Threat Detection with Devo Security Operations

Stopping Adversaries in Their Tracks

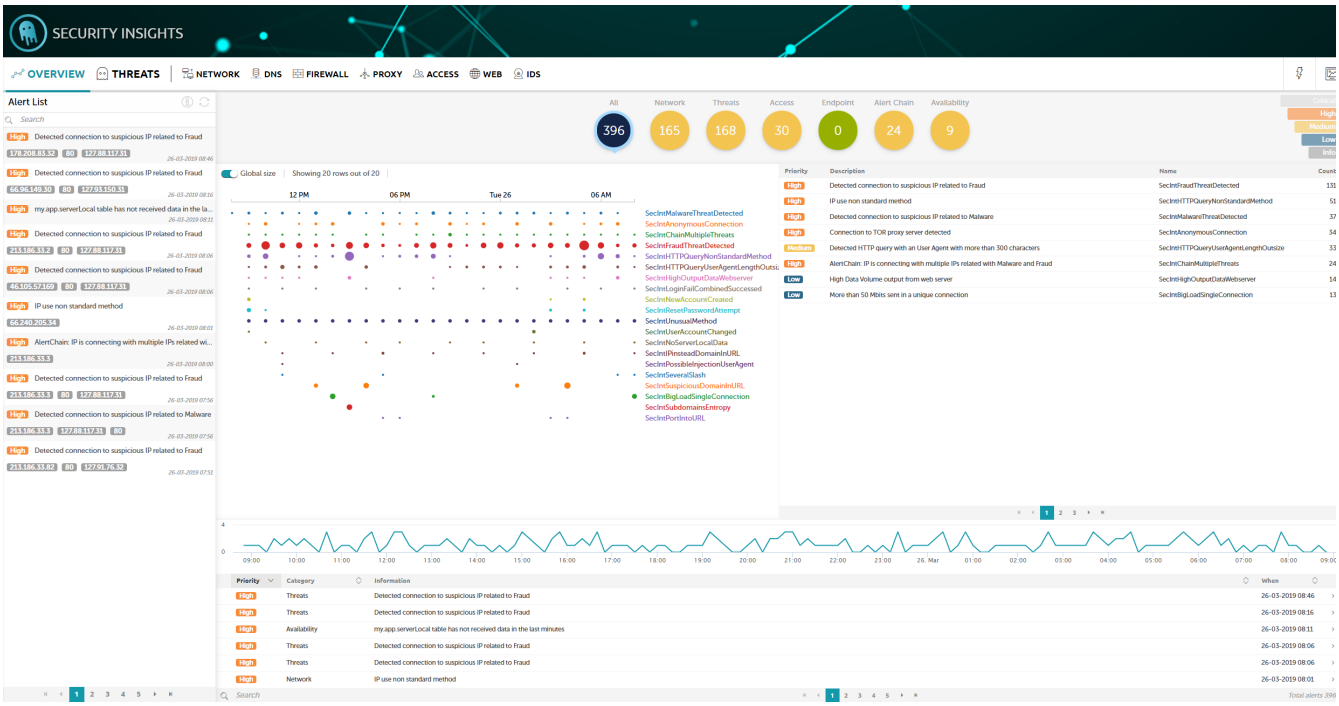

Figure 1: Devo Security Operations

One of our customers – a top five retailer with petabytes of data – shortened the time it took to detect malicious bots from hours to seconds, ultimately reducing fraudulent purchases.

The quicker you find a threat, the quicker you can respond to it. However, threat detection is difficult to master. Attackers are getting better and better at evading defense technologies. Threat detection requires a deep understanding of the global threat landscape, as well as the specific risks impacting your enterprise – a big ask. It is extremely difficult and time-consuming to piece together disparate data, industry intelligence, and new findings through human effort alone.

The Devo Approach

Devo Security Operations powers the SOC with advanced threat detection. Inform detection with threat intelligence, tribal knowledge, and advanced analytics; leverage consumable alerting dashboards to address signs of compromise and prioritize potential threats; and transform alerts into action through automation and machine learning.

Embed Intelligence and Analytics

Hackers 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 tactics. With Devo Security Operations, you can collect and access all your data; enrich your data with open and out-of-the-box threat intelligence feeds; and apply machine learning and data science models to intelligently inform detection.

Alert to *Critical* Threats

According to Verizon[1], 87% of compromises happen in a matter of minutes, while only 3% are discovered as quickly. Devo Security Operations speeds response time by automatically delivering *critical* alerts to your analysts. Establish a dynamic baseline for alert conditions and identify anomalies with enriched alerts in real time. Easily characterize and prioritize alerts with machine learning to reduce manual and time-consuming tasks. Link model attack patterns to alerts for more intelligent decision-making.

Pivot From Detection to Investigation

Detection gets the ball rolling – the next steps are to investigate and respond to potential incidents. Immediately investigate and validate high-risk alerts in the same view. Drill down into the raw data to build your case. Mobilize incident responders with an in-depth analysis of the compromise. Share findings either locally or globally, and tap into industry intelligence for more effective investigation, response, and recovery efforts.

Master the Art of Rapid Detection

The goal of detection is simple: find threats before they put your business at risk. Devo Security Operations enables you to detect incidents fast enough to stop them. Tap into cyber intelligence, historical patterns, and advanced analytics to detect signs of compromise; receive immediate alerts to anomalous behavior and real risks; investigate and act on high-impact threats; and evolve your detection practices based on new knowledge.

For more information on threat detection with Devo Security Operations, contact sales@devo.com.

[1] 2018 Data Breach Investigations Report, Verizon, 2018

.

ABOUT DEVO

Devo Technology is the data engine behind today's digitally-driven enterprises, helping organizations maximize the economic and operational value of their machine data. The Devo Data Operations Platform delivers real-time analytics on streaming and historical data to turn machine data into actions that help enterprises achieve sustained performance and growth. By collecting, enhancing and analyzing machine data, Devo provides business-driving insights for IT, security, and business teams at the world's largest organizations. For more information visit www.devo.com