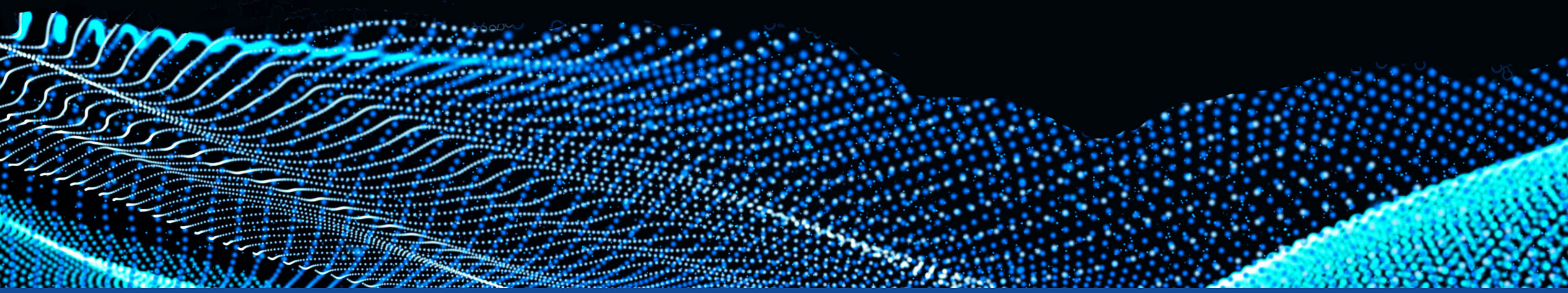

# Devo Security Operations

Everything your analysts wish a SIEM could be

## The Devo vision for the next-gen SIEM

Today, SOC analysts lack visibility across the expanding attack surface, are overwhelmed by the volume of security alerts, and struggle to identify and act on threats due to a lack of context on the threats and entities involved. The next-gen SIEM must evolve to become the central hub for all data and processes within the SOC, not simply provide alert management for traditional security events.

- **Behavioral analytics:** SIEM must make ML-based behavioral observations of users and systems on the network the foundation of detection. This shift is key to enabling analysts to move beyond restrictive rules-based detection to reliably identify high impact threats and gain the context required to act.
- **Community collaboration:** SIEM must foster a community among peers and with providers by operationalizing threat sharing of curated proprietary, open, and commercial intelligence, and providing access to a community of global CERTs. This enables SOCs to stand together through collaborative analysis and prevents repetitive investigative efforts.
- **Analyst insight:** SIEM must capture and learn from analyst behavior to help automate investigations, improve decision-making, and help speed onboarding of new security talent by incorporating best practices, continual learning, and analyst intuition.
- **Orchestration & automation:** SIEM must enable rapid threat response by integrating with solutions that automate manual, repetitive processes and orchestrate the incident response workflow.
- **Cloud:** SIEM must be cloud native, combining SaaS-based services with core product capabilities, and offer flexible deployment models that enable enterprises and MSSPs to streamline security operations as they shift to the cloud.

Finally, these capabilities must be delivered through a scalable, extensible data analytics platform, purpose-built for petabyte-scale data growth and the real-time and historical analytics demands of the modern SOC.

# Tech Preview

Devo Security Operations is a next-gen, cloud-native SIEM that enables analysts to gain complete visibility, reduce noise, and focus on the threats that matter most to the business.

### Bring together all security-relevant data

Gain a single, unified view of all security-relevant data and context – from traditional security sources to IT infrastructure, cloud, and business application data – enabling greater visibility into the threat landscape.

### Magnify analyst intuition

Improve identification, triage, and investigation of high impact threats by combining threat intelligence, behavioral observations, and context at scale.

### Turn intuition into automated, repeatable actions

Capture and continuously learn from analyst behavior to automate investigations and improve decision-making.

## Use cases

**Detect & hunt high impact threats in real time**

**Triage & investigate high confidence alerts**

**Increase signal with rich behavioral analytics**

**Enhance response speed through actionable insight**

## Learn more about Devo Solutions at [devo.com](devo.com)

Devo unlocks the full value of machine data for the world's most instrumented enterprises, putting more data to work now. Only the Devo data analytics platform addresses both the explosion in volume of machine data and the new, crushing demands of algorithms and automation, enabling enterprises to realize the full transformational promise of machine data to move the business forward. Visit www.devo.com to learn more.

www.devo.com