Devo DeepTrace

SOLUTION BRIEF

Augment your security team with autonomous investigations and threat hunting.

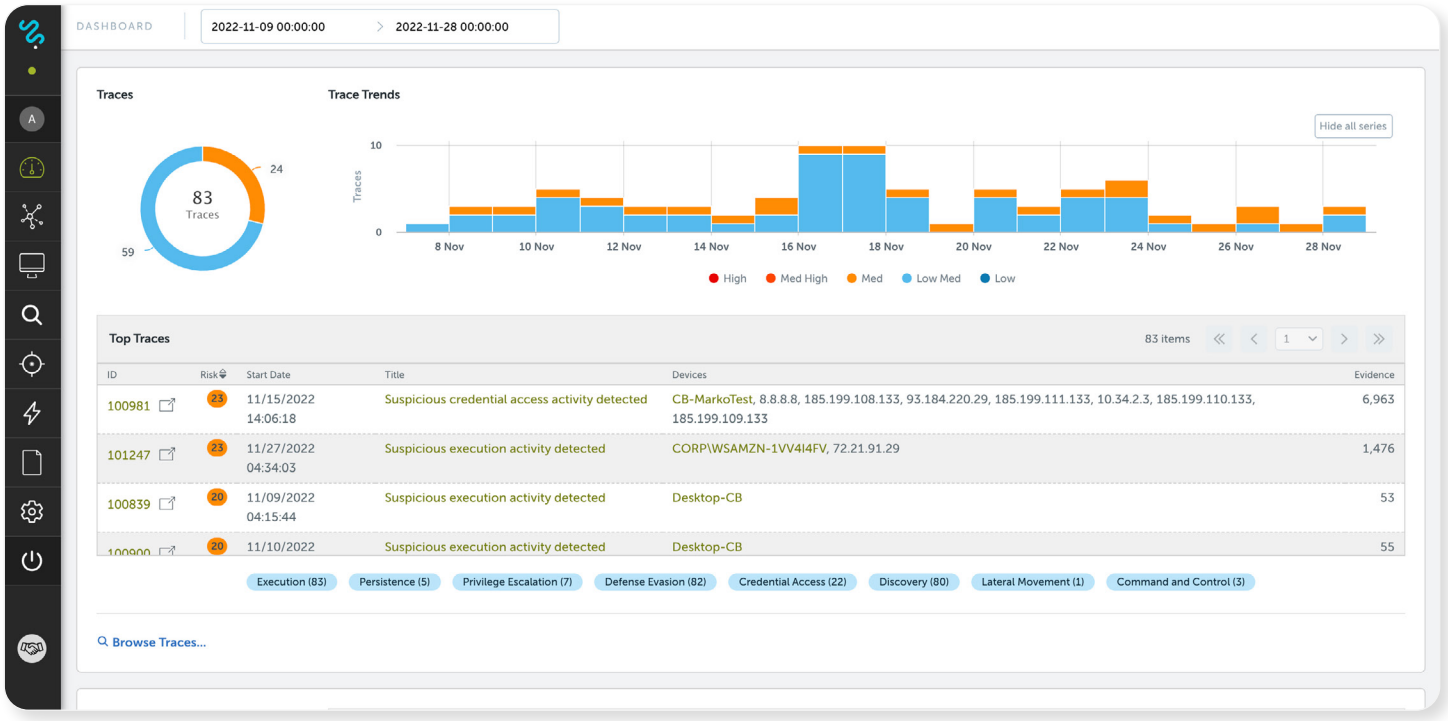
ANALYSTS CONTINUE THEIR STRUGGLE TO IDENTIFY REAL ATTACKS

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 challenges of integrating a plethora of tools have made working in the SOC more complex, resulting in higher frustration levels and slower response times.

For many SOCs, threat hunting is a stretch. Many security organizations don't have the proper resources or capacity to hunt for threats proactively. Those analysts who possess highly specialized skills must perform exhaustive, manual threat hunting, which limits their ability to reduce dwell times and uncover persistent threats.

