What Are the Priorities for the U.S. Administration Cybersecurity Spending in 2026?

Posted on August 14, 2024

The White House has laid out a road map on how executive departments and agencies should plan to spend their cybersecurity dollars in the coming years. On 10 July 2024, the Office of Management and Budget (OMB) released a memorandum outlining the administration's cybersecurity investment priorities. The memo intends to guide relevant government entities as they prepare their 2026 budget submissions to the OMB.

The U.S. government is taking a page out of its own National Cybersecurity Strategy (NCS) playbook, wrapping its investment priorities around five pillars to improve the country's cybersecurity posture, namely:

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience
- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals

Prioritizing these key areas will enable agencies to contribute to strengthening the nation's cybersecurity posture and safeguarding critical infrastructure.

What Will the Focus Areas of Government Agencies Be?

Whether a government agency is trying to protect taxpayer dollars or tech companies are looking to land or maintain government contracts, they'll need to align their strategies with the administration's priorities. The memo essentially sets the standards for what cybersecurity should look like in the coming years, and here are some areas to concentrate on.

Zero Trust Maturity

The first order of business is beefing up defenses as part of the first NCS pillar, "Defend Critical Infrastructure." The memo emphasizes upgrading security systems, thus requiring agencies to demonstrate progress across the Zero Trust Maturity Model. Zero trust is a security model that assumes no one or nothing inside or outside a network can be trusted, and agencies have until 7 November 2024 to submit an updated zero trust implementation plan to the OMB.

While 67% of government agencies are prepared to meet the zero trust requirements, the ultimate goal is for everyone to adopt a fully mature zero trust approach. As their maturity progresses, the requirements will significantly increase, as the Cybersecurity and Infrastructure Security Agency (CISA) depicts in the image below.

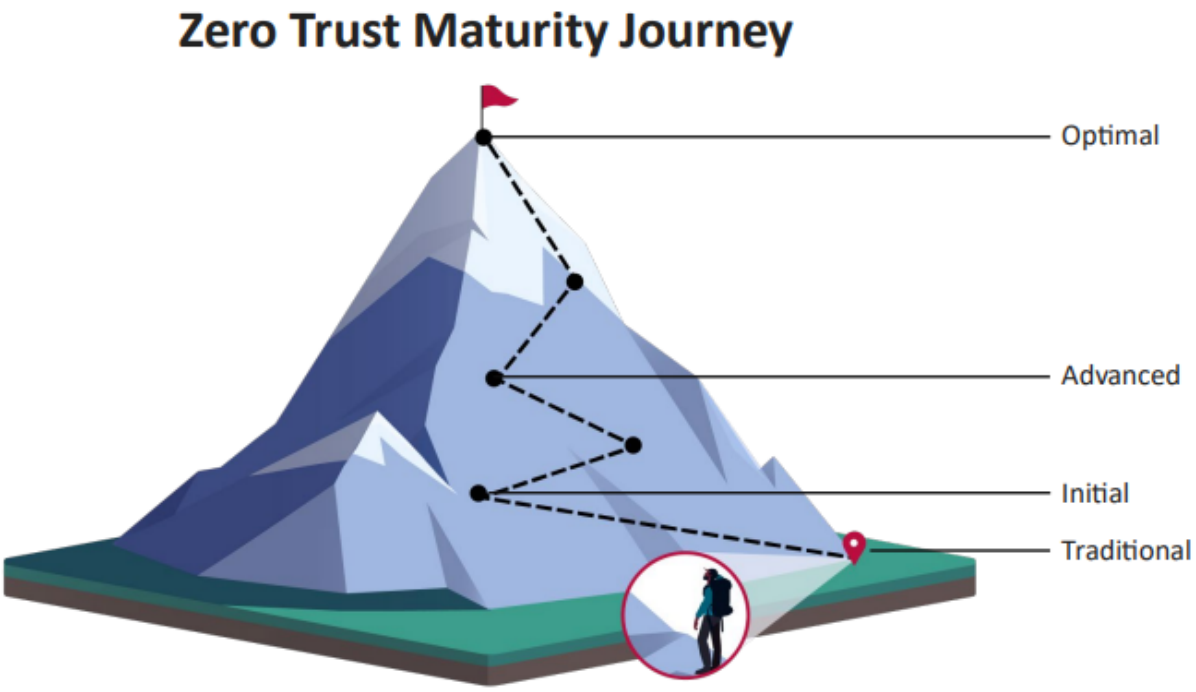

Figure 2: Zero Trust Maturity Journey

Figure 1: *CISA-Defined Zero Trust Maturity Journey in* *https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf*

Let's break down each phase of the journey.

