ActioNews

FALL 2020
THE NEWSLETTER OF ACTIONET

Turning VISION into ACTION®

CHAIRMAN'S NOTE

Dear Friends,

As we navigate through the COVID-19 pandemic together, Cyber incidents are on the rise and many organizations are moving workloads to the Cloud leveraging multiple Cloud Service Providers (CSPs) . End-to-end security and chargeback issues are key concerns. ActioNet continues to enhance its Cybersecurity Practice to meet the challenges that lie ahead.

Be well, stay safe and take care of each other.

Ashley W. Chen
Chairman & CEO

IN THIS ISSUE

Cybersecurity Considerations in a Multi-Cloud Environment 3
Team ActioNet Equal Justice Initiatives Exceeds Goal 4

The Cybersecurity Practice at ActioNet

By Andy Stevenson, VP, Civilian Programs

Many of us working in the government space are aware of the massive data breach at the Office of Personnel Management (OPM) announced in 2015 that exposed the personal information of over 22 million government and contractor employees. In the Washington D.C. area at least, that made big news. If you don't work in the cybersecurity world, however, some of the other massive data breaches that happen every day may go unnoticed. What's even more concerning is that they go unnoticed because they are all too common. Huge data breaches exposing social security numbers, credit card information, email addresses, passwords, and more happen with increasing regularity. Equifax, Marriot, Linkedin, Adobe, eBay, Yahoo, and many others have been attacked and breached by hackers – resulting in the compromise of hundreds of millions of user accounts. Foreign adversaries are also illegally accessing technology companies to steal valuable Intellectual Property, thus irreparably damaging our economy and our ability to compete in the world market. They target military technology and information, threatening the safety and security of our warfighters and their missions. Increasingly, industrial capabilities are being targeted through vulnerabilities in operational technology, giving attackers the ability to disrupt critical infrastructure.

"Cybersecurity is the most pressing need in light of constant data breaches."

As ActioNet further builds our digital engineering offerings to our clients, securing their data and infrastructure becomes a paramount component of our mission. Threat actors continue to improve their capabilities and tactics, and our expert cyber personnel stand ready to assist our government clients both defensively and offensively. ActioNet has a strong history of cybersecurity support, and we are using that expertise to harden and monitor infrastructure against an expanding threat landscape, while assisting our defense and intelligence clients in their proactive cyber missions. We have provided

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

Lynda D. Pitman

Contributing Authors

Michelle Washington Barnes
Mark Bortman
Reuben Maher
Andy Stevenson

"A clear architectural and engineerig roadmap is key to building an efficient, effective security infrastructure."

The Cybersecurity Practice at ActioNet

continued from page 1

cybersecurity support for DOD, Treasury, DOC, SEC, HHS, and many others. Our services have included SecDevOps, COOP design, security systems engineering, vulnerability and patch management, and information assurance. At the Department of Energy, we provided a full range of cybersecurity services, including Security Operations Center (SOC) design, build, and operation, penetration testing, and infrastructure hardening.

Cybersecurity is the most pressing need in light of constant data breaches. Globally, cybersecurity is a $112 billion market, projected to more than double over the next six years. The US Government alone will spend about $19 billion on cybersecurity this year, up over 40% from just three years ago.

Cybersecurity requires a workforce of highly skilled operators, and government contracts frequently require these resources to have one or more certifications in various areas of cyber practice. Skilled operators are scarce, and the number of open positions in the marketplace requiring certifications is much greater than the number of certificate holders. ActioNet's Cyber Community of Interest and internal training support programs build these skillsets within our workforce, providing an expert organization to our client base.

ActioNet operates in five broad Cybersecurity areas:

CISO Advisory Services: Chief Information Security Officer (CISO) advisory services are delivered at the program level to provide C-level executives with vision, roadmaps, and decision support services. ActioNet assists executives with overall program design, development, and governance, providing the roadmap to build a mature and capable cybersecurity organization. We develop investment priorities to fill gaps in capability, and help executives identify areas of cost savings by decommissioning duplicative tools and processes. We also develop important decision support capabilities through meaningful metrics and targeted dashboarding. From program design to gap analyses and technology evaluation, ActioNet helps executives make the right investments and the right decisions.

