Devo DeepTrace

Discover and derail your most sophisticated adversaries in minutes with autonomous investigations and threat hunting.

SOLUTION BRIEF

ANALYSTS CONTINUE TO STRUGGLE TO IDENTIFY REAL ATTACKS

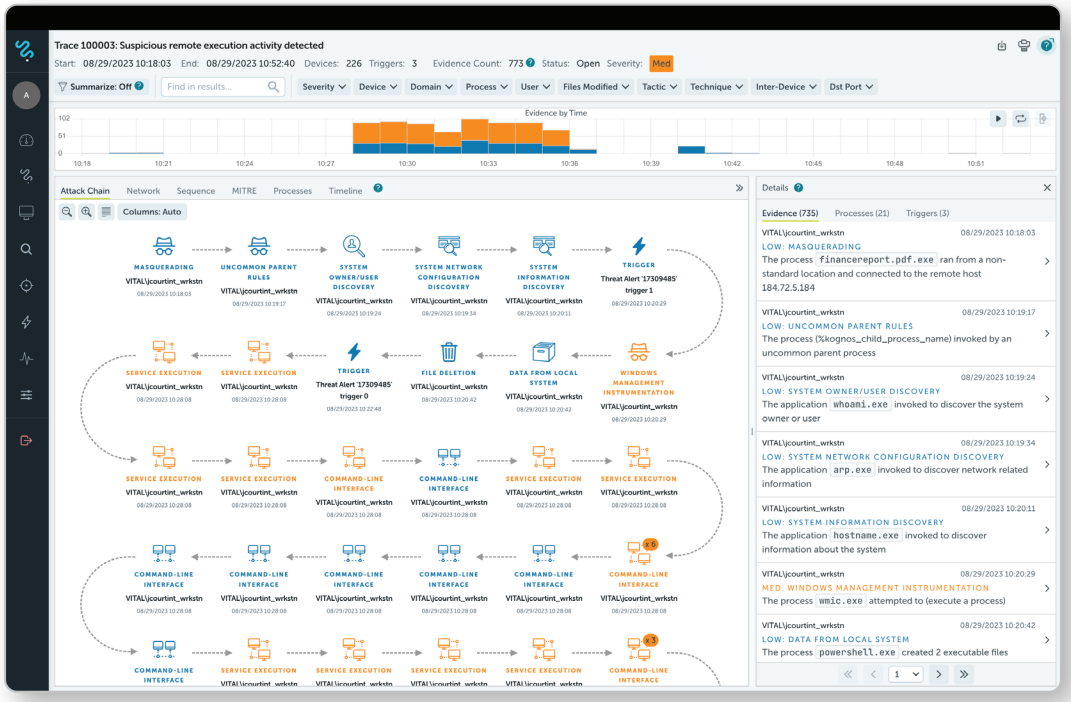
Today's SOCs are overwhelmed. With rapidly expanding attack surfaces and increasing amounts of data, they face a never-ending stream of alerts. To make matters worse, the unwieldy combination of time-consuming, manual investigative processes and the burden of running various tools have made working in the SOC more complex, resulting in higher frustration levels, unidentified security gaps, and slower response times.

Many security organizations lack the proper resources to proactively hunt for threats. For those who do, analysts with highly specialized skills must perform iterative, manual hunts, which incur additional investigative overhead. Consequently, this limits their ability to uncover low and slow persistent threats within reasonable timeframes.

DEVO DEEPTRACE HELPS ANALYSTS IDENTIFY THE ROOT CAUSE OF EVERY ATTACK

Devo DeepTrace performs autonomous investigation and threat hunting using attack-tracing AI, advancing how security teams identify attacks, investigate threats, and secure the organization. DeepTrace augments analysts' work by building complete traces of suspicious activity detected across an organization's infrastructure, alleviating much of their mundane, repetitive tasks.

Devo DeepTrace is a key element of the Devo Security Data Platform. Its autonomous, AI-powered investigations provide actionable intelligence that supports a broad range of security use cases, including malware, ransomware, and insider threats. Once an alert or event occurs, DeepTrace automatically produces a trace within minutes, providing analysts with evidence and insights that can be tracked and remediated.



DeepTrace builds traces that identify and isolate the root cause of every attack.

