Devo Platform

The cloud-native TDIR platform that combines SIEM, SOAR, UEBA, and AI

SOLUTION BRIEF

SECURITY ORGANIZATIONS CONFRONT BUDGET, TECHNOLOGY, AND RESOURCE CHALLENGES

Businesses face a myriad of security challenges. CISOs face shrinking budgets and higher levels of accountability. Rapidly evolving multi-vector threats, staff recruitment challenges, and the inability to retain experienced professionals are amplified by tightening cost controls. As a result, security organizations are continually forced to make tradeoffs between operational expenses and assurance. Combined, this has the potential to negatively impact security, profitability, and brand reputation.

With today's expanding threat landscape and the increased sophistication of attacks, security organizations are attempting to harness substantial amounts of data across an expanding number of sources. Legacy tools cannot rapidly ingest and process the needed data, and a lack of advanced analytics to predict and prevent attacks make it impossible for analysts to detect, investigate, and respond to threats in a cost-effective manner. Instead, inadequately staffed teams find themselves overwhelmed by alert noise and burdensome mundane, repetitive tasks - all while struggling to manage the infrastructure that is supposed to support them.

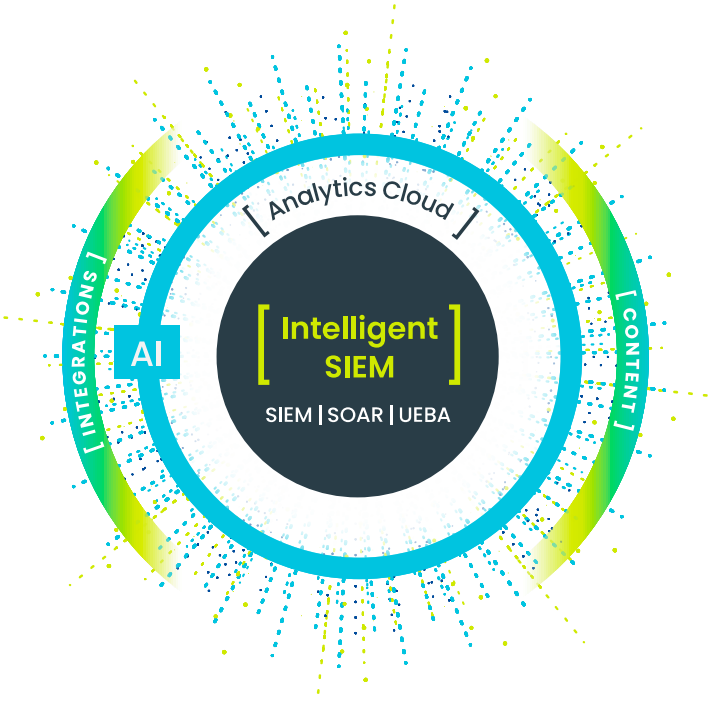
A MORE EFFECTIVE SOC SO ANALYSTS CAN WORK FASTER AT SCALE

The Devo Platform helps enterprises overcome their security challenges. Its unique implementation of speed, scale, and AI delivers a lower TCO with SaaS simplicity.

The Devo Platform lowers the time and cost of investigations. With machine-speed ingestion and rapid query response capabilities, the Platform provides integral TDIR capabilities and the speed and scale organizations need to effectively monitor the ever-changing attack surface while providing the complete visibility analysts need to proactively detect and thwart even the most insidious attacks.

Analysts work best when they can rapidly make informed decisions. The Devo Platform employs multi-layer AI, delivering ML-derived threat research, behavioral analytics, autonomous investigation, and intelligent task automation. This reduces the volume of false alerts and the manual grind that bogs analysts down while driving timely, impactful action.

