U.S. Military Branch Chooses Devo to Make its SOC of the Future a Reality Today

CUSTOMER SUCCESS STORY

A branch of the U.S. armed forces decided two years ago to replace its legacy SIEM solution in a new cyber weapons system it planned to implement. This was due to numerous issues, primarily that the technology had fallen behind the market and would be unable to meet the mission to capture and remediate nation-state cyberthreats in less than 18 minutes and 49 seconds.

This military branch embarked on an ambitious project to implement a modern cyber weapons system, with a next-gen SIEM solution at its core, along with a "12N12" mission to reduce the number of security technologies it used to just 12 within 12 months to improve the efficiency of its cyber warriors. The branch's Cyber Command security architecture team spent two years reviewing contenders, seeking technology vendors that had all of the capabilities to make this service branch's far-reaching vision a reality. Ultimately, the team realized that only one company—Devo—met all of the requirements for the global next-gen SIEM solution. That choice was reinforced by seeing Devo Security Operations in use at one of the world's largest cybersecurity infrastructure vendors, and a referral from a leading industry analyst. Those recommendations, and a rigorous proof of concept (POC), led to the selection of Devo.

WANTED: A SOLUTION TO DELIVER THE "SOC OF THE FUTURE"

After the frustration of realizing the incumbent SIEM lacked the capabilities that would enable the armed forces unit to achieve the "12N12" mission, this branch set to work building its "SOC of the Future."

As part of the project, the branch was downsizing to just 12 security tools in 12 months, which set a high bar for the capabilities of the desired next-gen SIEM. A critical requirement for the new solution was to enable operators to detect, isolate, and remediate a cyberthreat in less than 18 minutes and 49 seconds, which CrowdStrike estimates is how long it takes nation-state hackers, once they have compromised the first machine in an organization, to move laterally toward the data they want to capture.

The military branch was increasingly displeased that most of the current-generation tools the team evaluated failed to meet its needs. Devo Security Operations, on the other hand, met all of its expectations and also had the recommendation of a leading industry analyst.

INDUSTRY: Public Sector
HEADQUARTERS: United States

CHALLENGE

This U.S. military branch needed to implement a modern cyber weapons system, with a next-gen SIEM solution at its core.

SOLUTION

Devo Security Operations, a cloud-native, next-gen platform, enables the SOC team to quickly discover and remediate threats, while providing a powerful, flexible, and visual query ability that is well-suited to operators who rotate through the SOC on a regular basis.

REQUIREMENTS

- Built-in workflows that enable analysts to detect and address threats in less than 18 minutes and 49 seconds
- Capable of ingesting more than a petabyte of data per day and quickly make it available for comprehensive security analysis
- Low TCO to meet government procurement requirements
- Easily deployed and managed around the world within AWS GovCloud

WHY DEVO

Several key capabilities quickly made Devo attractive to the customer, including:

- Devo is the first security operations solution to combine critical security capabilities with threat intelligence community collaboration, a central evidence locker, and a streamlined workflow, to make security operators more effective and reduce burnout.
- The solution empowers a dramatically improved hunting process that proactively identifies threats before they cause damage by analyzing the entire defense surface to reveal historical threat patterns and explore new data for ongoing attacks.
- Devo enables operators to quickly and intelligently query and pivot across petabytes of diverse data to identify and take action against IOCs, while also leveraging historical data to map advanced threat campaigns across time—no matter how far back they go.
- The Devo interface includes easy-to-use Activeboards that can be used by both advanced and novice security professionals. This is especially important since the majority of the organization's security operators are on two-year rotational assignments.
- The ability to easily scale, manage, and smoothly ingest large volumes of data (e.g., more than 50TB per day) and query the data instantly, as needed, during peak traffic times.
- Lower TCO is possible because Devo enables significantly reduced cloud costs for both compute and storage due to superior compression and indexing capabilities. Devo compresses data at a 10:1 ratio, which translates to just one-third the storage cost of a competitor.
- As a cloud-native application, Devo is easy to deploy and manage in AWS GovCloud.

NEXT STEPS

The military branch plans to deploy Devo at 130 bases, reflecting the multitenant capability of the Devo Platform. Other future initiatives include using Devo in an external, commercial SOC to supplement its rotating schedule of internal SOC operators.

THE BENEFITS DEVO SECURITY OPERATIONS DELIVERS TO YOUR ORGANIZATION

- **Close the gap** between detection and response
- **Improve signal, reduce noise** with entity-based detection
- **Accelerate and simplify investigations** with auto enrichment
- **Gain unparalleled visibility** across the entire threat landscape
- **Operationalize the knowledge** of the security community
- **Eliminate the swivel chair** with a streamlined workflow

WHY POUR MORE MONEY AND RESOURCES INTO SECURITY SOLUTIONS THAT ARE FAILING OPERATORS?

Legacy SIEM and log management solutions are failing to meet the needs of security operations centers (SOCs) for two primary reasons: a rapidly expanding attack surface and adversaries who go from initial access to lateral movement in minutes. SOC teams are flooded with too many false positives, broken workflows, and speed, scale, and performance issues that hinder effectiveness.

Skilled analysts—who are in short supply—are burdened with determining what's important to investigate, analyzing large volumes of data, and piecing together the workflow from detection to response. This leads to analyst burnout, missed threats, and greater risk to businesses.

Learn more at devo.com

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**.