Enterprise SecOps is Under Pressure

SEE ALL THREATS
across the entire defense surface

INVESTIGATE IN SECONDS
lowering your mean time to resolution

CAPTURE KNOWLEDGE
to enrich data and automate processes

ACCELERATE DECISIONS
with clear, actionable insight

Growth in cloud technologies and new business applications is driving exponential data growth and expanding the defense surface; this growth is directly impacting security operations. According to an ESG research survey, 72% of cybersecurity professionals said cybersecurity analytics and operations are more difficult now than they were two years ago. Clearly, SOCs are struggling to meet the demands of modern SecOps. Analysts gain access to only a portion of the data story – either due to high costs or inability to scale. Traditional security solutions and manual workflows fail to keep pace with sophisticated actors. Disconnected expertise across the community leads to a lack of centralized threat intelligence. The volume of alerts and the repetitive nature of the SOC analyst's role makes it difficult to retain top talent. The result: the SOC must undergo a transformation to more effectively empower and support analysts.

How Devo is Supporting the SOC

Today, all data is security data – and Devo helps turn that data into actionable threat insight. Devo empowers your analysts with visibility, speed, and practitioner-led workflows across security operations. Our highly scalable, cloud-native security analytics solution, built on a powerful enterprise log management platform, enables you to collect, enhance, analyze, and visualize all your event data from IT network devices and endpoints to business applications. Devo functions as a stand-alone security analytics solution. It can also extend and complement existing solutions, like a SIEM, by ingesting, storing, and analyzing data in real time, and forwarding the most relevant events to the SIEM, lowering overall costs. Devo is available as a cloud, hybrid, or on-prem deployment.

See All Threats

How do you manage the number and advanced nature of modern attacks with only part of the threat story? Empower your team with a complete line of sight across all your data to drive analytics. Devo ingests and visualizes all data, from traditional security data to non-traditional data sources and threat intelligence feeds. The interactive drag-and-drop interface enables you to then organize and correlate your data, create customized dashboards to monitor key security metrics, and interact with streaming data. The end result: you are able to quickly hunt and investigate advanced threats, understand hidden relationships, and enable rapid detection and response.

Investigate in Seconds

Remediation and recovery plans are only as effective as the accuracy and immediacy of the insight underpinning those decisions. However, sifting through large volumes of data to identify real threats wastes time and is extremely difficult. The net: you are left at risk from multiple threat vectors, while your analysts are struggling to identify the true source of an issue. Help your SOC analyst be more agile and creative with Devo. Devo's query speeds empower your team to quickly pivot, filter, and iterate on your analysis. Instantly analyze streaming and historical data with all hot, live data; enrich data with contextual intelligence; and compare results against industry frameworks for threat profiling and mapping.

Capture Knowledge

Threat intelligence formalizes your understanding of your adversaries. Devo integrates streaming data from open and proprietary intelligence feeds for threat context. Data enrichment is performed on the fly by aggregating and correlating multiple data sources using standard operations. By leveraging Devo's threat intelligence integrations, you limit the unknowns to more accurately test evolving hypotheses, establish defense mechanisms, react to ongoing breaches, and transform insight into automated actions.

Accelerate Decisions

Security operations works against the clock. It takes 66 days on average to contain a breach – and every second counts. Devo's superior speed, scale, and advanced analytics help to accelerate event triage and response by providing accurate and actionable information to your analysts. Devo provides real-time access to all your data regardless of source or time-horizon. Imagine: You can run queries across petabytes of data to validate threats, visualize the threat campaign, determine a response plan to close threat pathways, and establish repeatable alert triggers – all in one solution.

How Customers are Leveraging Devo

Leading enterprises are using Devo to expand their SOC strategy, reduce risk, cut operational costs, empower analyst creativity, and drive decision-making. One of our customers – a leading retail manufacturer with a mature SOC and terabytes of data generated every day – was struggling to scale operations and combat malicious bots. With Devo, the enterprise was able to ingest all its data for complete visibility; detect and alert to malicious bots in seconds, instead of hours; and scale security operations without degrading performance.

Take Your SOC to the Next Level

The SOC is under ever-increasing pressure to meet the demands of data growth and threat sophistication, and must evolve to support analysts' creativity with data analytics and automation. Devo sets a new standard for speed, scale, and ease of security operations. Bringing Devo into your SOC will improve the analyst experience and enable the SecOps team to flex its security muscles.

For more information on getting started with Devo, contact **sales@devo.com**.

[1] ESG Research Report, Cybersecurity Analytics and Operations in Transition, July 2017. All ESG research references and charts in this white paper have been taken from this research report unless otherwise stated.

ABOUT DEVO

Devo Technology is the data engine behind today's digitally-driven enterprises, helping organizations maximize the economic and operational value of their machine data. The Devo Data Operations Platform delivers real-time analytics on streaming and historical data to turn machine data into actions that help enterprises achieve sustained performance and growth. By collecting, enhancing and analyzing machine data, Devo provides business-driving insights for IT, security, and business teams at the world's largest organizations. For more information visit www.devo.com