- **Traditional:** This old-school approach relies on manual processes and isolated security solutions. Think spreadsheets for asset management, firewalls as the only defense, and security teams reacting to attacks with limited visibility into their data and systems.
- **Initial:** Here, organizations must start automating basic security tasks and integrating some security systems. While they should have improved visibility into internal systems, security remains reactive, meaning teams wait for something to happen before acting.
- **Advanced:** This stage brings a higher level of sophistication. Automation takes center stage, requiring security teams to manage assets and enforce policies. Security teams and systems

must proactively hunt for threats with a heightened focus on data protection.

- **Optimal:** This level is the ultimate goal, translating to fully automated security operations, dynamic access controls, comprehensive visibility across the entire environment, and continuous security improvement.

As you can see, visibility is essential throughout the zero trust maturity journey. After all, you can't determine if something is safe if you don't know it exists. This approach applies to both internal and external assets.

To meet that and other requirements wherever they are in their maturity journey, 64% of federal agencies are turning toward low-code security automation platforms. These platforms are often composed of third-party solutions that help them automate security without relying excessively on coding, especially since agencies find filling security team positions difficult.

Threat Detection, Investigation, and Prevention

Government organizations handle massive amounts of data, making them prime cyber attack targets. For instance, the digital footprint of the National Aeronautics and Space Administration (NASA) extends across more than 1,700 public-facing websites, while the Federal Deposit Insurance Corporation (FDIC) manages approximately 1.8 petabytes of personally identifiable information (PII).

To counter threats, the government prioritizes investing in proactive threat detection, investigation, and response, in line with the first two pillars of the NCS (i.e., "Defend Critical Infrastructure" and "Disrupt and Dismantle Threat Actors").

Agencies need to monitor networks, systems, applications, and user behaviors by employing next-generation cybersecurity solutions. These systems must be able to identify and log not only sophisticated threats but also those that threat actors commonly employ.

Among their favorites? Newly registered domains often created using domain generation algorithms (DGAs) and typosquatting techniques. These domains are then weaponized as malware and ransomware command-and-control (C&C) servers and phishing vehicles. An example is TA4903, a threat group known for posing as government entities, such as the U.S.

Department of Labor, the Department of Housing and Urban Development, the Department of Commerce, the Department of Transportation, the Department of Agriculture, and the Small Business Administration (SBA).

Agencies need visibility over these types of domains and their associated DNS records logged in passive DNS databases. The chart below shows what a first step toward DNS visibility can look like.

