

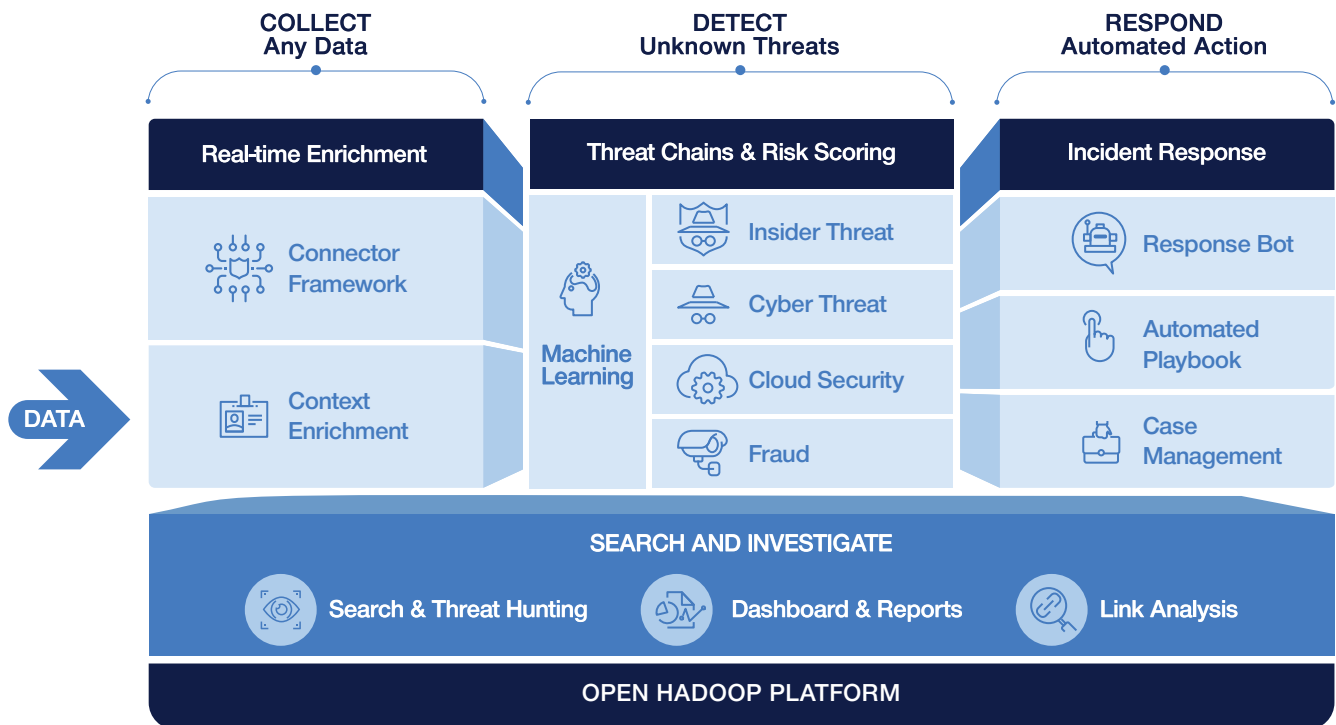
Securonix Next-Generation SIEM

Harness the Power of Big Data Using Machine Learning

The cybersecurity landscape is getting more complex. Hackers continue to innovate, and business technologies generate increasing amounts of data. This is making legacy security monitoring solutions obsolete as they struggle with an inability to scale and weak rule-based threat detection techniques.

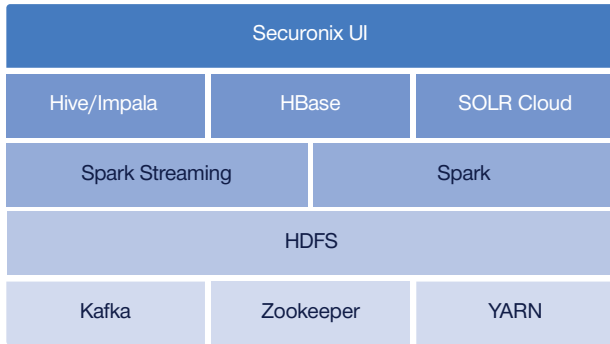
Built on big data, Securonix Next-Generation SIEM combines log management, user and entity behavior analytics (UEBA), and security incident response into a complete, end-to-end security operations platform. It collects massive volumes of data in real-time, uses patented machine learning algorithms to detect advanced threats, and provides artificial intelligence-based security incident response capabilities for fast remediation.

