Better Intelligence for Stronger Security

Next-gen SIEM technology provides cloud-native agility with unrivaled scale — all at a lower cost than legacy solutions.

Government security operations centers (SOCs) are under mounting pressure due to constrained budgets and a tight talent market. These challenges are multiplied by outdated security information and event management (SIEM) solutions that are costly, require highly specialized skills to operate and can't ingest all the data needed to safeguard today's organizations.

Fortunately, government SOCs can now benefit from a new generation of SIEM technology that helps them enhance cybersecurity while saving money and making it easier to recruit and retain cybersecurity professionals.

Key Benefits of Next-Gen SIEM

Next-gen SIEM solutions are built for the cloud and they use artificial intelligence (AI) to support fully autonomous SOC environments. This new technology surpasses earlier SIEM solutions in important ways.

More hot data: Most SIEM solutions offer only 90 days of "hot" data — information in its raw, native format that is ready to be searched. But 90 days of data isn't nearly enough. Malware often sits quietly in a system for months before it attacks. With older technologies, you'll pay extra to re-ingest data when you need to do historical lookups to identify suspicious activity. A next-gen SIEM includes 400 days of hot data, providing access in seconds to insights that could prove crucial in detecting threats.

Cloud-native: Legacy SIEM solutions may be hosted in the cloud, but that doesn't mean they were designed for the cloud from the ground up. Unlike earlier technologies, cloud-native solutions easily scale to ingest the many terabytes or petabytes of data that SOCs require for full visibility. They also support multiple concurrent queries while producing fast results. Next-gen SIEM solutions enable agencies to quickly ingest more data, store hot data longer, search it faster and limit the noise — all of which makes SOC analysts more efficient and effective.

In addition, a cloud-native SIEM is completely managed by the vendor, reducing total cost of ownership. There's no need to install and maintain hardware and software to support the solution or employ staff to manage those assets.

Superior licensing model: With legacy SIEM solutions, the more data sources the solution ingests, the more you pay. This forces agencies to limit the number of data sources they monitor. That's a risky tactic because it reduces visibility into network activity, possibly leaving your agency exposed to threats. With a next-gen SIEM, you get access to all the data you need for a single price.

Faster, easier queries: Legacy SIEM technologies employ proprietary query language. To use these solutions, agencies must recruit analysts who know that language, or invest time and money to train staff in this specialized skill. Once they learn the language, analysts often find querying a legacy SIEM to be slow and tedious, which can reduce job satisfaction.

A next-gen SIEM uses simple SQL language and offers time-saving capabilities such as click-drag-and-drop querying. This reduces the need for expensive specialists and helps lighten the load on overworked security teams. Instead of spending hours to complete a query, an analyst can get results in minutes.

Multi-tenancy: When multiple departments manage their own cybersecurity, a jurisdiction may have multiple SIEMs. That approach protects the privacy of each organization. For example,

the fire department's cybersecurity team sees just its own data, not data that belongs to the police or sanitation departments.

But this model makes it nearly impossible for the chief information security officer (CISO) and other top executives to gain visibility across all government security operations. A multi-tenant next-gen solution gives leadership an enterprisewide view while ensuring appropriate data privacy protections among departments.

Easy integration: Adding new applications or data sources into a SOC can be difficult with legacy SIEM solutions, often requiring specialized integration skills that in-house staff may lack. With next-gen SIEM technology, your vendor can build the integration for you, show you how to build it yourself or give you access to a marketplace stocked with ready-to-use integrations.

Better user experience: With a next-gen SIEM, analysts can manage all use cases in one place. The solution correlates data from all sources and domains, offering all its functionality in a single workspace to streamline workflow. By providing a seamless user experience, an advanced SIEM ensures that organizations can quickly detect potential threats and stop them before they do damage.

Faster searches and alerts: By storing data in raw format, a next-gen SIEM lets analysts search information immediately and quickly issue alerts about potentially dangerous activity. The technology also saves time by running data ingest and query processing as separate functions. This lets organizations run thousands of concurrent queries without ever blocking data ingestion.

Conclusion

With tight budgets and an even tighter talent market, today's SOCs need tools that cost-effectively strengthen security and enhance the capabilities of existing staff. Next-gen SIEM technology gives agencies the tools they need to detect and correlate suspicious events as early as possible, while reducing cost and easing workloads for security teams.

University of Oklahoma Centralizes Security

At one time, the University of Oklahoma had three separate security groups and multiple SIEM instances. When the university decided to merge those security groups and centralize their activities, it chose a cloud-native, next-gen SIEM solution to deliver information the security team needs to investigate incidents and provide an effective response.

Modern cloud architecture was a primary requirement for the new SIEM solution, says university CISO Aaron Ballio. "This was important because the university had three geographically separated campuses that were collecting logs locally, including cloud log instances from other sources.

"We also wanted advanced correlation rules, complete with predefined or customized use cases, to defend the university against threat actors," Ballio says. In addition, the team sought a system that could provide a visual representation of the environment they were monitoring, along with its overall security status in real time.

Based on those needs, the university chose a next-gen SIEM platform from Devo. "It met all of our criteria," Ballio says.

The new solution enables the university to collect and store server logs and other security data on a single platform, ensuring analysts have all the information and functionality they need to investigate and respond to any incident.

This piece was written and produced by the Center for Digital Government Content Studo, with information and input from Devo.

Produced by:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by:

DEVO

Devo is the only cloud-native logging and security analytics platform that empowers public sector IT and cybersecurity teams to log, detect, investigate, hunt and stop threats to safeguard government and citizens. The Devo Platform provides unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, all at significant savings over other solutions. **https://www.devo.com/solutions/public-sector**

SHUTTERSTOCK