DEVO DEEPTRACE HELPS ANALYSTS IDENTIFY THE ROOT CAUSE OF EVERY ATTACK

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



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

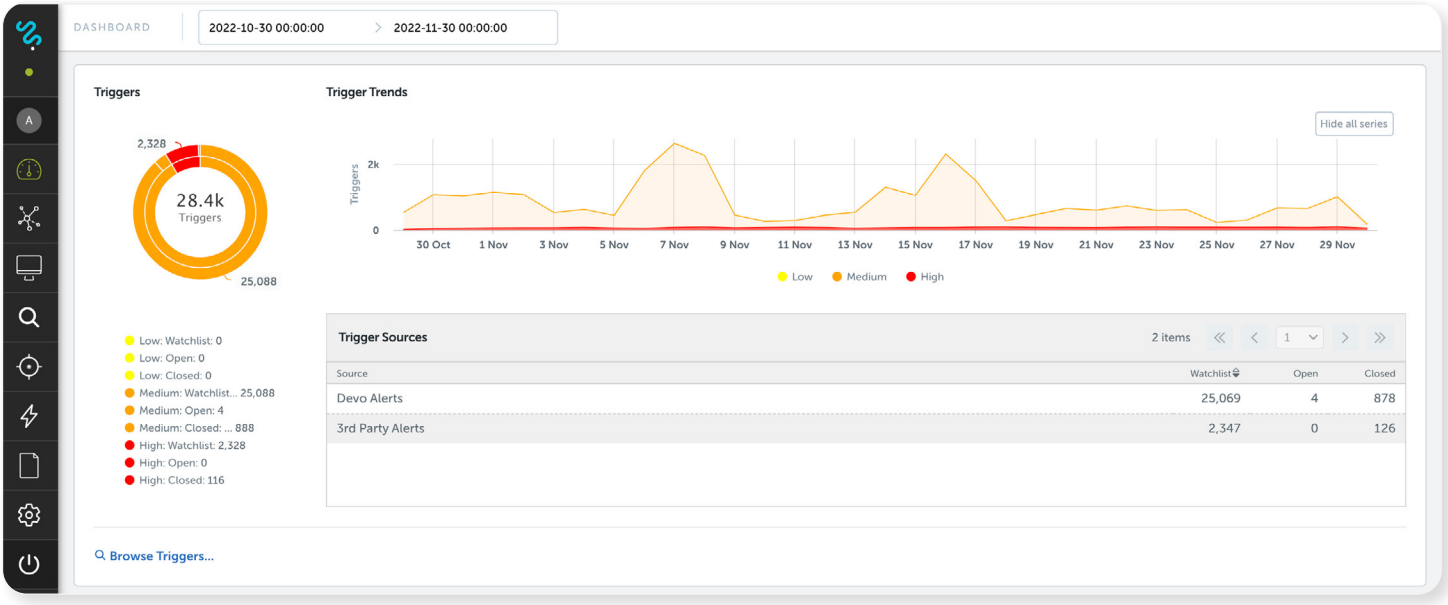
Devo DeepTrace helps security teams autonomously investigate alerts and suspicious events and perform threat hunting via the Devo Platform:

- **Fully documented attack chains that speed investigations:** Utilizing attack-tracing AI and graph technology, DeepTrace helps alleviate the work overwhelming today's analysts by building artifacts known as traces, which fully and chronologically document each attack chain. DeepTrace exposes the adversary's activity, enabling security teams to quickly and confidently respond to each threat.
- **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 potentially hundreds of thousands of questions to autonomously construct traces detailing an attacker's actions. DeepTrace then overlays its results against the MITRE ATT&CK framework, which provides analysts with advanced context and additional points of reference 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 start to finish of an attack, providing the facts analysts need to take effective action.
- **Autonomous threat hunting to upskill 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.

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 ingested by the SOC is becoming untenable, resulting in a deluge of alerts. Each alert requires many manual, repetitive steps to understand, which negatively impacts overall response time and overwhelms analysts.