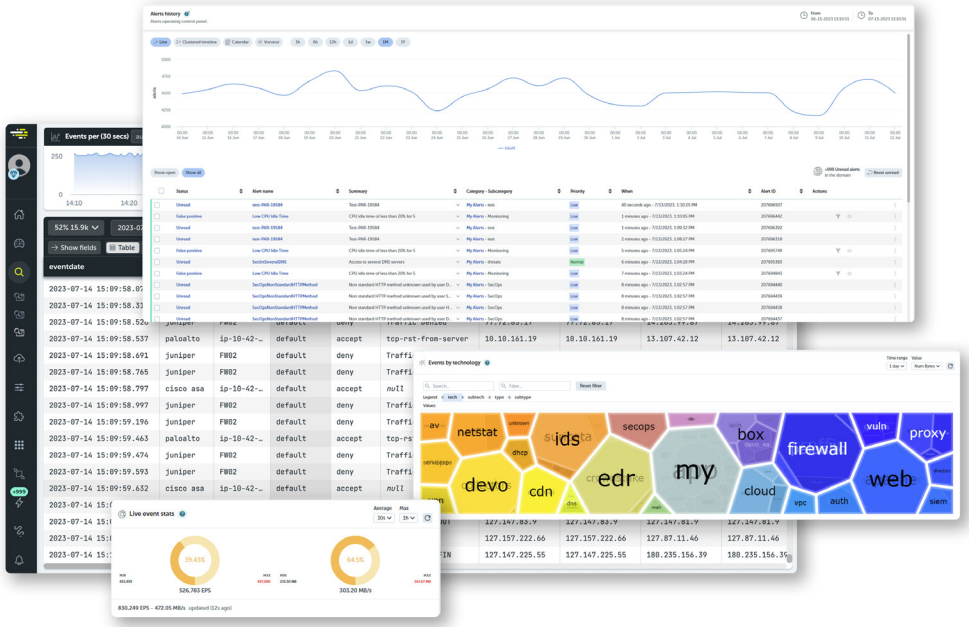
At its foundation, the Devo Platform provides access to over a year's worth of hot data in a security data lake that ingests and stores data from diverse sources. By leveraging the data lake's scalable storage and AI-enabling capabilities, security organizations improve collaboration and job satisfaction while reducing costs.



The Devo Platform boosts analyst efficiency via speed, scale, and AI.

TRANSFORM YOUR SECURITY OPERATIONS WITH LEADING CAPABILITIES

Devo Analytics Cloud



Devo Analytics Cloud is the industry's leading log and analytics solution.

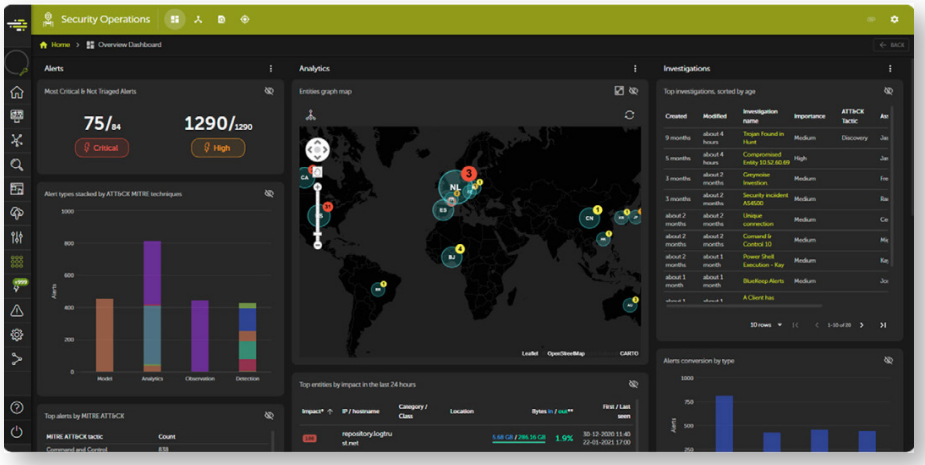
At the core of the Devo Platform, Analytics Cloud manages data at any scale and always delivers real-time results and analytics across the full data set. This is important for improving the analyst experience, reducing organizational risk and complexity, and enabling Devo to deliver differentiated AI capabilities.