Security Architecture and Engineering: From a foundational base in enterprise architecture, ActioNet provides architecture and engineering support for diverse infrastructure requirements, including cloud, hybrid cloud, multi-cloud, mobile, and operational technology environments. ActioNet system engineers adeptly work within defense-in-depth environments, and as personal devices and cloud capabilities blur the lines of enterprise boundaries, we mature those enterprises into **Zero Trust environments**, authenticating every transaction in an automated, seamless user experience. ActioNet uses a technology-agnostic process to objectively evaluate, select, tune, and configure tools to meet our clients' needs, and decommission those tools that present opportunities for efficiency and savings. A clear architectural and engineering roadmap is key to building an efficient, effective security infrastructure.

What is Zero Trust?

Previous security models operated under the "security and moat" model where everything inside a company's firewall was trusted with the assumption that users have been validated and are therefore trustworthy. The problem is when an attacker gets inside the network, they have broad access to data. Yet with the blurring of traditional network boundaries, Zero Trust takes an entirely different approach of "Never trust; Always verify." It assumes the entire network could be compromised and requires verification from every person and device to access network data and resources. Zero Trust incorporates principles like least-privilege access (aka need-to-know), multi-factor authentication (MFA), microsegmentation, and strict controls on both device and user access to protect today's increasingly connected business environments from emerging digital threats.

Cyber Operations: ActioNet cyber specialists perform the vital real-time operational roles necessary to advance our clients' missions. We start with fundamental system hygiene – system operations and maintenance, configuration, vulnerability, and patch management. Taking advantage of our comprehensive threat intelligence capabilities, our monitoring teams customize SIEM content to prevent, discover, and respond to cyber adversaries. Speed to action is paramount, and our proactive hunt teams seek out attackers before they access sensitive information, leveraging Security

Orchestration and Automated Response (SOAR) to dramatically improve response times. ActioNet also develops extensive insider threat programs, guarding against the malicious and the simply careless actions of insiders. When security incidents do happen, our security incident management teams quickly contain and mitigate data exposure.

Assessment and Testing: The process of obtaining Authorization to Operate (ATO) should be fast, automated, and must ensure the comprehensive security of the system being tested. ActioNet's technical experts focus on the highest risk attack vectors, ensuring valuable time and resources are spent testing and validating critical controls. This results in true continuous monitoring of systems, constantly testing critical controls in an automated way, while de-prioritizing low-risk controls – limiting cost and increasing program efficiency. Our penetration testers look for ways to take advantage of planned system functionality in unforeseen ways, misusing systems in ways that scanners cannot. We develop mis-use cases to clearly explain to system stakeholders how attackers can take advantage of vulnerabilities. Most importantly, we advise the best and most efficient methods to mitigate cyber weaknesses and close the Plan of Action and Milestones (POA&Ms), enabling stakeholders to harden their systems against attack.

SecDevOps: ActioNet's deep development experience combined with our cybersecurity expertise provides the most efficient, secure code development available. Along with disciplined requirements definition and release scheduling, we perform automated testing through multiple gates in containerized environments to provide secure, high-quality code that works. By integrating security into the development lifecycle from Day One, ActioNet supports rapid release cycles with security built in, supporting automated continuous ATO environments.

ActioNet's expert capability in the cyber marketplace is a valuable and necessary part of the digital product we create for our clients. Cybersecurity ensures that services are available when they are needed, that information is correct when it is accessed, and that sensitive and personal information is protected. Our cybersecurity experts demonstrate every day how truly vital they are to protecting our clients' missions, our government's critical infrastructure, and the nation's economy. For more information on ActioNet's Cyber capabilities, please contact info@actionet.com.

Cybersecurity Considerations in a Multi-Cloud Environment

By Mark Bortman, Director, Cloud Innovation, & Reuben Maher, SVP & Chief Innovation Officer

Remember when moving data into the cloud was a radical idea? Those days are long gone.

Forbes estimates that 83% of all enterprise workloads will be performed in the cloud by the end of 2020, a remarkable shift in an already rapidly changing digital landscape.

Yet the market is increasingly moving beyond single cloud instances into a multi-cloud environment. Companies are leveraging a strategy of running applications and testing out new capabilities in multiple clouds simultaneously, and often with a mixture of both public, private, and hybrid cloud instances. Whereas 90% of companies have invested in at least one type of cloud service provider, the numbers moving to multi-cloud solutions are skyrocketing. In 2018, Forrester Research estimated that 62% of public cloud adopters were using two or more different cloud providers. Gartner predicts that "by 2021, over 75% of midsize and large organizations will have adopted a multi-cloud and /or hybrid IT strategy." Additionally, companies innovating on applications development and testing often use five private or public cloud environments.

