Threat Detection with Devo
Stop Adversaries in Their Tracks

The more quickly a threat is found, the sooner a response can be launched. However, the art of threat detection is becoming increasingly challenging to master, as attackers are regularly developing new ways to evade defense technologies. In today’s modern SOCs, threat detection requires a deep understanding of the global threat landscape, as well as the specific risks impacting the enterprise—a big ask. Analysts can no longer continue the difficult and time-consuming process of piecing together disparate data, industry intelligence, and new findings with manual effort alone.

TRANSFORM ALERTS INTO ACTION
Devo Security Operations empowers analysts to better apply their expert knowledge and quickly mature SOC operations to improve effectiveness. Devo combines advanced threat detection, threat investigation, forensic analysis, and threat intelligence in an integrated workflow, so analysts can quickly isolate points of compromise and prioritize potential threats, leveraging automation to quickly transform these alerts into action.

HELPING ANALYSTS FOCUS ON THE THREATS THAT MATTER—BEFORE THEY HARM THE BUSINESS
Attackers maintain networks of shared intelligence and use machine learning and artificial intelligence to constantly change how they infiltrate enterprises. Threat detection methodologies must continuously evolve to keep pace with these modern TTPs. With Devo, all security data can be collected, accessed and enriched with ease, to intelligently inform detection methods and analytics. The millisecond query speeds and unlimited scale enable teams to quickly analyze and correlate across petabytes of security data.
INCREASE SIGNAL, DECREASE NOISE
Devo Security Operations speeds response times by automatically delivering critical alerts to analysts. Devo Security Operations is built with an entity focus—the classification, modeling and associations of entities become the foundation for reliably detecting and investigating high-impact threats. Devo Security Operations offers four types of advanced alerting:

- **Observations**: Identify malicious events by applying entity behavioral analytics based on classifications, associations, and traffic volumes.
- **Analytics**: Automatically apply analyst security expertise to raw data with indicators, aggregations, statistical analysis, and context to surface new insights and threats.
- **Detections**: Use signatures, heuristics, common industry correlations, and Sigma rules to identify known threats.
- **Models**: Test and apply Devo advanced machine-learning models or create custom models to keep pace with sophisticated adversaries.

These advanced detection methods reduce noise and increase signal so analysts can quickly identify and triage the most critical threats.

AUTO ENRICHMENT ADDS CONTEXT
Analysts can say goodbye to the swivel chair forever—Devo Security Operations does the work of gathering the information necessary to triage threats. Threat data and additional context are automatically added to alerts to speed triage.

Devo Security Operations automatically populates alerts with actionable, real-time data, context and entity behavioral insights including indicators from the Devo Threat Data Service, the community and partners. This context-rich view at an analyst’s fingertips reduces alert fatigue and accelerates the triage process by quickly homing in on the threats that matter. An entity-focused approach enables better prioritization, identification and investigation of high-impact threats.

ONE CLICK TO INVESTIGATION
Detection gets the ball rolling; the next steps are to investigate and respond to potential incidents. Devo Security Operations delivers an intuitive workflow so analysts can immediately investigate and validate high-risk alerts in the same view with a quick view of triggered events and related data.

MASTER THE ART OF RAPID DETECTION
The goal of detection is simple: find threats before they put the business at risk. To do that requires advanced detection methods to identify whether a threat is meaningful to the business. Devo provides the complete view analysts need. Organizations can tap into cyber intelligence, historical patterns, and advanced analytics to detect signs of compromise; receive immediate alerts to real risks; investigate and act on high-impact threats; and evolve detection practices based on new knowledge, enabling organizations to master the art of rapid detection.

Learn more at [devo.com/solutions/security-operations/threat-detection/](https://devo.com/solutions/security-operations/threat-detection/)