- **Ubiquitous ingestion:** Consume and enrich any data type in real time. Store it hot for 400 days
- **Real-time analytics and alerts:** Data is searchable immediately upon ingestion, and alerts fire with sub-second latency
- **Single data set:** Unlimited scalability provides complete visibility for effective decision-making

Devo Intelligent SIEM

Devo Intelligent SIEM delivers on the need for a SaaS-based, scalable, and high-performance SIEM integrated with UEBA, SOAR, and the power of AI.

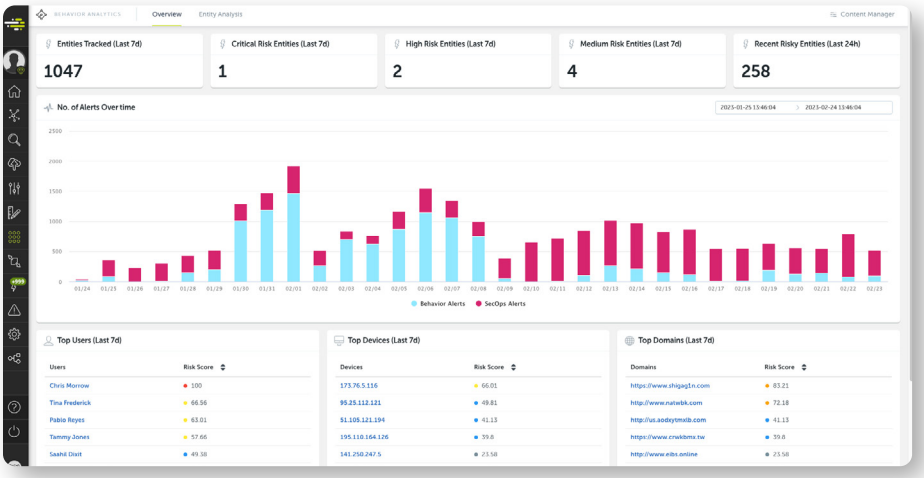
Security Operations



Devo Security Operations provides a singular view of risk posture, security operations and threat detection.

Gain a singular view of your risk posture, security operations, and threat detection by leveraging MITRE ATT&CK framework context, Devo Exchange security content, and automated enrichment and correlation across cloud, hybrid, and on-premises security environments. Learn more about Devo Security Operations.

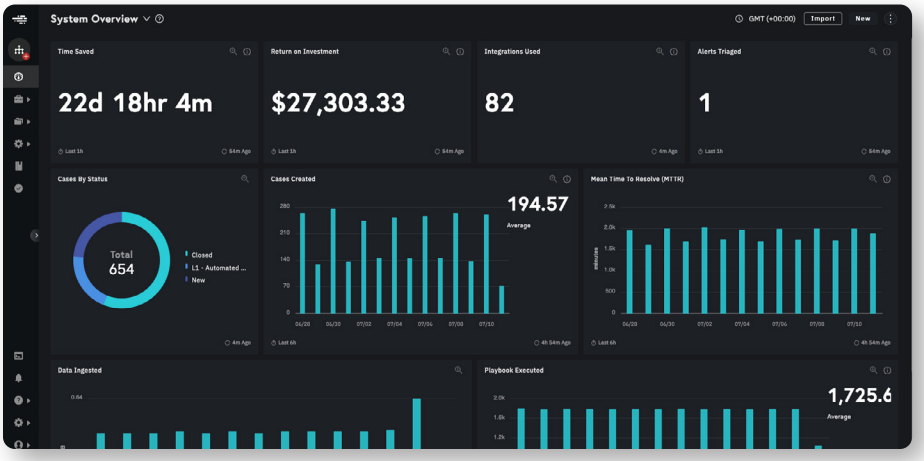
User and Entity Behavior Analytics (UEBA)



Devo Behavior Analytics identifies threats and anomalies across cloud, network, and user behavior-driven events.

