Devo Security Data Platform

Unlock the full potential of your data to accelerate threat detection and response.

SOLUTION BRIEF

SECURITY TEAMS CONFRONT DATA, TECHNOLOGY, AND RESOURCE CHALLENGES

Organizations are confronted with a perfect storm of security challenges as the exponential growth of data collides with an expanding attack surface. Legacy SIEM solutions, designed without a data-at-scale mindset, struggle with diverse data sources and an increasing volume of events. Their inability to simultaneously ingest and analyze these vast amounts of data leads to vulnerabilities that attackers can exploit.

As the attack surface expands and budgets shrink, the conventional strategy of incremental enhancements, such as upgrading hardware and increasing computing power, is inadequate. And until the underlying data problem is resolved, the potential of AI will remain unattainable due to its need to train models on extensive datasets.

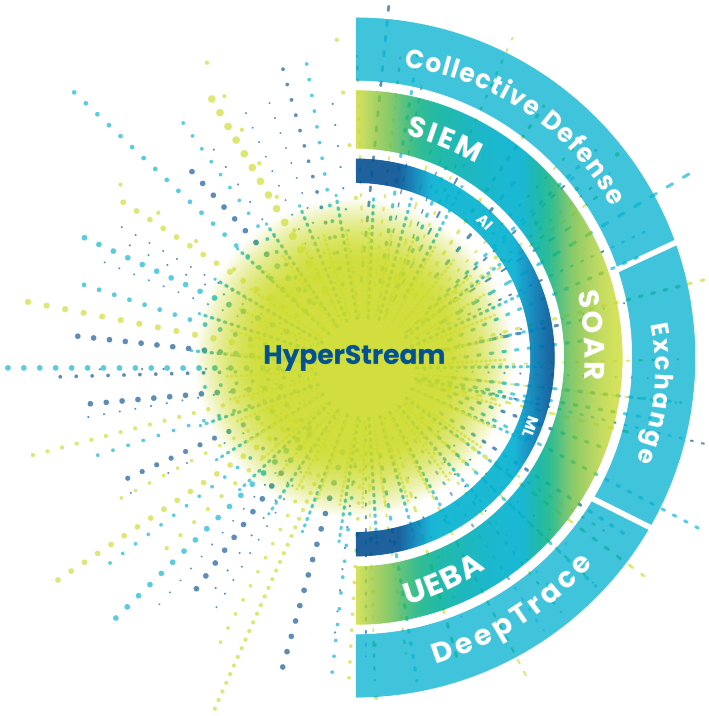
Moreover, the escalating costs of collecting, storing, and searching this expanding data volume using outdated SIEMs impede investments in pivotal areas such as augmenting headcount and providing essential skills training in the SOC.

Only a cutting-edge security data platform capable of real-time ingestion, analysis, and automation can address these challenges.

WORK FASTER AT SCALE WITH THE DEVO SECURITY DATA PLATFORM

The Devo Security Data Platform, powered by proprietary HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence that organizations require to unleash the power of the SOC.

Speed and Scale	Real-Time Analytics	Actionable Intelligence
Achieve unmatched visibility as your infrastructure scales and evolves **Act faster** than the threat actor with sub-second speed **Always get the full picture** by maintaining data in its original form **Find the signal** over an extended time horizon with always-hot data	**Find threats with zero lag** with streaming alerts **Pinpoint threat actor actions** with full context and precision **Assess threat trends** across the entire environment at scale	**Visualize your threat posture** and prove the efficacy of your security operations **Get the full attack story** within minutes with attack-tracing AI **Identify emerging threats** with community-based threat intelligence