Collect, Detect, and Respond to Advanced Threats



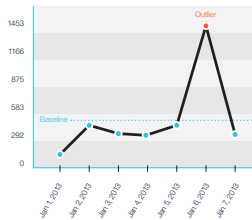
Product Features

Big Data Architecture



- Powered by Hadoop, a massively scalable, fault-tolerant open data platform that ingests hundreds of terabytes per day and supports economical long-term data retention.
- An open data model means you can maintain a single copy of your data in an open data format and make it available to other applications as needed.
- Unlimited long-term retention with over 90% compression.
- 100% native Hadoop components certified on Cloudera and Hortonworks.
- Cost is based primarily on identity instead of by events per second or gigabytes, so costs are predictable, even as your data requirements increase.

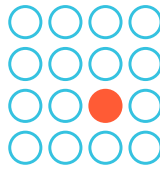
Built-In User and Entity Behavior Analytics



Behavior Analysis



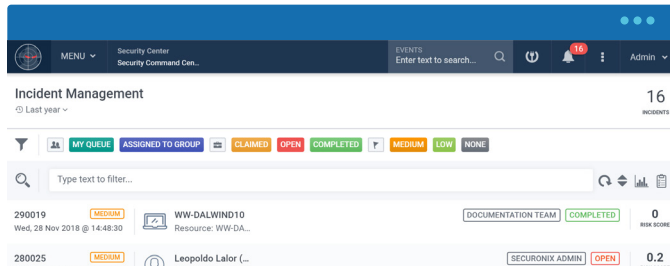
Peer Analysis



Event Rarity Analysis

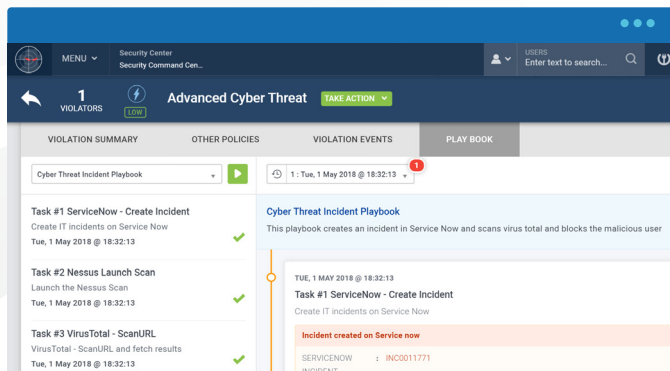
- Built-in UEBA with patented machine learning algorithms accurately detect advanced and insider threats.
- Stitch together a series of events over time using threat chain models in order to surface the highest risk events.
- Securonix comes with out-of-the-box applications delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time to value.
- Continuously refresh use case content through the Threat Library and Threat Exchange.

Threat Hunting and Investigation



- Securonix Spotter enables blazing-fast threat hunting using natural language search.
- Searching for threat actors or indicators of compromise is simplified with visual pivoting available on any entity in order to develop valuable threat context.
- Visualized data can be saved as dashboards or exported in standard data formats.

Intelligent Incident Response



- Securonix Investigation Workbench allows you to rapidly investigate incidents by pivoting on anomalous entities and tracing associated activities and events.
- Built-in incident playbooks include configurable automated remediation actions to shorten time to respond.
- Comprehensive incident management and workflow capabilities allow multiple teams to collaborate on an investigation.
- Securonix Response Bot is an artificial intelligence-based recommendation engine that suggests remediation actions based on previous behavior patterns of Tier 3 analysts.

For more information about Securonix Next Generation SIEM visit www.securonix.com/products/securonix-next-generation-siem/



LEARN MORE
www.securonix.com

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

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix