CRIBL | OPTIV + CLEARSHARK

Gain choice, control and flexibility over security data

Visibility and control over event logging are the keys to finding actionable data and complying with federal mandates

Edward Resh | Optiv + ClearShark

Government agencies are facing more challenges than ever, with dramatically increasing volumes of machine-generated data growing at a compound annual growth rate of 28% and given the incredible number of shapes and forms that data often takes.

Gathering data is not overly difficult, but knowing exactly what to look for and what to take action on is the challenging part of data analysis. From a security perspective, finding the proverbial needle in that haystack means identifying which data is actionable.

Optiv + ClearShark acts as a systems integrator for the leading data security technologies, and that means our customers have a number of different tools at their disposal — and those tools work together seamlessly. Specifically, our partnership with Cribl helps agencies find actionable data by using Cribl's technology to route, reduce, reformat, enrich or otherwise structure data in flight then send it to any destination.

Making it easier and faster to take action

Cribl Stream gives federal agencies an observability pipeline that provides visibility into the data as it's coming in, which makes it easier and faster to take action on information. Agencies can set up pipelines that allow them to deal only with the data they need to act on.

When federal agencies integrate Cribl Stream into their IT environments, they can quickly and securely optimize their security information and event management for cost and performance while complying with the latest government mandates, including the Executive Order on Improving the Nation's Cybersecurity.

In addition, the Office of Management and Budget's M-21-31 memo focuses on improving the federal government's ability to investigate and remediate cybersecurity incidents and specifically addresses the executive order's requirements related to logging, log retention and log management. The memo presents a maturity model for event log management, and Cribl Stream supports the most critical elements of each maturity level by augmenting an agency's current logging environment.

Creative solutions to the toughest challenges

Optiv + ClearShark has a razor-sharp focus on the federal sector and a broad-ranging cybersecurity practice. Together, we have produced a deep bench of vendor-certified engineers and solution experts who can solve even the toughest challenges facing government. At Optiv + ClearShark, we bring together talented professionals who can deliver creative solutions to what others might see as unsolvable problems.

We view ourselves as the leading partner in ensuring that government agencies can meet today's and tomorrow's cybersecurity challenges. We operate under the belief that nothing should stand in the way of making government more secure. ■

Edward Resh is a consulting engineer at Optiv + ClearShark.