Devo and Kognos

Achieve the Autonomous SOC with AI, Automation, and the Industry's Most Scalable SIEM

SOLUTION BRIEF

DEVO + KOGNOS

A Devo Company

PUT AUTOMATION TO WORK FOR YOUR SECURITY TEAM — AT CLOUD SCALE

Today's organizations face many challenges, from the need to secure complex infrastructures to a fast-evolving threat landscape and a constant struggle to retain cybersecurity talent. All of that is in addition to keeping their day-to-day business operations running smoothly while fostering innovation.

The autonomous SOC addresses these challenges and reinvents how security professionals work by providing complete attack-surface visibility, security analytics to pinpoint threats, and access to security community expertise and content. It empowers security teams to become more productive with automation and AI so teams can punch above their weight and perform fast, effective threat detection and incident response.

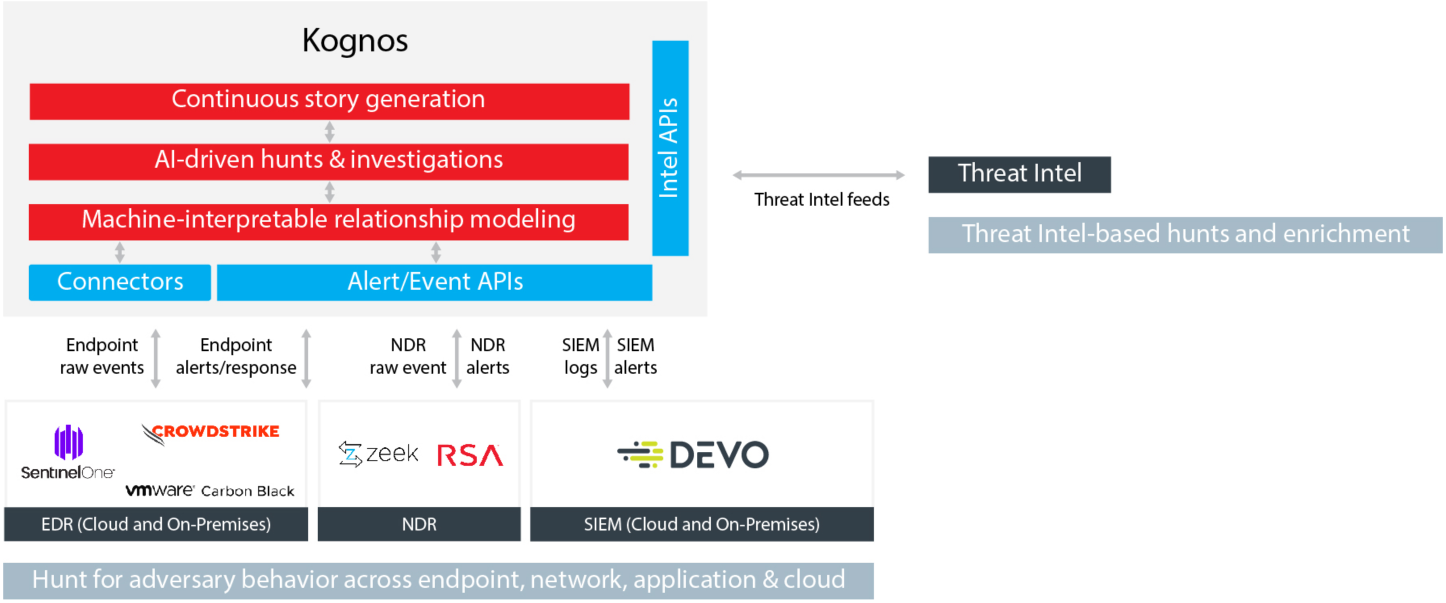
Devo and Kognos underpin the autonomous SOC by combining logging and security analytics with attack-tracing AI to accelerate the triage, investigation and hunting for threats. Now security teams can cut through the noise and focus on critical, high-impact tasks to protect their organizations against the threats that matter most.

YOUR SIEM SHOULD TELL STORIES, NOT CREATE ALERTS

Every attack has a story. A sequence of steps an adversary takes to learn, access and control a victim's resources and data. Unfortunately, the tools in today's SOC predominantly focus on alerts. These individual point-in-time indicators of malicious activity force SOC analysts to manually uncover the attack stories behind the thousands of alerts they receive every day. The combination of Devo and Kognos empowers the SOC to move beyond alerts by enabling analysts to begin an investigation with an attack story — a full blueprint of the attack and a complete understanding of its impact.

BEGIN WITH THE FULL BLUEPRINT OF AN ATTACK WITH AUTONOMOUS TRIAGE, INVESTIGATION AND HUNTING

Devo and Kognos


Kognos
Continuous story generation
AI-driven hunts & investigations
Machine-interpretable relationship modeling
Connectors
Alert/Event APIs
Intel APIs
Threat Intel feeds
Threat Intel
Threat Intel-based hunts and enrichment
Endpoint raw events
Endpoint alerts/response
NDR raw event
NDR alerts
SIEM logs
SIEM alerts
SentinelOne
CROWDSTRIKE
vmware Carbon Black
zeek
RSA
DEVO
EDR (Cloud and On-Premises)
NDR
SIEM (Cloud and On-Premises)
Hunt for adversary behavior across endpoint, network, application & cloud

Organizations today are overwhelmed with volumes of data, and they lack the ability to analyze it all and identify the attack signals within it. That's where Devo excels by collecting data from across the entire attack surface — from any source, at any scale — and providing advanced analytics and threat detection. These alerts feed directly into the Kognos attack-tracing AI engine that mirrors how analysts work by asking thousands of questions that dig into the data to understand the attack and providing end-to-end threat stories that radically improve analyst decision-making and shift their starting point from an alert to a full attack blueprint.

The powerful combination of Devo and Kognos automates key aspects of the threat lifecycle — detection, triage, investigation and hunting — eliminating the repetitive manual tasks that lead to analyst burnout and SOC inefficiency. It also accelerates incident response by continuously updating a real-time view of all assets and their relationships, which enables you to assess the potential impact on your organization with a clear view of what needs to be remediated.

Together, Devo and Kognos form the foundation of the autonomous SOC by providing the data analytics, automation and AI that SOC teams demand to keep pace with sophisticated adversaries while avoiding analyst burnout.

Are you ready to learn more about Devo and Kognos?
Contact your sales representative to schedule a demo or visit our website to learn more.

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**.