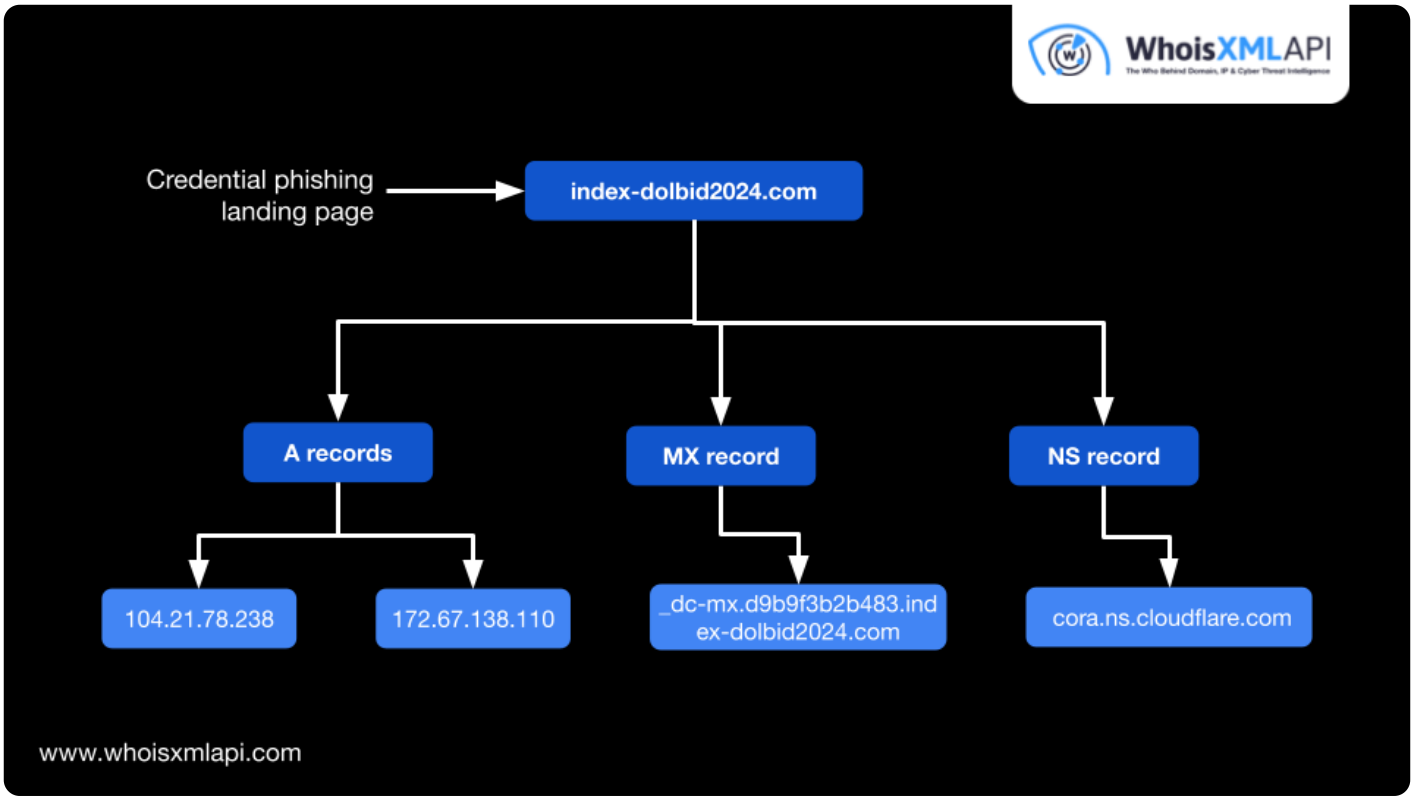

Figure 2: *Known domain indicators of compromise (IoCs) used to spoof the U.S. Department of Labor mapped to its DNS records*

Taking down malicious resources may seem like a game of whack-a-mole. New threats emerge constantly, making it challenging to stay ahead of the game. That's why global cooperation and predictive and automated adversary disruption are essential.

Supply Chain Risk Management

While on the subject of international cooperation, it's important to note that the memorandum also highlighted the fifth pillar of the NCS—"Forge International Partnerships to Pursue Shared Goals." Agencies are urged to work hand-in-hand with law enforcement agencies worldwide and strengthen their global supply chains.

In line with this goal, the third pillar (i.e., "Shape Market Forces to Drive Security and Resilience") also requires agencies to only work with software providers that comply with government-mandated secure software development practices. Many enterprise software companies have already embraced this concept, as evidenced by several signatories to the Secure by Design pledge during the RSA Conference 2024. However, it does set the bar high for the industry.

Cybersecurity solution providers must now adhere to the National Institute of Standards and Technology (NIST) guidance on secure software development and align their development processes with the recommendations for mitigating and managing risks.

Government agencies are also expected to invest in security intelligence to meticulously and continuously assess third-party risks.

Enterprise Solutions

Lastly, among the top investment priorities are solutions that can bring together disparate security functions. NCS Pillar 1 "Defend Critical Infrastructure" emphasizes the need to modernize federal defenses through investments in "department-wide, enterprise solutions."

That could mean implementing a centralized security information and event management (SIEM) system, obtaining multiple cyber threat intelligences from one solution, using an advanced attack surface management (ASM) platform, or consolidating all these in a security orchestration, automation, and response (SOAR) platform.

Regardless of how the consolidation goes, the transition should be away from siloed systems and

toward a more interconnected defense strategy for agencies with federated networks to align cybersecurity efforts, ensure consistency, and facilitate data sharing.

Conclusion

The public sector is among the most targeted by threat actors. In fact, about 40% of the incidents studied in Verizon's 2024 Data Breach Investigations Report (DBIR) zoomed in on the sector. Prioritizing cybersecurity budgets in accordance with the memorandum is anticipated to enhance federal agencies' capability to detect threats, prevent breaches, and respond to incidents more effectively.

Learn how our intelligence services can help you align with the U.S. cybersecurity budget priorities. Contact us now for more information about our data solutions.