TRANSFORM DAYS OF WORK INTO MINUTES OF AI-POWERED INVESTIGATIONS

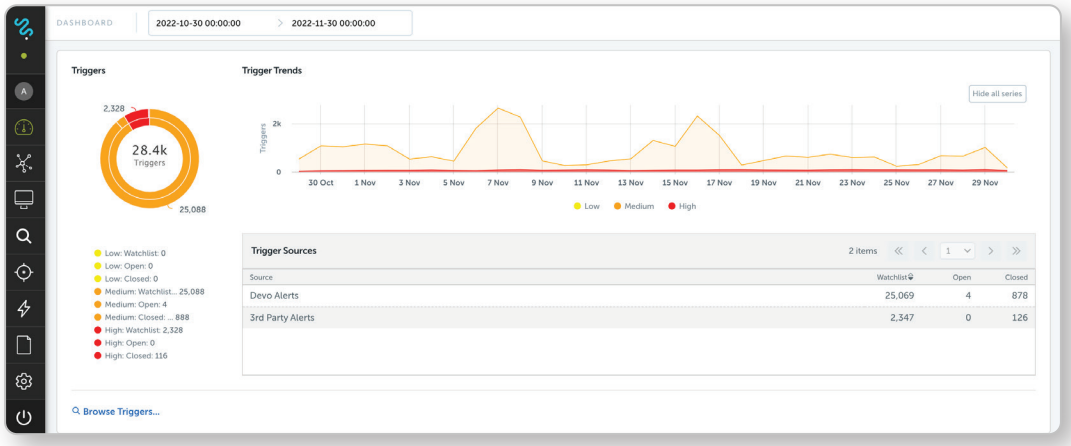
Devo DeepTrace helps security teams autonomously investigate alerts and suspicious events and perform threat hunting via:

- **Fully documented attack chains that speed investigations:** Utilizing attack-tracing AI and relationship graph technology, DeepTrace transforms days of work into real-time results by building artifacts known as traces, which fully and chronologically document each attack chain.
- **An AI engine that augments analysts:** DeepTrace helps analysts by performing investigations at machine speed and scale. Starting with an event or an alert, its AI engine asks hundreds of thousands of questions in minutes to autonomously construct traces detailing an attacker's actions. DeepTrace automatically overlays its results against the MITRE ATT&CK framework, providing analysts with additional context and reference points to analyze attacks, identify patterns, and assess existing defenses within the organization.
- **Autonomous investigations that accelerate context-based decision-making:** DeepTrace autonomously traverses historical data to document an adversary's behavior from the start to finish of an attack, providing the facts analysts need to take effective action.
- **Autonomous threat hunting that upskills analysts:** DeepTrace helps threat hunters quickly construct and configure new hunts that map to MITRE ATT&CK framework tactics and techniques. Once refined and validated, these can be converted to new cadence-based threat detections.
- **Single-click investigations:** Analysts can launch DeepTrace investigations from the Devo Security Data Platform. Within minutes, analysts can review evidence and gain insights to make informed decisions and take action, improving operational efficiency.

RAPIDLY INVESTIGATE SUSPICIOUS ACTIVITY ACROSS A VARIETY OF USE CASES

Devo DeepTrace provides the full context and details security teams need to understand and respond to every attack.

Use Case: Autonomous Investigations



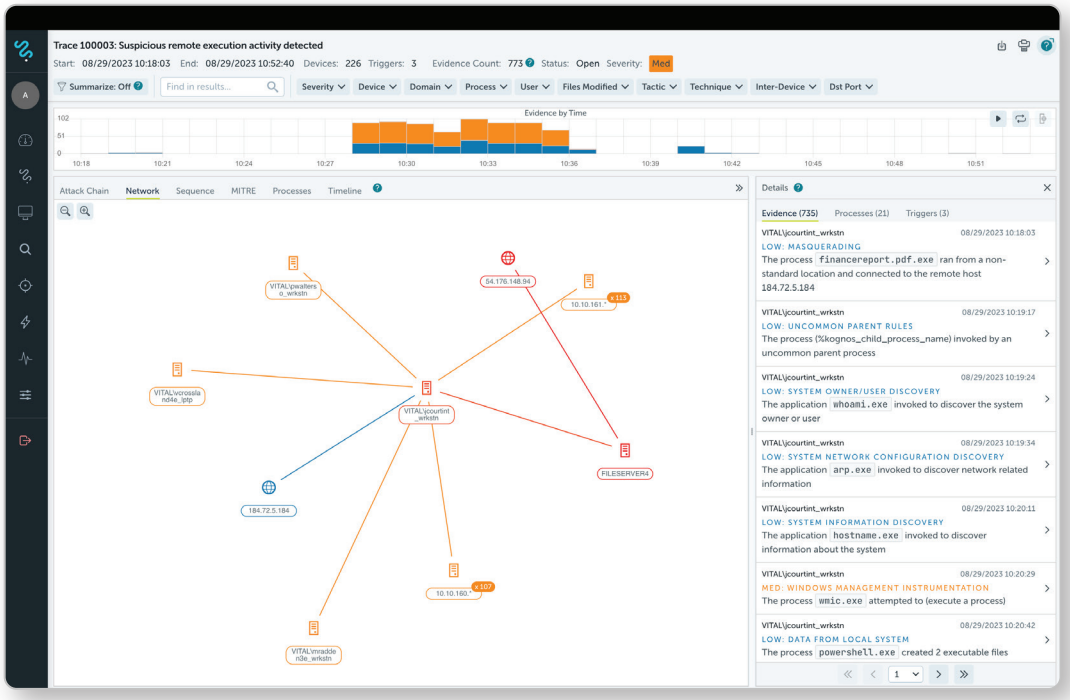
DeepTrace flags alerts that warrant further investigation.

The Challenge: The ever-increasing volume of data the SOC ingests and relentless surge of alerts produced is becoming untenable. Each alert requires many manual, repetitive steps to understand, which lengthens overall response time and overwhelms analysts.

