SECURONIX
Security Analytics. Delivered.

DATASHEET

SNYPR® SECURITY ANALYTICS

[Log Mgmt + Next-Gen SIEM + UEBA] on HADOOP

SNYPR® Security Analytics platform fulfills the promise of legacy SIEM in the new IT landscape. Legacy SIEMs built two decades ago on old technology stacks can no longer collect or understand the volume and variety of IT data coming from a new generation of IT devices. The cyber threat landscape has become more treacherous with advanced targeted attacks, porous perimeters and increased business interdependencies. The landscape has evolved, but legacy security monitoring tools have not. They have become obsolete in the face of new cyber threats across this new IT fabric.

Securonix Security Analytics is developed on a big data security analytics framework, and transforms big data into actionable security intelligence. Built on a Hadoop big data platform, Securonix combines log management, SIEM, and UEBA into a complete, end-to-end platform that can be deployed in its entirety or in flexible, modular components. Securonix performs advanced security analytics using machine learning algorithms over massive volumes of data in real-time and provide actionable intelligence.

SMARTER

The SNYPR Security Analytics Platform uses a combination of context enrichment, machine learning and threat modeling to predict, detect and contain advanced threats, anywhere, in real- time. Unlike SIEM solutions that inundate security teams with false positives, SNYPR leverages sophisticated machine learning algorithms to accurately identify the most hard-to-detect cyber threats, insider threats and fraud. All alerts are automatically risk- ranked, so analysts know what to investigate first.

Organizations that already leverage a SIEM can use SNYPR as a comprehensive threat detection and analytics layer that transforms SIEM data into actionable intelligence; those without an effective SIEM in place can leverage SNYPR for all of their needs from data collection and retention to advanced threat detection and remediation.

FASTER

SNYPR is quick to deploy with out-of-the box connectors and threat models perfected by years of production deployments with hundreds of customers. The behavior-based approach using machine learning provides fast and accurate threat detection with minimal false positives. The solution comes packaged with Securonix Spotter®, a blazing-fast, natural language search engine that enables threat hunting across heterogeneous data sources and empowers analysts with all the tools needed to investigate threats over long periods of time, with direct access to historical data. With elegant visualization, simple, point-and-click data-link analysis, automated response, and customizable case management workflows, security teams can hunt, investigate and report quickly, accurately and efficiently.

ECONOMICAL

SNYPR drinks petabytes of data from a firehose, while super enriching raw events in real-time with meaningful identity, asset, network, geo-location and threat intelligence context. Built on an underlying Hadoop platform, SNYPR provides a true open data model where customers can build their own applications for any business use with open access to all data collected, eliminating the need to create multiple data stores and the cost associated with licensing and maintaining them.

SNYPR enables long-term retention and scalability in a cost effective manner with use of commodity hardware and automated data life cycle management. The solution is priced by identity, providing you a lower predictable cost that is easy to estimate and manage in the long run.