Identify threats and anomalies across cloud, network, and user behavior-driven events via analyst-centered workflows by leveraging ML behavioral models, risk-based alerting, and analytics. Out-of-the-box self-service customization options enable security teams to tailor their security experience. Learn more about Devo Behavior Analytics.

Security Orchestration, Automation, and Response (SOAR)



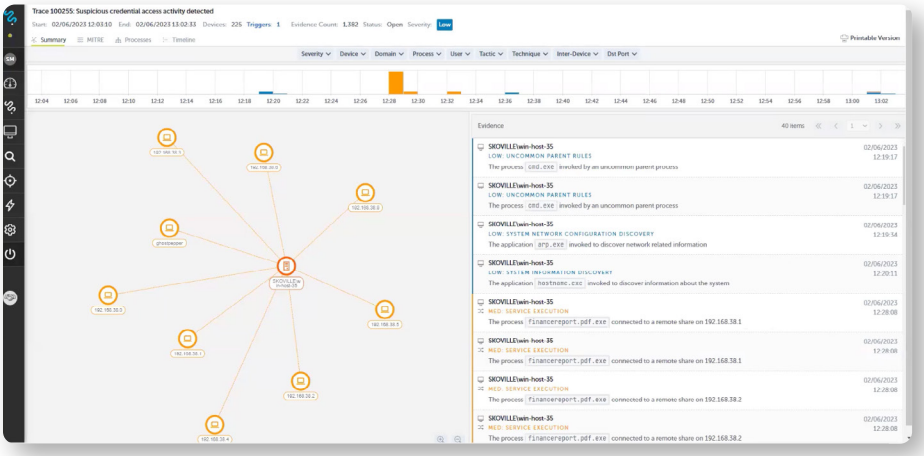
Devo SOAR utilizes AI-powered playbooks and decision automation to safeguard against threats.

Use AI-powered playbooks and decision automation to proactively safeguard against threats. Benefit from automated triage, no-code SOAR playbooks, intuitive investigations, and case management. Learn more about Devo SOAR.

Autonomous Threat Detection and Incident Response (TDIR)

Threat Detection and Incident Response (TDIR) is a technology-driven process that combines advanced threat detection with efficient incident response mechanisms. Combined with the automated response capabilities of SOAR, TDIR further advances the efficiency of the SOC with analytic and AI-derived, validated threat data in a single platform. This eliminates the all-to-common swivel chair investigation process while preserving data fidelity and speeding up threat remediation.

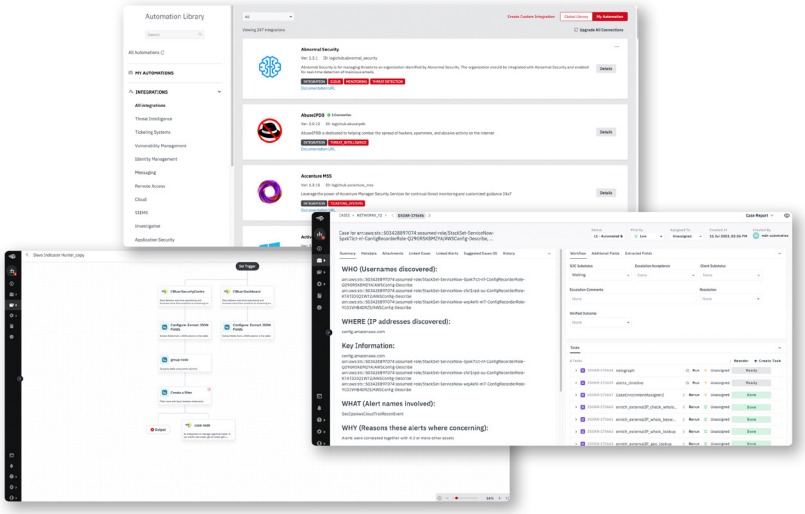
Devo advances the capabilities of TDIR further by integrating AI and automation. A key element of the Devo Platform, DeepTrace's autonomous, AI-driven TDIR improves SOC efficiency by continuously learning from past incidents while monitoring new data and threats. In addition to improving analyst capabilities, this self-learning approach continuously improves the Platform's capabilities over time, ensuring timely and up-to-date defense against attacks. Additionally, automation relieves analysts from mundane, repetitive tasks, enabling them to focus on the more complex aspects of threat detection and response.