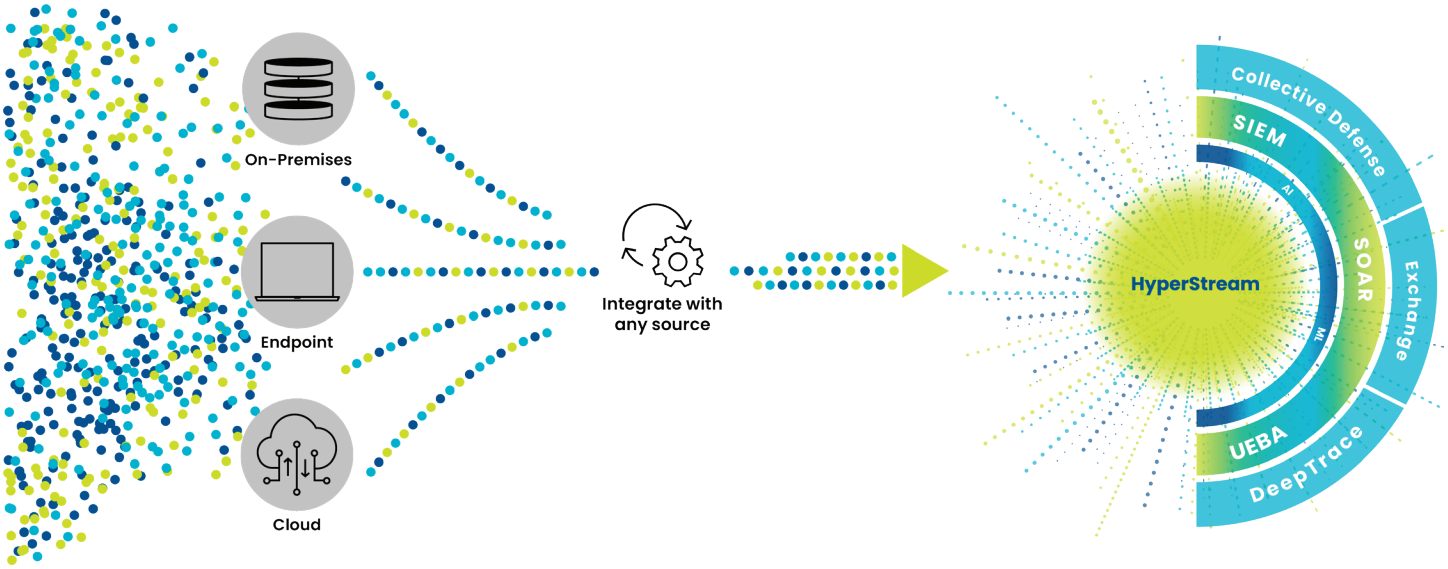
The Devo Security Data Platform, powered by HyperStream, provides speed and scale, real-time analytics, and actionable intelligence to protect growing and evolving environments.

HyperStream: The power behind the Devo Security Data Platform

HyperStream is Devo's proprietary data analytics engine that enables real-time actionable insights. HyperStream enables limitless data ingestion and querying, adapts to any infrastructure for seamless integration, and scales linearly on demand. With HyperStream, the Devo Security Data Platform unlocks the full potential of data to accelerate threat detection and response across the most demanding environments.

HyperStream enables the Devo Security Data Platform to provide the following capabilities:

- **No indexing or normalization at ingestion,** enabling SOCs to act instantly against any and all of their data.
- **Streaming architecture for real-time insight,** ensuring that SOCs can pivot in real time to detect and track threat actors.
- **Enriched data on-query for unlimited context,** speeding threat investigations by arming SOCs with actionable context.
- **Queries without limits,** enabling security analysts, automation playbooks, and AI workloads, such as Devo DeepTrace, to use massive amounts of data to detect, investigate, and remediate cyber threats.
- **AI and ML enablement,** powering the next generation of security capabilities for SOCs.
- **Cost-optimized architecture,** saving buyers money while supporting massive amounts of data.



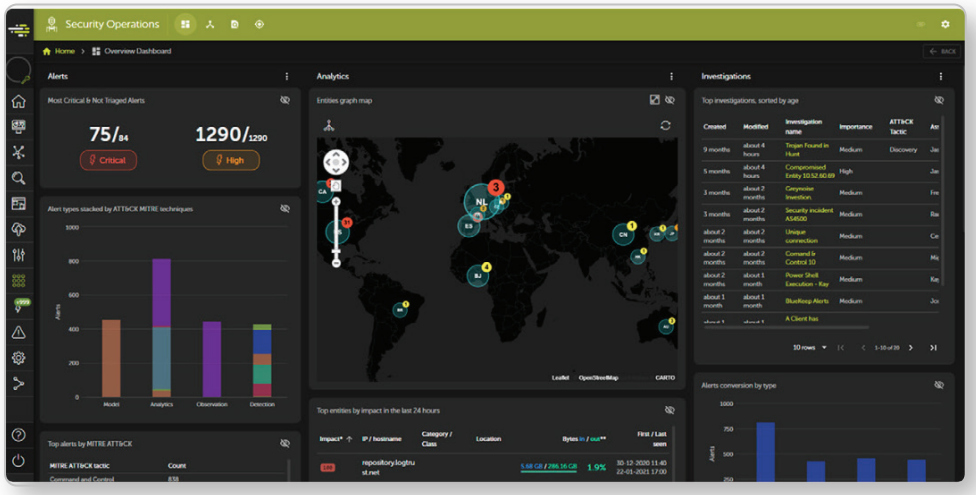
Devo HyperStream enables limitless data ingestion and querying and fuels the end-to-end security capabilities of the Devo Security Data Platform.

