ANALYST1™

WHAT DOES THE NEW EXECUTIVE ORDER MEAN FOR THE FUTURE OF CYBERSECURITY?

On May 12, the White House issued an Executive Order aimed at improving the nation's cybersecurity and protecting federal government networks. This order was put in place to counter increasingly sophisticated cybersecurity incidents, such as those targeting SolarWinds, Microsoft Exchange, and the Colonial Pipeline. Read on to learn the impact this order will have on the cybersecurity industry and how Analyst1 is already a step ahead.

The Executive Order breaks down the overall improvement into seven efforts:

1

Removing Barriers to Sharing Threat Information (See Section 2 of Executive Order)
The first effort focuses on making sure IT Service Providers are able to share information with the government and requires them to share certain breach information. There will no longer be contractual restrictions that bar them from sharing this information outside their organizations. This sharing between the government and private sector ensures more effective defenses of Federal departments and civilian entities.

How Analyst1 fits in: Analyst1 makes it easy for private and public sector organizations to share cyber threat information with CISA and the FBI, not just IoCs, but also the action they can take to identify and prevent potential threats. In fact, CISA is already using our product because of this.

2

Modernizing Federal Government Cybersecurity (See Section 3 of Executive Order)
Gone are the archaic standards of government cybersecurity. Outdated security models and unencrypted data have provided attackers easy access to our systems for too long. This second effort aims to force adoption of innovative best practices such as employing a Zero Trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption.

How Analyst1 fits in: Analyst1 has already been leading the charge for cybersecurity innovation in government agencies spanning the Department of Defense, Department of Homeland Security, Department of State, and the Department of Energy.

3

Enhancing Software Supply Chain Security (See Section 4 of Executive Order)
This effort ensures that software sold to the government meets baseline security standards. These standards include requiring developers to maintain greater visibility into their software and making security data publicly available. The permitted software roster will be available to the public, so everyone will know which software is deemed secure enough for the government — ideally creating a sort of "Energy Star" label of approved software.

How Analyst1 fits in: As previously stated, Analyst1 has already been implemented by many government agencies and solidified those relationships with a product they can trust.

4

Establishing a Cyber Safety Review Board (See Section 5 of Executive Order)
A Cyber Safety Review Board, comprised of both government and private sector members, will be established to convene in response to significant cybersecurity incidents. Think of it as a crisis response team that analyzes an event and makes recommendations for improvements. The objective here is to bring established thinkers together to spot vulnerabilities and work together to fix them to avoid future incidents.

How Analyst1 fits in: The group mentality is at the core of what we do at Analyst1. Every member of an organization has the power to defend it, and we give each individual the tools to **Be the 1** to impact change.

5

Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents (See Section 6 of Executive Order)
In an attempt to shift from responsive measures to preventative measures, a uniform set of procedures will be implemented for federal departments and agencies to follow so they can work with each other to better identify and mitigate threats. This standardized playbook will be the Standard Operating Procedure when it comes to cyber incident prevention and response.

How Analyst1 fits in: CISA and others are using Analsyt1 to automate, inform, and defend actions through its threat information collection and analysis capabilities.

6

Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks (See Section 7 of Executive Order)

This effort motions for a government-wide endpoint detection and response system and improved information sharing. Both are critical when it comes to detecting malicious cyber activity. Pairing teamwork and smarter, more efficient technologies will set the stage for a stronger nationwide defensive posture.

How Analyst1 fits in: Analyst1 is used to automate and augment EDR configurations before an incident. It uniquely provides rapid access to agency data that is relevant to threat, incident response, and vulnerability analysis.

7

Improving the Federal Government's Investigative and Remediation Capabilities (See Section 8 of Executive Order)

Improper logging habits can obstruct an organization's ability to detect, prevent, and learn from cyberattacks. The final effort of the Executive Order mandates cybersecurity log requirements for federal departments and agencies, creating consistent practices to greatly improve log effectiveness.

How Analyst1 fits in: Analyst1 already works with CISA to mitigate threats using comprehensive data found in logs.

For more information on the Executive Order, you can read the official document here. If you'd like to learn more about how Analyst1 steps above traditional threat intelligence platforms, you can request a demo today.

https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/