No enterprise is 100 percent secure. Attackers are constantly working to infiltrate organizations, requiring SOC teams to always be ready to detect and respond to threats. Threat investigation is critical to this effort. The better an organization knows its enemies, the better prepared it is to respond to a threat. The goal of a threat investigation is to develop a complete and accurate view of the incident—as quickly and accurately as possible, including zeroing in on the threat, collecting evidence, and running a forensic analysis to understand and record the attack details, drawing conclusions from the analysis, and mobilizing incident response with actionable insights.

**Triage and Threat Investigation with Devo Security Operations**

Devo Security Operations empowers analysts to better apply their expert knowledge and quickly mature SOC operations, improving effectiveness. The biggest issue for analysts is beating the clock on dwell time. Analysts have a tough job—they must quickly validate threats, gather evidence, understand adversarial TTPs, and determine an appropriate response. With legacy SIEMs, an alert event could be two hours old by the time it’s triggered, but with Devo Security Operations investigators get real-time insight about what is happening to all entities associated with that alert and whether the information is important. Devo changes the game by accelerating triage and investigations with entity modeling, high-signal contextual alerting, and auto enrichment across an integrated incident-management workflow.

**All the Evidence Needed to Construct the Full Threat Story**

The first step in any investigation is to collect and enrich evidence to build a case. Devo Security Operations empowers analysts with complete visibility at scale. Analysts can easily draw enterprise-wide insights, from business applications to user behavior; explore findings through interactive visualizations; dig into their data right from the dashboard; and build on that data with threat intelligence feeds, industry frameworks, and the Devo Threat Data Service to more quickly establish the full threat story.
The goal is greater accuracy and confidence in the priority and impact of threats as they move through the kill chain. In addition, the Devo Security Operations triage workflow addresses the different skill levels and focus areas of the multiple investigator types in a SOC, enabling them to easily filter by time horizon, alert priority, alert type, and MITRE ATT&CK tactic or technique. This helps analysts focus on the alerts that matter and save that workflow for future analysis.

**AUTO ENRICHMENT IS ESSENTIAL FOR SHORTENING INVESTIGATIONS**

The foundation for successful investigations is an analyst’s ability to ask hard questions of their data—from detection to response. But getting the right answers is very difficult without supporting evidence and context. Auto enrichment is the automatic population of NTA, IDS, EDR, threat data (commercial, private and OSINT), entitlements, business significance, and more to determine the importance of an event and speed investigations. Devo Security Operations combines the many forms of context behind a threat including:

- **Alert Priority Score**: Priority scoring, assigned at alert creation, to denote whether an alert requires immediate attention based on a range: informational, low, medium, high or critical.
- **Investigation Importance**: Score based on collective alert priority and entity impact scorings for any past investigations.
- **Entity Impact Score**: 0 - 100 score based on number of associations, volume of traffic to and from an entity, behaviors, and associated entity impact scores to signify a potential threat and its impact on the business.
- **Entity Severity Score**: Magnitude of change of an entity over a 24-hour period.
- **MITRE ATT&CK Framework**: Labels that map alerts to an ATT&CK tactic and technique with focus on the post-exploitation segment of the kill chain to understand and communicate coverage.
- **Threat Data**: The Devo Threat Data Service enables indicator consumption, sharing and collaboration with the MISP community, as well as from open-source, paid and proprietary intelligence feeds.

**DEEPEN THE FORENSIC ANALYSIS OF THE COMPROMISE**

Threat investigators are tasked with determining the who, what, when, where, how and why of a compromise. Forensic analysis enables investigators to completely eradicate a threat and inform long-term strategy with a more thorough understanding of an incident. Devo Security Operations simplifies the process of centralizing and analyzing forensic evidence for better and faster decisions. For example, the Devo Evidence Locker makes it easy to centralize artifacts such as files, images, memory dumps, and PCAPs to make evidence-based decisions. Analysts also can submit binaries to the MISP Viper sandbox and push the indicators from the analysis into an investigation. These indicators can be used to identify new indicators across current and historical data. Analysts can then leverage their forensics skills to quickly analyze data to gain a deep understanding of threats and learn from historical breaches with saved queries and high-confidence threat intelligence.

**MOBILIZE INCIDENT RESPONSE**

Enterprises must institute near-real-time remediation measures to effectively close attack pathways, limit the impact of a breach, and address and resolve vulnerabilities in the environment. This requires a data-driven and targeted approach with a focus on cyber-threat intelligence, increased collaboration, and automation. Devo Security Operations provides unparalleled speed and scale for faster triage and response, and access to community threat intelligence for more evolved incident response. The flexible, open APIs enable analysts to integrate with various orchestration and automation solutions for seamless response.