Threat Hunting with Devo
Hunt Across All Data—Quickly and Easily

Modern enterprises face evolving threat vectors, combination attacks, and coordinated campaigns, all contributing to an ever-expanding defense surface. Many mature SOCs are shifting their strategy to tackle these challenges, with proactive threat hunting a high priority.

Threat hunters must be able to continuously test an evolving set of hypotheses—on the fly—to detect evidence of an intrusion, understand the risk level of potential threats, and inform incident response. However, SOCs today are plagued by a lack of visibility, and often have limited resources they can dedicate to developing the full threat storyline. It takes significant time and effort to dig into the findings, manually enrich data with threat intelligence and context, and provide the detail needed to effectively respond to and recover from an incident.

A NEXT-GEN SECURITY OPERATIONS PLATFORM CHANGES THE GAME
Devo Security Operations is a next-gen platform that empowers analysts to better apply their expert knowledge and quickly mature SOC operations, improving effectiveness. It combines advanced threat detection, threat investigation, forensic analysis, and threat intelligence in an integrated analyst workflow that automatically adds rich context to alerts and investigations.

HUNT ALL OF THE DATA
Enterprises can no longer simply build lines of defense around the business to protect against attackers. They must proactively and iteratively respond to ongoing attacks. Modern threats are cleverly crafted to slip past an organization's defenses. Organizations can speed the hunting process by proactively identifying threats before they cause damage by analyzing the entire defense surface to reveal historical threat patterns and explore new data for ongoing attacks. The Devo Security Operations 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.
SUPPORT CREATIVE DETECTIVE WORK AND TEST FAST-EVOLVING HYPOTHESES
It is nearly impossible to detect evidence of an advanced threat by manual efforts alone. Effective threat hunting requires speed, scale and performance. Analysts need complete visibility and flexibility to rapidly test changing hypotheses. With Devo, analysts can quickly and intelligently query and pivot across petabytes of diverse data to identify IOCs and take action, as well as leverage historical data to map advanced threat campaigns across time—no matter how far back they go.

AUTO ENRICHMENT AND FLEXIBILITY TO EMPOWER THREAT HUNTERS
Creativity is vital for fast, effective threat hunting. Devo unleashes analyst creativity by providing easy access to threat and malware intelligence, behavioral observations, and real-time context for richer analysis. With legacy SIEMs, analysts must manually query multiple sources and systems to understand the threats that truly matter and piece together their potential impact. Devo Security Operations dramatically speeds the hunting process by automatically populating events in an actionable context including indicators from the Devo Threat Data Service, the community and partners.

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**: Go right into raw LINQ for all query needs.

MOVE QUICKLY FROM HUNTING TO INFORMED INVESTIGATIONS
Threats are increasingly difficult to detect, much less explore and eradicate. Devo provides the insight needed to isolate the source of an incident and drive response activities. The Devo Hunting Workbench makes it easy for analysts to add hunting results as context to an existing investigation or to start a new one. This enables analysts to take decisive action against threats and continuously improve by streamlining the process to incorporate findings into investigation workflows. The result: improved SOC operations, less redundancy, and more time to tackle the next hunt.

THREAT HUNTING DONE RIGHT
Threat hunting uplevels SOC defenses against the rapidly evolving threat landscape. The speed, scale and analytics from Devo enable threat hunters to do what they do best—hunt. Organizations can now reduce analysis from hours to seconds, lower the number of incidents impacting the business, and beat malicious actors at their own game.

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