But transitioning to a multi-cloud strategy is not without risk. Common missteps include moving to a multi-cloud environment without a sound business reason and the proper cybersecurity posture in place. Gartner explains, "For an enterprise using cloud services across multiple geographies, finding just one public cloud infrastructure provider to meet its needs is a struggle. In

continued on page 4

"FORBES estimates that 83% of all enterprise workloads will be performed in the cloud by the end of 2020.... "

- CMMI®-DEV Level 4 Externally Assessed
- CMMI®-SVC Level 4 Externally Assessed
- ISO 9001 (Quality) Certified
- ISO 20000 (ITIL) Certified
- ISO 27001 (Information Security) Certified
- HDI Certified Support Center
- Contract Vehicles Available for Multiple Civilan and Defense Agencies:
  - **Air Force NETCENTS-2**
  - **ARMY ITES-3S**
  - **DISA Encore III**
  - **GSA Alliant 2**
  - **GSA IT Schedule 70**
  - **NAVY Seaport-NxG**
  - **NIH CIO-SP3 SB OTSB**
  - **NIH CIO-SP3 8a OTSB**
  - **HHS NGITS**
  - **NRC GLINDA**
  - **SEC OneIT**
  - **HHS SPARC**
  - **US Courts JMAS IV**
- "92 out of 100" Rating from Open Ratings
- "Exceeds Customer Expectations" from D&B
- "5A1" the Highest Rating from D&B
- DCAA-Compliant Accounting System
- Government Approved Purchasing System
- Government Approved 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

Cybersecurity Considerations in a Multi-Cloud Environment continued from page 3

organizations like this, the decision to use a multi-cloud strategy is clear."

Of all current risks (including those associated with cost and chargeback complexities), security has quickly jumped to the top of major concerns expressed by IT professionals across the world. In fact, approximately 66% of technology leaders stated that security is their number one concern when considering moving workloads into the cloud, an issue amplified when considering the increased involution associated with a strategy dependent on multiple heterogeneous cloud service providers (CSPs). With the average cost of a data breach now at $8 million (estimated at around $75 per compromised record), the stakes are simply too high to not have a robust, end-to-end cloud strategy.

This is where ActioNet's Cyber team brings years of in-depth knowledge to each unique cloud mission engagement. Our Security Architecture and Engineering team leverages our technology-agnostic process to work across lines of infrastructure and enterprise boundaries to develop a concise architectural and engineering roadmap tailored to your environment. We then evaluate, select, and customize the cloud cyber solution to your unique mission requirements.

We also bring proven cloud managed service solutions which help clients make more informed decisions around governance, risk, and compliance in any cloud environment while delivering an industry standard FedRAMP compliant solution.

Ensuring a strong multi-cloud strategy is in place and having appropriate governance controls is critical. ActioNet's Security Architecture and Engineering team combined with our holistic managed services solutions provide robust options for organizations to effectively lower their threat profile while having greater confidence in the privacy and security of their multi-cloud environment.

Team ActioNet Equal Justice Initiatives Exceeds Goal

By Michelle Washington Barnes, Executive Assistant & Office Manager

During one of the most challenging periods in our generation with the COVID-19 crisis and the major shift in how and where we work and interact with each other, we take great pride that our ActioNeters continued to support our community and helping others in need, never missing a beat in showing that we care and can help make a difference.

Team ActioNet participated in the Equal Justice Initiative (EJI) and its deep commitment to promoting diversity, by sponsoring a fund drive from July 1 until July 31, 2020. The goal was $2,500 in employee donations with a 100% corporate matching donation.

EJI is committed to ending mass incarceration and excessive punishment in the United States, to challenging racial and economic injustice, and to protecting basic human rights for the most vulnerable people in American society. EJI provides legal assistance to innocent death row prisoners, confronts abuse of the incarcerated and the mentally ill, and aids children prosecuted as adults.

ActioNet would like to extend a heartfelt thank you for the sponsorship ActioNeters provided to our Equal Justice Initiative (EJI) fund drive. With their generous giving, Team ActioNet was able to surpass its goal of $5,000.00. Employees donated $3,259.89 and the company matched that amount with $3,357.69. In total, ActioNet donated $6,617.58. A huge success!

Our collective commitment to support our communities and each other has, and will continue, to make a difference!