Putting the National Cybersecurity Strategy in Motion

The National Cybersecurity Strategy released by the Biden-Harris administration in March 2023 was designed to provide direction for developing and evolving the digital ecosystem that will become a key line of defense for the security of our nation. It is the latest in a series of cybersecurity guidance, strategy, and mandates released by the executive branch to help government agencies and private sector companies working with them to reevaluate and harden their approach to cybersecurity.

The latest strategy is focused on five key pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

A key theme among these pillars is the need for better coordination of knowledge and action among the many parties currently responsible for our nation's cyber defense. The data streaming approach that Confluent powers provides the framework for this shared responsibility. There are a couple of key areas where Confluent is uniquely positioned to help agencies reframe how they approach the responsibility for and the coordination of cyber defense and resilience.

Integrate federal cyber efforts

The strategy calls out the need to integrate the cybersecurity activity already happening across the government, including both the various cybersecurity centers and the counter disruption strategies already taking place. Ensuring information is shared widely and quickly is paramount to the collaborative aims of the strategy. While there are logistical, process-oriented activities that need to happen, the ability to share real-time data, patterns of interest, and findings among the groups can go a long way in building tighter integration.

One of the biggest problems dealing with cyberattacks and cyber criminals is that the many sources of data are treated in a highly siloed manner—one group may just look at system logs while another looks at network operations, and another looks at application access and performance. Still other groups may look at user behavior which is a more qualitative dataset than other security measures. This data is rarely shared across the groups, which means that activity is never placed in a greater context to flag issues before they have an impact.

Data streaming allows a source of data to be published once durably and received across any parties that need access efficiently in real time as it is created. Data streaming is built from the ground up to break down data-at-rest silos and perfectly aligns with the demands of cyber data collection and processing required to combat cyberthreats. It also provides a more cost-effective solution for meeting Office of Management and Budget mandates for retention since processing data through cyber tools can become incredibly expensive.

Defend critical infrastructure

IoT and sensors of all kinds are key components of modern critical infrastructure. While this allows them to be more effective in their mission, they open new vectors for threat actors. Most IoT devices are already leveraging data streaming to collect and process their telemetry and data. Being able to use this real-time data as part of security monitoring is critical to securing infrastructure. Disparate teams can deploy streaming services for detection, analysis, and action.

Disrupt and dismantle threat actors

The strategy states, "Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States." While agencies have a host of security tools in place, coordinating the data they gather and the action they take is a critical step that can be complex to complete with a traditional data management mindset. The most effective way to disrupt attacks is to act as quickly as possible using real-time streams of data. It's not enough to dump data into many data stores and try to keep up with retroactive queries.

Data streaming is more than just curating data and sending it to data-at-rest technologies like SIEMs. The event-driven nature means that actions can be taken immediately as threats are discovered in the streams, allowing mitigation and response steps to be initiated.

Meeting strategy goals

Improved real-time information sharing is key to securing our nation's assets and citizens. Data streaming can power the government through many of the integration and access challenges of moving across and coordinating between agencies. While cyber data sharing is important, potentially even more important is the sharing of threats that have been detected as well as the ways they can be identified. One powerful way to improve threat identification is through the use of an open and cross-platform technology like Sigma.

Sigma allows rules to be specified in a human readable format so that security operations teams can describe patterns and the corresponding sources they can be found in. These rules can then be shared across the agencies and speed the communication of emerging cyberthreats and activity. The ability to apply Sigma to both traditional at-rest technologies like SIEMs and in real time with Confluent's data streaming platform provides the environment to evolve the way the government approaches the securing of systems and data.

If you want to learn more about how Confluent can help you advance your cybersecurity goals contact us today to get started.