ACTIONABLE

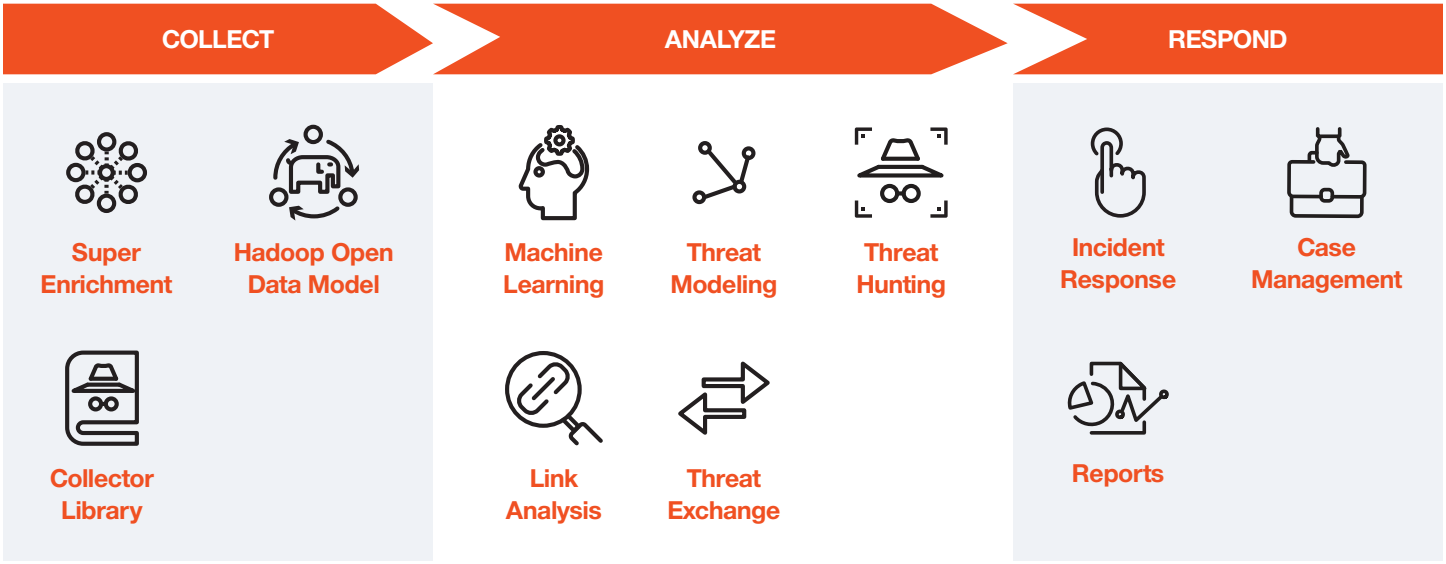
Securonix SNYPR Security Analytics uses patented supervised and unsupervised machine learning across the petabytes of collected and enriched data. The algorithms are applied to event data streaming in real-time across the ingestion nodes, and every alert is assigned a highly accurate priority and criticality based on dozens of evaluative criteria. SOC analysts aren't just bombarded with another source of security alert flood, but are guided in their day to day tasks with risk based priorities, automated forensic data collection, and incident response. This allows security analysts and the SOC team to perform as a coherent unit when faced with a potentially crippling cyber incident. Securonix incident response framework provides automated workflow and response playbooks to rapidly take action on high risk threats.

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2017 Securonix

DEPLOY THE COMPLETE PLATFORM OR MODULAR SOLUTIONS



KEY CAPABILITIES

Open Data Model

Securonix open data model uses a common data format for all security events in the Security Data Lake. This enables organizations to maintain a single copy of data in the Security data lake and make it available to any number of applications to run their own custom analytics. Unlike traditional log mgmt. your data is not locked into a proprietary data store, enabling you to use, share, manage and own your data without dependencies on the vendor platform

Contextual Awareness With Super Enrichment

Super enrichment of security data with contextual information at the time of ingestion transforms raw events into meaningful information that is easy to understand, search and investigate. Contextual enrichment adds user identity, asset metadata, network information, geo-location and threat context to an event.

Actionable Intelligence With Behavior Analytics

SNYPR detects threats using patented machine learning and statistical analytic models including mix-max clustering, peer analysis, event rarity analysis, predictive learning, robotic pattern detection, DGA detection and sequential learning. Using out-of-the-box threat models, the solution stiches together a chain of events to surface the highest risk events.

Threat Hunting With Securonix Spotter

Securonix Spotter threat hunting capability enables blazing-fast hunting using natural language search. Searching for threat actors and IOCs is simplified with visual pivoting on any entity to develop valuable threat context. Visualized data can be saved as dashboards or exported via standard data formats.

Out-of-The-Box Applications

Securonix provides out-of-the-box content in the form of packaged applications specifically designed for insider threat, cyber threat, fraud and cloud security analytics. The content is delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time to value.

Threat Model Exchange

The Securonix Threat Model Exchange™ is a library of threat models sourced by the Securonix cyber research team in collaboration with our cross-industry client base, partners and national security leaders. The exchange enables customers to access, download and deploy the latest Securonix threat models with a single click.

Long Term Data Retention

Context aware enriched events are stored in HDFS and can be used for long term analysis, search and reporting. Raw event also maintained in HDFS for legal and compliance purposes. Securonix supports transparent disk encryption for security and privacy reasons. The solution also supports archival of data to external storage as needed. The data is HDFS is easily accessible to any external applications.

Investigation & Incident Response

The Securonix Investigation Workbench allows for point-and- click link analysis to rapidly investigate incidents by pivoting on anomalous entities and tracing associated activities and events. With comprehensive incident management and workflow capabilities, SNYPR allows multiple teams to collaborate on investigation and remediation of an incident. Securonix automated incident response framework enables organization to automate remediation actions on select threats.