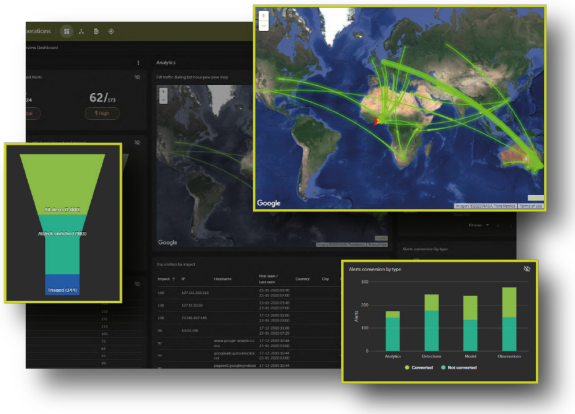
DATA SHEET

Devo Security Operations

Transform the SOC by Reinventing the SIEM

- **Close the gap** between detection and response
- **Improve signal, reduce noise** with entity-based detection
- **Accelerate and simplify investigations** with auto enrichment
- **Gain unparalleled visibility** across the entire threat landscape
- **Operationalize the knowledge** of the security community
- **Eliminate the swivel chair** with a streamlined workflow



WHY POUR MORE MONEY AND RESOURCES INTO SECURITY SOLUTIONS THAT ARE FAILING ANALYSTS?

Legacy SIEMs are failing to meet the needs of security operations centers (SOCs) thanks to a rapidly expanding attack surface and adversaries who go from initial access to lateral movement in minutes. Skilled analysts, who are in short supply, are burdened with determining what's important to investigate, analyzing large volumes of data, and piecing together the workflow from detection to response. This leads to analyst burnout, missed threats, and greater risk to businesses.

SOC teams are flooded with too many false positives, broken workflows, and speed, scale and performance issues that hinder effectiveness. Analysts must try to manually close the gap between detection and response. But it's not working.

IT'S TIME FOR A NEW APPROACH

Devo Security Operations is the first solution to combine critical security capabilities with auto enrichment, threat intelligence, community collaboration, a central evidence locker, and a streamlined analyst workflow, making security analysts more effective and helping transform the SOC. Analysts no longer require multiple tools or manual processes to assemble the data, context and intelligence required to identify and investigate the threats that matter most. Devo puts this information at analysts' fingertips across the entire threat lifecycle.

Devo arms analysts with everything they need for context-rich triage and investigation, slashing the time from detection to response. Devo Security Operations leverages powerful data analytics, a streamlined workflow, and entity modeling—all with a security practitioner's mindset. Analysts can act on context-rich alerts and investigations, giving them a greater understanding of the overall environment and the impact of threats

"There is a need for a solution that incorporates new technologies to extend the capabilities of often-overtaxed security teams. Too often, these technologies are fragmented and poorly integrated. Devo Security Operations fills this need by combining key functionalities—including entity analytics, automation and hunting—into a single integrated platform."

Scott Crawford, research VP, information security, 451 Research

BRING TOGETHER ALL SECURITY-RELEVANT DATA FOR TOTAL VISIBILITY

Powered by the Devo Data Analytics Platform, Devo Security Operations provides the scale and performance required for petabyte-scale data ingestion and analysis. SOCs can centralize data from any source, time horizon, or environment in a single location, eliminating the inefficiency of multiple data siloes and tools.

RELIABLY IDENTIFY AND INVESTIGATE HIGH-IMPACT THREATS WITH ENTITY ANALYTICS

Devo classifies, associates and models entities, providing a deep understanding of an organization's environment and business behaviors for faster and more effective detection and investigation. Entity modeling is based on real-time entity behavior so analysts can understand an entity's magnitude of change, such as when a server uses client software to access a client while still serving the application.

IMPROVE SIGNAL-TO-NOISE RATIO AND FIND HIDDEN SIGNAL WITH HIGH-SIGNAL ALERTING

Devo Security Operations triggers alerts with a variety of detection methods: security analytics based on practitioner experience; machine learning insights; observations from entity modeling; and known threat activity. The high-signal alerts in Devo reduce MTTR by focusing analysts on the alerts that matter most. Devo includes hundreds of pre-built alerts and supports custom alerts. Analysts also can define alert policies, set up and manage how and to whom alerts are delivered, and curate an alert list.

EASILY HUNT ACROSS ALL DATA AND CONTEXT

The Devo Hunting Workbench enables threat hunters to run queries across any volume of data, any number of sources, and any time horizon, using multiple filter criteria to proactively identify threats. The Workbench's different modes of hunting, which empower both experts and novices, include:

- Multi-table search: Hunt across multiple data tables at once using multiple filter criteria.
- Query replay: Look back across previous filters and apply them in new hunts.
- Expert mode: If an investigation query exists, or an analyst knows the Devo query language, they can ask questions in LinQ.

Threat hunters can apply their findings to investigations. They can add relevant tables, queries or filters as context to an existing investigation or use them to start a new one.

SIMPLIFY AND ACCELERATE INVESTIGATIONS THROUGH AUTO ENRICHMENT

Devo automatically pre-populates alerts and investigations with actionable, real-time data and context including threat data, priority scoring, MITRE ATT&CK labels, custom SOC taxonomy, entity impact, and more. This gives analysts a context-rich picture of an incident, without having to manually query data, speeding up the investigative process and improving SOC efficiency.

CONSUME THREAT DATA AND OPT TO SHARE FINDINGS THROUGH THE THREAT DATA SERVICE

Devo supports rapid extraction, consumption and analysis of indicators from proprietary, open, and paid feeds, and from partners. The Threat Data Service leverages the Devo MISP infrastructure to enrich alerts and investigations with attributes and indicators in any format. Users can choose to privately share indicators, sightings and events with other Devo users, organizations, or the broader MISP community. Devo developed the Sightings methodology to connect users searching for or detecting the same indicators. Sightings indicate how many times a given object appears and when it has been seen.

QUICKLY DIVE INTO THE DFIR EVIDENCE TOOLKIT WITH ALL APPLICABLE EVIDENCE

Devo provides a DFIR Evidence Toolkit for centralized evidence capture and analysis, such as PCAPs, memory dumps, PDFs, images, and context. The DFIR Toolkit includes PCAP analysis for network traffic data and malware analysis via Viper or VirusTotal, enabling investigators to centralize deeper evidence in one location.

Learn more about Devo Security Operations at devo.com/siem/

Feb. 2020