Gold Nugget | Cyber Defense the Sotera Way

Gold Nugget is Sotera's integrated Cyber Defense and Security Operations Platform. Gold Nugget performs large-scale behavioral/anomaly detection using raw data as well as data produced by cyber tools like FireEye and Splunk.

Gold Nugget does not replace your existing cyber tools – it just makes them better. Because our analytics span both raw and processed data, Gold Nugget uncovers insights that can be used to improve the rule sets and configurations of your existing arsenal of cyber defense tools. Gold Nugget integrates with existing cyber watch-floors to provide machine-guided automation of alert processing.

Under the hood, Gold Nugget applies unified data, analytics and visualization frameworks using an open source elastic compute cloud. Our machine learning engine identifies contextual based correlations among data sources. Unlike other products on the market, Gold Nugget provides behavioral analytics and anomaly detection without deep packet inspection, including accurately distinguishing between human and compuer-based activities. Gold Nugget handles both streaming and batch processing data for both real-time and historical analytics.

Cyber Advantage

* Detect coordinated activities and sophisticated users hiding in the noise on high volume ports.
* Machine-learning based attack detection accurately distinguishes human activity from bots even when attackers attempt to hide their behavior.
* Rapid discovery of anomalous behavior without deep packet inspection - runs faster and requires less hardware.

Analysts' Advantage

* Identifies weaknesses in cyber infrastructure.
* Create new rules in existing tools to improve security.
* Dashboards quickly highlight potential issues and anomalous behavior.
* Powerful visualization features enable analysts to rapidly process large volumes of data.

Committed to Open Source

Founded on delivering exceptional service to Government clients, Sotera is technology-neutral and not tied to vendors. All of our analytic tools are built with open source software. Our goal is to unleash innovation, avoid vendor lock-in, improve security, and reduce Total Cost of Ownership.

SOTERA
DEFENSE SOLUTIONS
Agility. Ingenuity. Integrity.
www.soteradefense.com

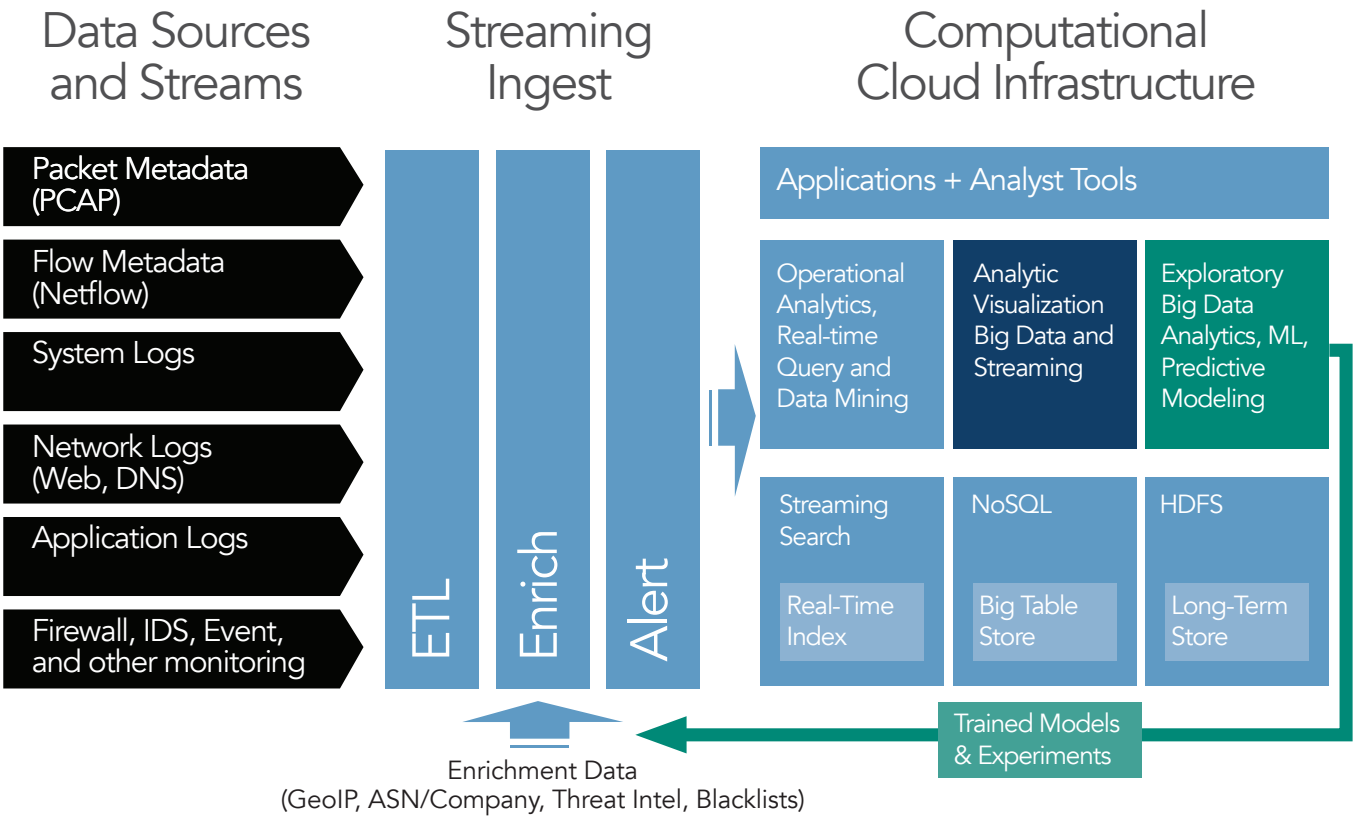
Success Stories:

* Identifying a pending bot net attack by finding 250 thousand out-of-place interactions among 5 billion communications.

* Detecting a network infiltration by identifying a single IP address hiding in 100 billion network log entries.

* Discovering an infiltrator conducting reconnaissance on the Government network by detecting out-of-norm behavior on a single IP address among 5 million.

Shift from Security as Opinions and Blind "Best Practices" to Security as a Science



Sotera Defense Solutions, Inc. is an agile, mid-size technology company that delivers innovative solutions to the agencies that provide for the safety and security of our nation.

We specialize in counterterrorism, cyber, data analytics, intelligence, and C4ISR missions and technologies.

SOTERA
DEFENSE SOLUTIONS
Agility. Ingenuity. Integrity.
www.soteradefense.com