Devo DeepTrace advances the capabilities of TDIR through the integration of AI and automation.

Devo DeepTrace is the industry's only autonomous, AI-powered TDIR solution. DeepTrace advances threat analysis and identification by combining cutting-edge analytics and attack-tracing AI. This empowers analysts to autonomously perform investigations at machine speed, enabling them to respond quickly to emerging threats. Learn more about Devo DeepTrace.

TURN DATA INTO ACTIONABLE INTELLIGENCE WITH MULTI-LAYER AI



The Devo Platform's AI-powered analytics continuously learns and improves to enhance threat-hunting accuracy.

The Devo Platform contains the best-in-class AI-powered analytics and automation, delivering the fastest detection and response times with a predictable and affordable cost basis.

Smarter decision automation: Intelligent SIEM continuously learns and improves its threat-handling accuracy to reduce the burden on analysts while scaling effortlessly to stay ahead of ever-increasing SOC workloads.

Autonomous threat detection: AI-powered TDIR supercharges analysts so they can perform investigations at machine speed.

Unmatched analytics: The industry's fastest query performance and real-time access to raw log data provide the foundation of Devo's security-targeted AI.

TRANSFORM YOUR SOC INTO A THREAT INTELLIGENCE AND RESPONSE HUB

Cloud-native infrastructure for reduced operation costs

The Devo Platform was built in the cloud, enabling it to scale beyond legacy solutions. Its machine-speed ingestion ensures that analysts can easily harness the full potential of their data, with access to the latest threat intelligence and out-of-the-box threat content, all while reducing TCO.

Leading edge threat detection with AI-driven security analytics

Rapid ingestion and instant query response across real-time and historical data provide the ideal environment for long-tail, multi-vector analytics. Analysts can rapidly and accurately triage, detect, identify, and respond to threats to make informed decisions and confidently take decisive action.

A more effective security team with upskilled and unburdened SOC analysts

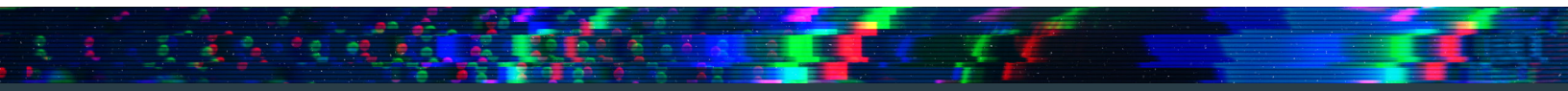
With its SaaS model, the Devo Platform is seamlessly managed and maintained by Devo. Therefore, analysts don't need to spend time maintaining their Devo Intelligent SIEM environment. Instead, they can focus on high-value activities, collaborate, and augment their abilities while experiencing less burnout and higher productivity.

Improved responses through increased collaboration and accuracy

The Devo Platform uses behavioral analytics and seamlessly integrated SIEM, SOAR, and AI to assist security teams in effectively monitoring, detecting, and investigating cyber threats as a collaborative team. Devo's advanced case management streamlines investigative workflows so teams can optimize and speed up the response process.

Are you ready to learn more about the Devo Platform and Devo Intelligent SIEM?

Contact your sales representative to schedule a demo or visit devo.com



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native security analytics platform that combines the power of people and intelligent automation to confidently defend expanding attack surfaces. An ally in keeping your organization secure, Devo augments security teams with AI — enabling you to continuously scale SOC efficiency, increase the speed of threat detection and response, and gain greater clarity to empower bold action, minimize risk, and maximize outcomes. Learn more at **www.devo.com**.