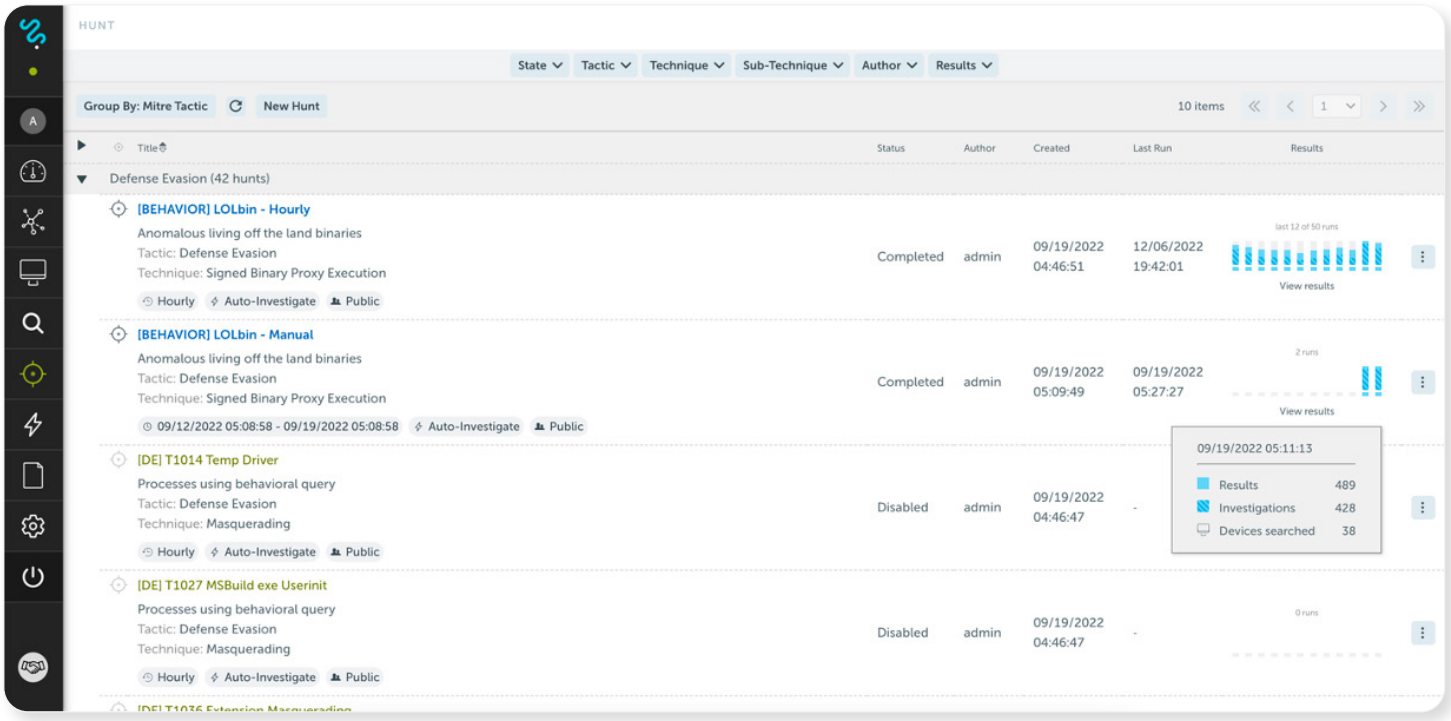
THE DEVO DEEPTRACE SOLUTION

DeepTrace autonomously investigates suspicious events and alerts using attack-tracing AI. It identifies each step in the attack chain, providing a full, evidence-based timeline of the attack. Each trace offers critical information that an analyst needs to nullify the threat.

BENEFITS

Devo DeepTrace helps analysts reduce alert fatigue, removing the bulk of pedestrian, manual investigation workflows to identify the alerts that matter. Analysts can review fully investigated traces in real time, eliminating laborious, repetitive tasks that overwhelm security teams. Even junior analysts can punch above their weight and perform higher-level tasks.

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, those analysts who possess highly specialized skills must perform iterative, manual threat hunting. These circumstances make it especially difficult, if not impossible, to search for unknown unknowns — the unseen, unidentified threats that could negatively impact the business.

