Government Zero Trust Guidance: How Devo Can Help

PUBLIC SECTOR

Even with all of the confusing guidance from the government on Zero Trust, one thing is clear: the critical need for log aggregation and analysis to automate a security operation center (SOC). Following are some quotes on this important topic from key government documents and some ways Devo can help.

Devo is charting the path forward for our customers so they can realize the autonomous SOC's many game-changing benefits. The autonomous SOC leverages advanced capabilities such as automation, AI, and machine learning so teams can focus on critical issues to perform faster, more effective incident response and detection to resolve threats on large-scale, cloud and legacy infrastructures.

CISA:

"Agency logs and analyzes all access events for suspicious behaviors. Agencies perform analytics on encrypted data."

How Devo can help:

Devo provides agencies with the most scalable and performant enterprise log management for full visibility across the organization. By default, it provides 400 days of always hot data. Devo can detect suspicious behavior throughout an enterprise and includes threat detections and security content crafted by Devo SciSec, our security research and data science team, that deliver continuous value to security teams. Devo also uses automated enrichments to add context to indicators of compromise and enriches alerts with curated threat intelligence.

"Pillar: Automation and Orchestration Capability"

How Devo can help:

Devo provides several time-saving and powerful automation and orchestration capabilities natively within the Devo Platform, including SOAR. Devo provides autonomous hunting to shift the threat investigation starting point for analysts from alerts to end-to-end threat stories. Autonomous alert triage, investigation, and response at machine speed boost the efficiency of analysts by 10x. No-code capabilities across threat hunting, threat detection, and response, and patented capabilities speed both time-to-deploy playbooks and enable highly accurate response actions to stop cyberattacks in their tracks. Devo maps detection coverage automatically to the MITRE ATT&CK Framework ensuring threat coverage is meeting agency goals.

NIST:

"The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision."

How Devo can help:

Devo detects and alerts on nearly any kind of attack, including identity-based attacks, using surveillance of user access and privilege.

*"**Network and system activity logs:** This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems."*

How Devo can help:

- Devo features data collection and aggregation from multiple internal, external, and third-party sources.
- Devo centralizes logs to facilitate real-time threat and user activity monitoring, actionable threat intelligence, and analytics.

*"**Security information and event management (SIEM) system:** This collects security-centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise assets."*

How Devo can help:

Devo provides several time-saving and powerful Centralized logging in the cloud is a hallmark of Devo, but logs are of little use by themselves. Devo customers note that it's easy to deploy the Devo Platform and build playbooks for common security scenarios — a requirement under the White House Executive Order 14028. Endless extensibility with comprehensive APIs and data connectors ensure organizations can seamlessly integrate it with the best-of-breed technologies they use.

DOD:

"Logging utilizing Security Information and Event Management: Activity data is aggregated and stored within the SIEM, which provides both a security information management (SIM) and security event management (SEM) capability."

How Devo can help:

Devo collects and aggregates security information from multiple internal, external, and third-party sources, but goes further by enabling real-time threat and user activity monitoring, actionable threat intelligence, and analytics. Endless extensibility with comprehensive APIs and data connectors ensure organizations can seamlessly integrate it with the best-of-breed technologies they use.

NSA:

"Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity."

How Devo can help:

- Centralized logging in the cloud — a Devo hallmark — is the fabric that ties this heightened emphasis on cybersecurity together.
- Moreover, the lightweight Devo endpoint agent can detect configuration changes on almost any operating system.

Devo is available on the AWS Marketplace, AWS GovCloud, CDM APL, GSA Schedule, SEWP, numerous state contracts, and more. Contact public-sector@devo.com for additional information.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With 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, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.