TRANSFORM YOUR SECURITY OPERATIONS WITH INNOVATIVE CAPABILITIES

Devo Intelligent SIEM

Devo Intelligent SIEM is a high-performance, SaaS-based SIEM that integrates UEBA, SOAR, community-based security content and threat intelligence, plus autonomous investigations and threat hunting.

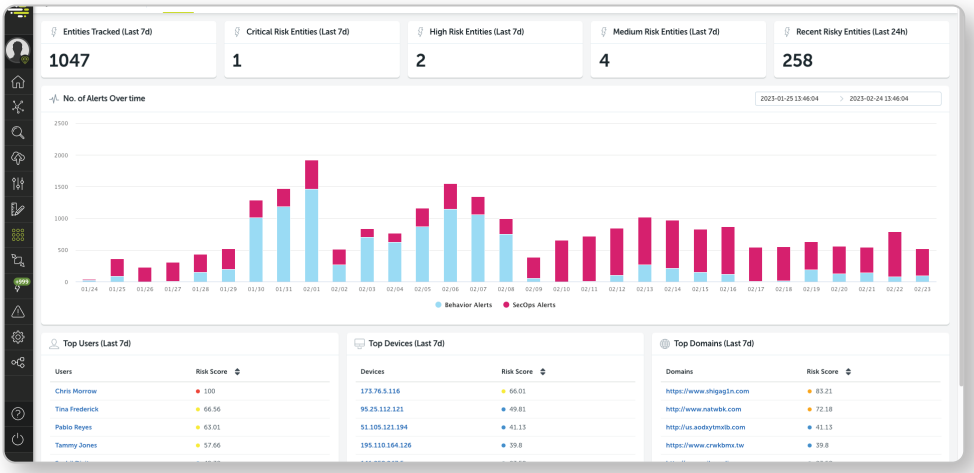
Security Operations



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, case management, and automated enrichment and correlation across cloud, hybrid, and on-premises security environments. Learn more about **Devo Security Operations** and **Devo Exchange**.

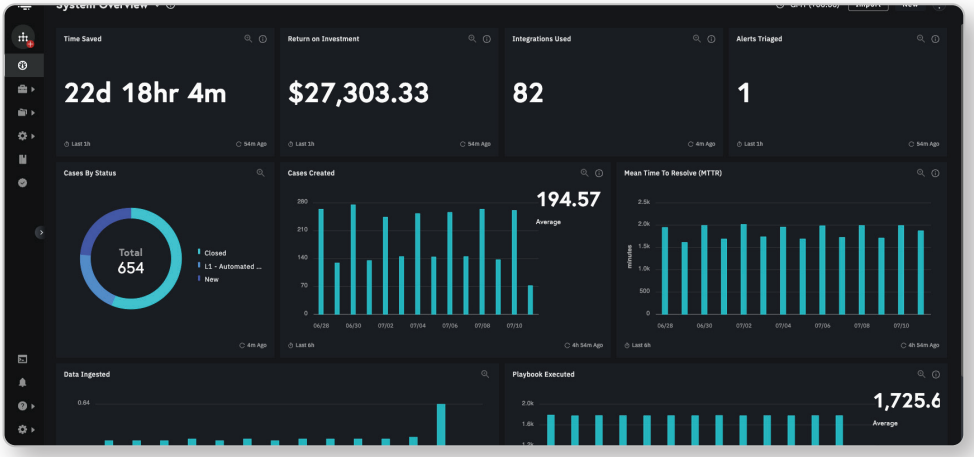
User and Entity Behavior Analytics (UEBA)



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 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**.

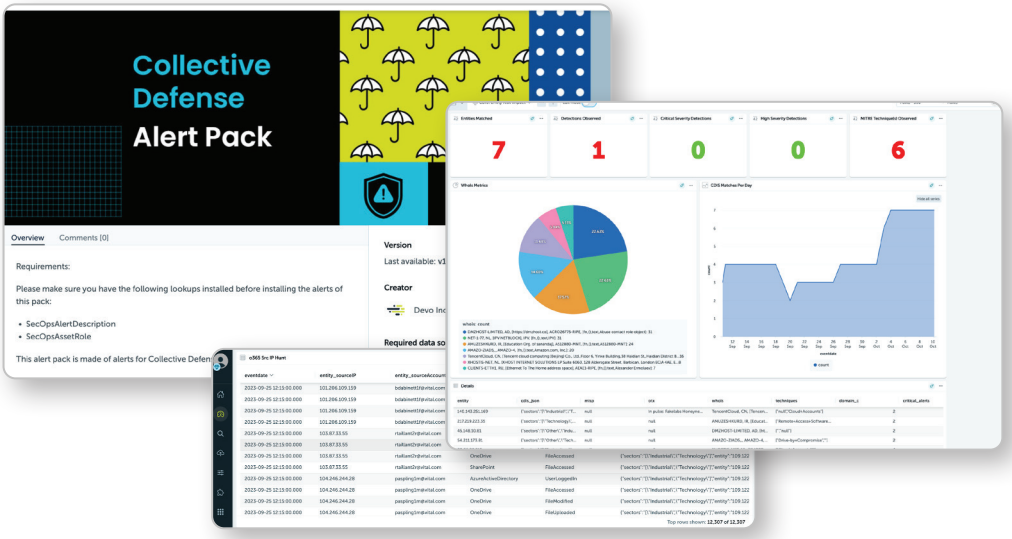
Security Orchestration, Automation, and Response (SOAR)



