cloudera®

SOLUTION BRIEF

THREATSTREAM®

Platfora

Industry
Cybersecurity

Website
www.threatstream.com

Company Overview
ThreatStream® is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, ThreatStream enables organizations to proactively identify and combat cyber threats targeting their operations.

Product Overview
The ThreatStream Optic™ threat intelligence platform makes sense of all the threat data security teams have to sort through to find the needle(s) in the haystack that threaten their business, customers, intellectual property and reputation.

Solution Highlights
- Aggregation & De-duplication
- Real-time Risk Analysis
- Correlation & Actionable Intelligence
- Collaboration & Community

Too Much Data, Too Little Relevance, Too Little Time

Security operations, threat research teams, and security analysts are in a race against time to stay ahead of the latest threats to their organizations. The good news is that there's an overwhelming amount of threat data available today. But those increasing data volumes also present a challenge. Rapidly converting this unstructured and duplicative data, adding contextual information, and running analytics in real-time is a cumbersome and time-consuming process for analysts who are already over subscribed.

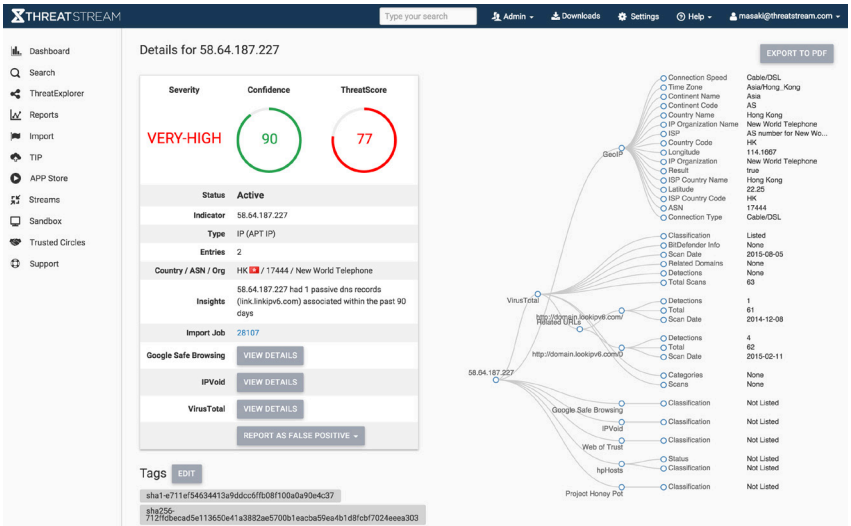
Running against a Hadoop-based enterprise data hub, ThreatStream customers are equipped to power a security monitoring practice that uncovers threats *as they happen*... for rapid, efficient, and reliable incident response. Without automated and complete integration from multiple threat data sources to your enterprise data hub, you're wasting critical time on a tedious and manual process based on homegrown integrations.

Operationalize Your Intel: Prioritize and Accelerate Incident Response

ThreatStream Optic provides the essential analysis and correlation that you need to translate raw, unstructured and duplicative data into true intelligence. Reduce the noise of false positives, outdated and irrelevant data in minutes, and what's left is true insight... in the form of pre-built rules, reports, and dashboards that you can immediately apply and manage within your current security infrastructure.

Setting ThreatStream apart from other threat intelligence platform providers is its unique ability to integrate community and operational security infrastructure to fully manage the entire lifecycle of threat information.

Use Cases
- Malware and APT detection
- Fraud & Crimeware



Benefits of Cloudera

- **Powerful** – Store, process, and analyze all your data to drive competitive advantage
- **Efficient** – Hadoop unifies compute and data to improve operational efficiency
- **Open** – 100% open source: CDH is the world's most popular open source distribution powered by Apache Hadoop
- **Simple** – Easy to deploy and operate with centralized administration
- **Compatible** – Leverage your existing investments for rapid adoption and lower TCO
- **Economical** – Rethink the economics of data management with an open source platform on industry standard hardware - up to 90% more cost effective than traditional solutions
- **Enterprise Ready** – Equipped with critical capabilities to support mission-critical operations

Benefits of ThreatStream

- Easy-to-use interface to view threat information received through STIX/TAXII feeds
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details
- Eliminate unnecessary, duplicative and irrelevant indicators - *before* they enter your infrastructure
- Identify and prioritize the events that matter now - without DIY scripting
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment

Benefits of the Joint Offering

The increasing number of high profile security breaches has demonstrated the need to detect and disrupt advanced persistent threats, fraud, and insider attacks. Traditional security technologies lack the sophisticated capabilities and visibility required to detect and protect against such attacks. ThreatStream Optic™ threat intelligence platform integrates with Cloudera Enterprise Data Hub for Cybersecurity (EDH Cyber) to enable security data mining and provides advanced threat and risk detection, combining deep security expertise with analytical insights on a massive scale.

Undercover threats as they happen

- ThreatStream Optic™ threat intelligence platform integrates with EDH Cyber via Optic Link, which allows for the augmentation of the data with timely and risk scored threat intelligence and the ability to analyze massive amount of security data and make connections between them to create a prioritized list of threats relevant to the organization.

Know your adversaries

- Analyzing massive security data also uncovers attacker's techniques and detailed context that could help identify hidden threats faster, track cyber adversaries and campaigns more proactively and effectively

Detect and disrupt attacks

- Armed with visibility and actionable intelligence, organizations can detect and respond to security incidents faster leveraging ThreatStream's integration with EDH Cyber, security monitoring technologies such as SIEM, endpoint security solutions and network security devices such as next-generation firewalls, web gateways, intrusion detection and protection systems, etc

About ThreatStream

ThreatStream® is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, ThreatStream enables organizations to proactively identify and combat cyber threats targeting their operations.

About Cloudera

Cloudera is revolutionizing enterprise data management by offering the first unified Platform for Big Data: The Enterprise Data Hub. Cloudera offers enterprises one place to store, process and analyze all their data, empowering them to extend the value of existing investments while enabling fundamental new ways to derive value from their data. Founded in 2008, Cloudera was the first and is still today the leading provider and supporter of Hadoop for the enterprise. Cloudera also offers software for business critical data challenges including storage, access, management, analysis, security and search. With over 15,000 individuals trained, Cloudera is a leading educator of data professionals, offering the industry's broadest array of Hadoop training and certification programs. Cloudera works with over 700 hardware, software and services partners to meet customers' big data goals. Leading organizations in every industry run Cloudera in production, including finance, telecommunications, retail, internet, utilities, oil and gas, healthcare, biopharmaceuticals, networking and media, plus top public sector organizations globally. www.cloudera.com.

cloudera.com

1-888-789-1488 or 1-650-362-0488
Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA