MeriTalk
Improving the Outcomes of Government IT

maximus

Secure by Design:

How Continuous Vulnerability Management Delivers Cyber Resiliency

While every Federal agency is now required to identify network assets and vulnerabilities and provide data to the Cybersecurity and Infrastructure Security Agency (CISA) regularly under CISA's Binding Operational Directive (BOD), Improving Asset Visibility and Vulnerability Detection on Federal Networks, gaps persist. Bad actors continue to exploit known vulnerabilities, some of which are the consequence of highly interconnected systems and data sharing between the public and private sectors.

Against this backdrop, Federal financial agencies are working to keep citizen data secure. In August, for example, a Government Accountability Office (GAO) report highlighted the need for an additional oversight structure to keep Internal Revenue Service (IRS) taxpayer information secure while it is held by third-party private-sector providers – tax return preparers and tax software providers.

MeriTalk recently sat down with Roger Colón, Senior Director of Cybersecurity, and Gina Bornarth, Senior Manager of Growth at Maximus, to explore current vulnerability management policy and practices across the Federal government and how continuous vulnerability management can help agencies achieve "secure by design" cyber resiliency.

MeriTalk: What steps is the Federal government taking to strengthen vulnerability management?

Colón: In the past, agencies actively searched for weaknesses, but they were not doing enough with what they found. Vulnerability reports were simply forwarded to security teams. There was minimal examination, verification, or documentation – and far too little sharing across departments, across agencies, and between the public and private sectors.

> Today, agencies are maturing vulnerability management with solutions that leverage artificial intelligence (AI) and machine learning to automate every step of the process – from detection to reporting and ultimately resolving the issue. This means vulnerability management is continuous and agencies can identify and contain threats much faster than with traditional point-in-time identification.

MeriTalk: Let's drill down on Federal financial agencies. Can you identify steps agencies can take to mature vulnerability management to continue to strengthen security?

Bornarth: Agencies with missions that involve managing and sharing citizen financial information, including the IRS, the Federal Deposit Insurance Corporation, and the Bureau of Fiscal Services, understand that they have unique challenges and responsibilities to maintain a high level of trust with the American public.

Steps that these and similar agencies can take to strengthen defenses include enhancing asset management, improving database vulnerability scanning, patching database vulnerabilities in a timely manner, and taking additional steps to ensure data held by third-party companies is secure.

MeriTalk: Overall, where are agencies having challenges with continuous vulnerability management?

Colón: Agencies face challenges on three fronts: people, technology, and process. First, there just aren't enough skilled cyber analysts, which is a serious problem as technology advances and threats increase in volume and complexity. Second, many cyber leaders face time and resource constraints that make it difficult to match tools and resources to cyber threats.

Fortunately, there are solutions available today – infused with AI – that help cyber teams detect anomalies in real time, prioritize resources, and focus on the greatest threats. There are also solutions to help automate tasks that proactively reduce risk – software patch management, as an example.

Lastly, sporadic vulnerability management can leave gaps that bad actors can exploit. At Maximus, our approach involves identifying these gaps and implementing corrective measures and technologies to effectively address vulnerabilities.

MeriTalk: Systems are only as secure as the underlying infrastructure – and as secure as their security controls. How can agencies design a vulnerability management program that covers all their IT systems and is truly "secure by design"?

Colón: There are three essential components when designing robust vulnerability management programs. The first is asset management, which involves identifying all hardware, software, and libraries in your environment. Without a clear understanding of the assets within your environment, you cannot properly protect them against threats and vulnerabilities.

The next component is configuration management, ensuring you are implementing mature processes that consistently track, document, and control the changes made to all hardware, software, and network settings.

And lastly, it is critical to have strong identity and access management practices that not only manage user identities and enforce authentication and authorization levels, but also monitor all access activities to resources, systems, and data across the organization.

MeriTalk: Federal agencies are focused on implementing the government's zero trust security mandates. How does vulnerability management help leaders mature their zero trust environments?

Bornarth: Vulnerability management and zero trust go hand in hand, to the point where one can't really exist without the other. Zero trust, the concept that nothing is inherently trusted on the network, calls for granular access controls, strong authentication mechanisms and policy controls, and continuous monitoring. Agencies employing continuous vulnerability management are able to identify security weaknesses across network infrastructure, applications, and endpoints; apply patches and updates; and ensure that systems are configured securely. All of these actions support zero trust security.

MeriTalk: How does Maximus help agencies achieve and maintain continuous vulnerability management?

Bornarth: Maximus specializes in uniting people, technology, and processes into cohesive solutions and services that we customize to address the unique requirements of our customers. We begin by assessing an agency's security posture, so we fully understand the current environment.

> Once we recognize potential weaknesses, we work with agency leaders to develop a roadmap toward cybersecurity maturity.

Our processes helped one civilian agency with more than 60,000 employees achieve a Cybersecurity Center of Excellence designation. For this agency, we manage more than 200 billion security events monthly from 40,000 different sources, and we process more than 10 terabytes of data per day from

multiple environments. For another agency, we've processed more than 25 terabytes of data each day from more than 100,000 endpoints.

In our work with Federal agencies, we help agency leaders determine what's already in their cybersecurity toolbox and make recommendations to build upon that foundation. We know our strengths, and we also recognize when it makes sense to bring in other expertise. It's our responsibility to do our due diligence and provide the best solution for our customers.

MeriTalk: Any final thoughts?

Colón: Across the Federal community, we must continue to pursue a coordinated, whole-of-government effort to identify, share, and remediate threats if we want to keep Federal missions and citizen data secure. We will be keeping an eye on new legislation introduced by Rep. Nancy Mace, R-S.C., that aims to help Federal contractors identify and fix software vulnerabilities before adversaries can exploit them. Her Federal Cybersecurity Vulnerability Reduction Act would require all Federal contractors to implement vulnerability disclosure policies (VDPs) to improve protections for public and private information systems.

These congressional efforts are important steps. Continuous vulnerability management and participation in vulnerability disclosure platforms help advance all of government toward "secure by design" cyber resiliency. We hope to see policymakers consider other issues, including software supply chain vulnerabilities, when considering requirements for Federal financial agencies and those who manage similar data.

Our collective job across industry and government is to stay ahead of threats – and we have important new opportunities for success if we move quickly.