this approach, we can ensure that the solutions we provide are secure, reliable, and built to withstand the challenges of tomorrow.

Our goal as Program Managers is to lead our teams to success, and DevSecOps is a powerful tool in that endeavor. Together, we can build a culture of security that not only protects our clients but also enables us to achieve our strategic objectives.

**Semper Fi.**

## Cybersecurity continued from page 4

### Secure Our World

The theme of Cybersecurity Awareness Month is "**Secure Our World**," which emphasizes the importance of cybersecurity best practices, such as recognizing and reporting phishing—still one of the primary tactics used by cyber criminals today. As criminals evolve their methods, phishing continues to be a prevalent threat, becoming increasingly sophisticated with the rise of generative AI (GenAI), which makes it more challenging for individuals and organizations to stay protected. What were once easy-to-spot phishing emails, marked by poor grammar or strange email addresses, are now harder to detect as AI enables attackers to craft highly convincing messages.

Here are some examples of new AI phishing scams along with tips to help you stay protected:

- **Fake QR Codes**: A newer form of phishing involves fake QR codes, which can be found not only in emails but also on websites, posters, flyers, and even product packaging. After scanning a code found in an email, text, postal mail, or on a flyer, some victims are directed to a website that requests personal information that can lead to identity theft, compromised passwords for online accounts, or downloads that track the user's activity on the device. Scanning these codes can lead to malicious websites or trigger unauthorized actions on your device.
- **AI-Generated Deepfakes**: Cybercriminals are using AI to create realistic videos, images, or voice clips that appear to come from trusted individuals or organizations.
- **Conversational Scams with AI Chatbots**: AI chatbots are being used to engage in seemingly normal conversations to extract sensitive information or persuade targets to perform harmful actions. These scams can be difficult to detect as the AI can mimic human conversation patterns.

### Protection Tips

1. Always verify the authenticity of any communication or request before taking action. Be especially cautious with QR codes, links, or attachments from unsolicited or unfamiliar sources.
2. Utilize security features such as QR scanner apps, email filters, and browser extensions that can help detect phishing attempts by previewing links, detecting phishing sites, and alerting you to potential threats.
3. Be cautious about sharing personal information online, especially in unsolicited chats or emails. Always ensure that the person or bot you are communicating with is who they claim to be.
4. If you receive a suspicious communication, whether it is a message, email, or even a phone call, cross-check it by reaching out to the person or organization through a known, secure channel.
5. Be wary of any unexpected or unusual requests, especially those that seem urgent or out of character. Scammers often use urgency to pressure you into making hasty decisions. As a general rule of thumb, if you don't expect it, reject it.

### Cybersecurity Awareness at ActioNet

Every Action Counts in Cybersecurity. Cybersecurity is a shared responsibility. That's why at ActioNet, we prioritize educating and engaging our team in safeguarding our digital environment by providing comprehensive security awareness training annually. This training includes how to identify phishing emails and empowers our employees to stay alert and informed. Additionally, we conduct quarterly phishing exercises using IronScales to test and strengthen our users' ability to identify phishing emails in real-world scenarios. These phishing exercises are tailored with templates that carry a difficulty ranking, allowing us to progressively challenge users who consistently perform well. If a user clicks on a phishing link during these exercises, they are redirected to a brief, interactive training module via IronScales. This ensures that every interaction becomes a learning opportunity. These proactive measures are integral to safeguarding our digital assets and maintaining a secure environment for our clients and partners.

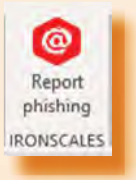
### Incident Reporting At ActioNet

At ActioNet, your awareness and prompt action are crucial to maintaining our cybersecurity posture. If you encounter any security events, incidents, or vulnerabilities, or if you suspect phishing attempts, it's essential to notify us immediately.

Please report immediately if you:

- Observe any breaches in security policy
- Identify a potential weakness or vulnerability
- Encounter any attempts at unauthorized access to Information Systems (IS)
- Suspect that an account may have been compromised
- Lose an MFA/Authentication device, such as a cellphone

For suspicious emails (Spam/Phishing): Use the "Report Phishing" button in Outlook.




### Cybersecurity Awareness Month Resources

Cybersecurity Awareness Month continues to build momentum and impact with the goal of providing everyone with the information they need to stay safer and more secure online. ActioNet is proud to support this far-reaching online safety awareness and education initiative which is co-managed by the Cybersecurity and Infrastructure Security Agency and the National Cybersecurity Alliance.

For more information about Cybersecurity Awareness Month 2024 and how to participate in a wide variety of activities, visit *cisa.gov/cybersecurity-awareness-month* and *staysafeonline.org/cybersecurity-awareness-month/*. You can also follow and use the hashtag *#CybersecurityAwarenessMonth* and *#SecureOurWorld* on social media throughout the month of October.

ActioNews

- SBA Certified WOSB under NAICS 517111, 517121
- GWAC and IDIQ Contract Vehicles
  - GSA Alliant 2
  - GSA MAS
  - GSA OASIS Pool 1
  - CIO-SP3 SB/WOSB OTSB
  - DHA MHS GSP
  - DISA Encore III
  - ARMY ITES-3S
  - NAVY Seaport-NxG
  - FAA eFast
  - HHS SPARC
  - NRC GLINDA
  - SEC OneIT
- Past Performance on Large Contracts
  - DOE ITSS, $1.2B
  - DOT COE, $350M+
  - FAA ATO, $300M+
  - CMS CICDIM, $200M+
  - DOS CA DEDM, $150M+
  - DISA CORENet, $78M
- "CMMI®-DEV V2.0 Level 4 with SAM
- CMMI®-SVC V2.0 Level 4 with SAM
- HDI Certified Support Center
- ISO 20000/27001/9001
- Approved Accounting System
- Approved EVM System
- Approved Purchasing System
- Approved Cost Estimating System
- DoD Top Secret Facility Clearance

TOP WORK PLACES 2014-2024

**Cybersecurity Awareness Month 2024**

**"Secure Our World"**

ActioNet

# ActioNet Takes Part in 2024 Cybersecurity Awareness Month

**By Sandra Montiel, Sr. Information System Security Officer**

*Cybersecurity Awareness Month highlights the increasing significance of cybersecurity in our daily lives and encourages both individuals and businesses to take essential steps to stay safe online.*

ActioNet is promoting and participating in the 21st Cybersecurity Awareness Month campaign. My name is Sandra Montiel, a recent addition to the ActioNet Innovation Center (AIC), your resource for cybersecurity initiatives. **October is Cybersecurity Awareness Month**, a global initiative dedicated to helping everyone stay safe and secure when using technology. Since 2004, the President of the United States and Congress have officially recognized October as a time for the public and private sectors to collaborate in raising awareness about the critical importance of cybersecurity.


From smart devices to connected home systems (IoT) and more, technology is deeply intertwined with our lives. As technology evolves, cybercriminals are equally determined to exploit vulnerabilities, disrupting both personal and business environments. For more than 20 years, Cybersecurity Awareness Month aims to highlight some of the emerging challenges that exist in the world of cybersecurity today and provide straightforward, actionable guidance that anyone can follow to create a safe and secure digital world for themselves and their loved ones.

**Continued on page 3**

# ActioNet Exhibited at DHITS 2024

At our booth at the DHITS 2024 Conference, we shared our innovative solutions including digital twin technology, cloud-based network operations centers and secure, scalable IT infrastructures. The synergy between ActioNet's vast experience and our joint venture's agility has positioned us as a leader in delivering impactful solutions for our Customers.