How Agencies Can Prepare Today and Defend Tomorrow



Agencies don't need more security data. They need the right data — and for it to be connected, accessible and ready to use before an incident occurs. IT teams already face an overwhelming volume of logs. The challenge isn't collecting more information. It's gaining visibility across hybrid cloud and legacy systems and ensuring that critical logs are available when they're needed.

At a recent GovLoop virtual event, government and industry experts discussed how a proactive approach can strengthen cyber defenses. Here are key insights from their discussion.

The Speakers



Jim Chen, Director, University Consortium for Cybersecurity Coordination Center at the National Defense University, College of Information and Cyberspace



Eric Cobb, Principal Solutions Architect, Elastic

The Key to Visibility: Usable Data, not More Data

Under the new federal logging mandate M-26-14, agencies are moving away from a "collect and retain everything" approach and toward risk-based logging focused on operational security outcomes. The priority is no longer simply collecting more data, but ensuring that the right data is clean, accessible and available when needed.

Know what assets you have.
Effective cyber defense starts with visibility. Before agencies can hunt threats, continuously monitor their environments or respond to incidents, they need to understand what assets they have, including shadow IT, temporary cloud resources and contractor systems, said Chen, with the University Consortium.

That doesn't mean collecting everything. It means identifying and prioritizing the data that matters most. "Priorities need to be set," Chen said, to ensure visibility at the device, network and application levels.

Normalize the logs.
Data must be visible and usable. That requires a common schema that aligns timestamps, identities and asset IDs across sources. "Normalize the data down into a common framework," said Elastic's Cobb.

Identity data requires similar attention. Different credential providers may represent the same person in different ways. Agencies therefore need "entity resolution," Cobb said, to recognize when multiple accounts belong to the same person.

The Priorities: Risk and Mission Impact

With so much security data in play, agencies must focus on their most vulnerable systems and mission-critical resources.

Sort systems into tiers.
Agencies can't devote equal attention to every potentially vulnerable system and application. Instead, they need to prioritize based on risk. As Chen put it, "How can we actually prioritize the tasks" needed to ensure cyber resilience? One answer is to sort systems into tiers.

Mission-critical systems should receive the highest priority, followed by business systems and then lower-risk systems. This approach allows agencies to target their analytics and make more effective use of available logging data.

Leverage SIEMaaS capabilities.
IT teams can prioritize threats by focusing first on high-value assets, such as domain controllers, identity systems, cloud control planes and critical network paths, Cobb said. They can then expand coverage using capabilities such as Security Information and Event Management as a Service (SIEMaaS).

The U.S. Cybersecurity and Infrastructure Security Agency, for example, has launched a SIEMaaS offering for federal civilian agencies featuring Elastic Security on Elastic Cloud. For federal teams with limited resources, Cobb said, the as-a-service model can help extend their reach.

What to Do Before a Crisis

Effective cyber response depends on preparation. Agencies need to practice how they will respond and ensure they have the right data when an incident occurs.

Practice incident response.
Agencies should determine how they will handle a cyber incident before one happens. "What are the courses of action you're going to have? And which course of action is the most appropriate one for this particular context?" Chen said.

"We always play war-gaming exercises," he said. Introducing unexpected challenges gives cyber defenders a chance to practice their response. Repeated exercises help establish processes, particularly for collecting and using log data across multiple cloud providers.

Hold a logging readiness review.
For each critical asset, agencies should check their data, Cobb said. "Identify what logs we need to be able to collect, make sure that we are collecting them and make sure that they are the logs that the security team needs," he said.

This information can come from a logging readiness review. In this exercise, stakeholders identify critical assets and ensure the right data will be accessible in a usable form when needed, Cobb said. Agencies can turn any gaps into action items in their M-26-14 logging plan.

By taking a proactive approach, IT teams and cyber defenders can ensure the right data is available when they need it most, helping them protect mission-critical resources.

govloop elastic

Also discussed in this session:

- Using AI to speed analytics while keeping humans in the decision-making loop
- Ensuring security amid workforce shortages and limited resources
- Treating compliance as an ongoing process, not a checkbox

To learn more, view the full session on demand.