The Devo DeepTrace Solution: Analysts can launch DeepTrace investigations with the click of a button from the Devo Security Data Platform. Using attack-tracing AI, DeepTrace identifies each step in a given attack chain, providing a full, evidence-based timeline of an attack. Each trace offers critical information that an analyst needs to mitigate the threat.

Benefits: DeepTrace helps analysts reduce alert fatigue, removing the bulk of monotonous and manual investigation workflows to identify high-priority alerts. This enables analysts to perform in-depth analysis and broader forensic work, resulting in faster investigation times. Even junior analysts can punch above their weight and perform higher-level workflows.

Use Case: Optimized Incident Response



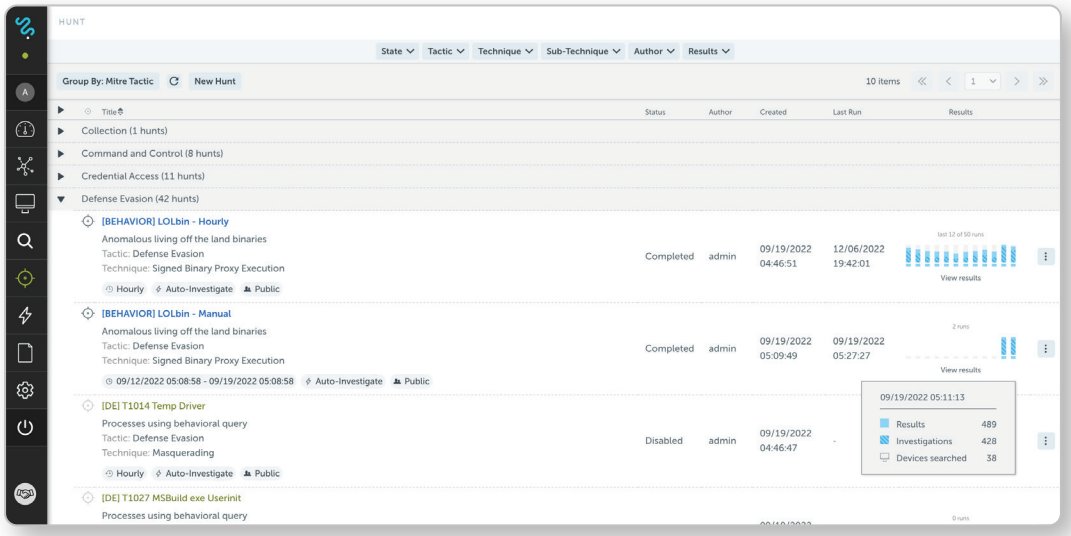
DeepTrace documents the attacker's footprint across the entire organization.

The Challenge: Given that an intrusion's average dwell time can be months, analysts need to mine through petabytes of telemetry data to fully understand what the adversary has done and where they have been throughout an organization.

The Devo DeepTrace Solution: DeepTrace harnesses the organization's endpoint log data to perform retroactive hunts that pinpoint attacks and malicious activity. Once an attack is identified, DeepTrace produces interactive traces and reports documenting an attacker's footsteps.

Benefits: DeepTrace helps analysts mine immense volumes of data in seconds or minutes instead of hours or days. By providing relationship and time-based views of evidence, DeepTrace enables security teams to replace time-consuming, laborious workflows with targeted forensic analysis, reducing investigation times and decreasing MTTR from hours to minutes.

Use Case: Autonomous Threat Hunting



DeepTrace enables the creation of new threat detection signals and alerts.

The Challenge: Though security teams aspire to be proactive, many organizations find it difficult to hunt for threats because of limited resources and capacity. In the meantime, analysts with highly specialized skills must perform iterative, manual threat hunting, which incurs additional investigative overhead. In the face of overstretched capacity, threat hunters face the impossible task of searching for unknown unknowns – the unseen, unidentified threats that could imperil the business.

The Devo DeepTrace Solution: DeepTrace helps threat hunters quickly construct and configure new hunts that map to MITRE ATT&CK framework tactics and techniques. Once refined and validated with autonomous investigations, these hunts can be converted to new cadence-based threat detections. By configuring broad threat hunts and traversing historical data, DeepTrace can surface unreported anomalies and hone in on suspicious behaviors that can lead to new traces.

Benefits: DeepTrace enables SOC teams to establish and add to their repertoire of hunt hypotheses, starting with the ability to select from a pre-configured set. Using these foundations, they can customize and derive new hunts without starting from scratch. This helps ensure a strong foundation of proactive threat hunting, which can be built upon over time with reduced effort and without overreliance on specialized expertise.

Are you ready to learn more about Devo DeepTrace?
Contact your sales representative to schedule a demo or visit devo.com

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native security analytics platform that combines the power of people and intelligent automation to confidently defend expanding attack surfaces. An ally in keeping your organization secure, Devo augments security teams with AI — enabling you to continuously scale SOC efficiency, increase the speed of threat detection and response, and gain greater clarity to empower bold action, minimize risk, and maximize outcomes. Learn more at **www.devo.com**.