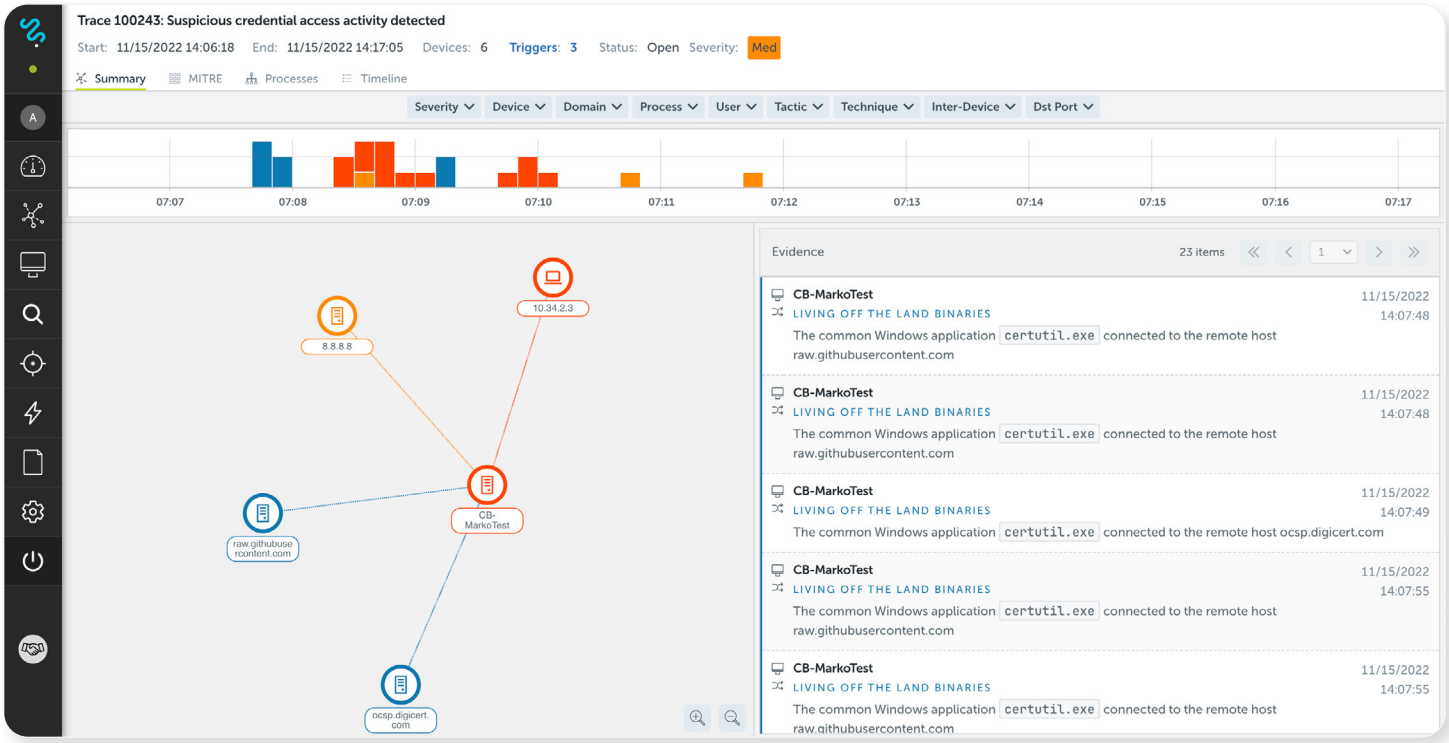
THE DEVO DEEPTRACE SOLUTION

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 the use of autonomous investigations, these can be converted to new cadence-based threat detections.

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 over reliance on specialized expertise.

USE CASE: Optimized Incident Response



DeepTrace produces a graphical, interactive story that 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 over a period of weeks to fully understand what the adversary has done and where they have been throughout the organization.

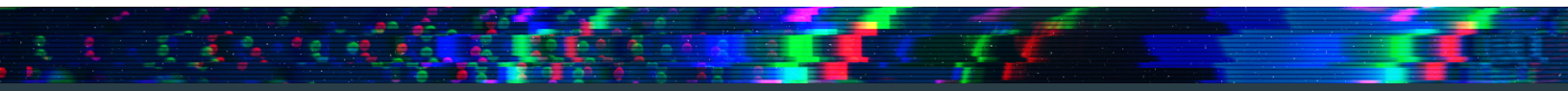
THE DEVO DEEPTRACE SOLUTION

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

BENEFITS

Devo DeepTrace helps analysts mine immense volumes of data in seconds or minutes instead of hours or days. It enables security teams to replace time-consuming, laborious hunts and workflows with autonomous investigations, reducing investigation times and decreasing MTTR from hours to minutes.

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 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**.