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**.

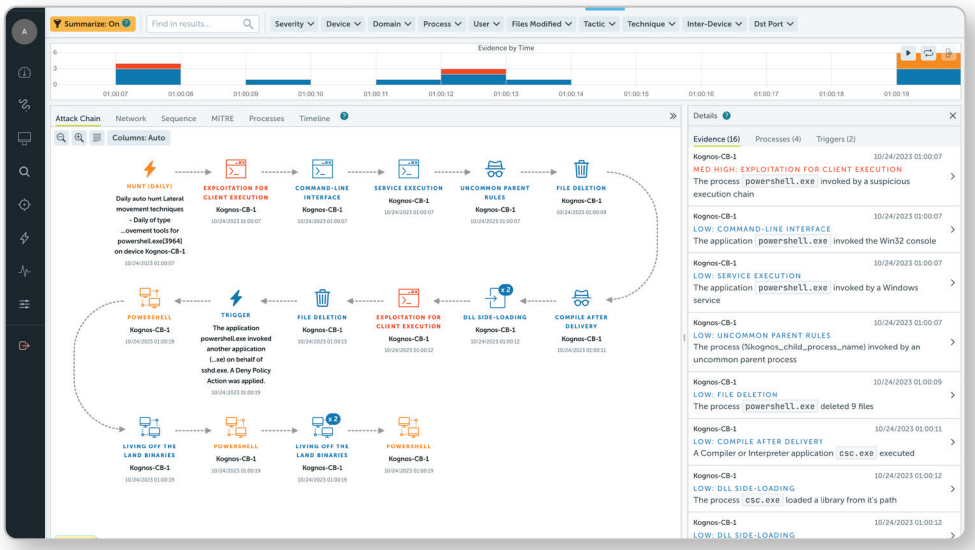
Community-based threat intelligence



Devo Collective Defense is a community-based intelligence-sharing program that provides knowledge of threat activity and trends.

Leverage knowledge of threat activity and trends across the Devo user community to identify insights, trends, and Indicators of Compromise (IOCs). Devo users have exclusive access to an integrated intelligence feed, out-of-the-box content, and alert enrichment. Learn more about **Devo Collective Defense**.

Autonomous Investigation and Threat Hunting



Devo DeepTrace advances the capabilities of TDIR by integrating AI and automation.

Autonomously perform investigations at machine speed with attack-tracing AI, relieving analysts from mundane, repetitive tasks so they can focus on the more complex aspects of threat detection and response. Learn more about **Devo DeepTrace**.

TRANSFORM YOUR SOC INTO A THREAT INTELLIGENCE AND RESPONSE HUB

Cloud-native infrastructure for reduced operation costs

With its cloud-native, SaaS model, the Devo Security Data 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.

Leading edge threat detection with AI-driven security analytics

Rapid ingestion and sub-second 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 take decisive action.

Improved responses through increased collaboration and accuracy

The Devo Security Data Platform seamlessly integrates SIEM, behavioral analytics, SOAR, community-based security content and threat intelligence, autonomous investigation and threat hunting to help security teams effectively monitor, detect, and investigate cyber threats as a collaborative team. Devo's advanced case management streamlines investigative workflows so organizations can optimize and speed up the response process.

A more effective security team with upskilled and unburdened SOC analysts

Automation facilitates the acceleration of routine and repetitive tasks, such as data correlation and analysis, surpassing the speed of manual processes. HyperStream enables analysts to automatically ingest, query, and analyze data. The Devo Security Data Platform enhances security team capabilities with AI-powered decision-making and autonomous investigations. This enables analysts to concentrate on high-value activities, fostering collaboration and skill augmentation while mitigating burnout and increasing overall productivity.

Are you ready to learn more about Devo Security Data Platform?
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**.