SECURONIX™

DATASHEET

Securonix User and Entity Behavior Analytics

Detect Unknown Threats Using Behavior Analytics and Machine Learning

Today's cyber threats are more sophisticated, executed on a larger scale, and have the ability to spread rapidly. For example, in 2017 WannaCry infected 45,000 systems across 74 countries within 24 hours. Traditional correlation-based security monitoring tools are not capable of detecting advanced threats like these because they lack the ability to scale, lack a broader context, and have weak analytic capabilities.

Securonix User and Entity Behavior Analytics (UEBA) leverages patented machine learning and behavior analytics to analyze and correlate interactions between users, systems, applications, IP addresses, and data. The solution learns what normal behavior patterns are and creates baselines in order to identify outliers. Light, nimble, and quick to deploy, Securonix UEBA comes with pre-packaged use case content to detect advanced insider threats, cyber threats, fraud, cloud data compromise, and non-compliance. Built-in link analysis, automated response playbooks, and case management workflows allow you to investigate and respond to threats quickly, accurately, and efficiently.

Address a Wide Range of Use Cases

Insider Threat

- Data Exfiltration
- Privileged Account Misuse
- Patient Data Snooping
- IP Theft
- Access Anomalies

Cyber Threat

- Pass-The-Hash
- Lateral Movement
- Ransomware
- Beaconing, DGA
- Phishing

Cloud Security

- Payment Fraud
- Retail Fraud
- Customer Fraud
- Internal Fraud
- Trade Surveillance

Fraud

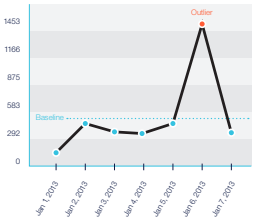
- Anomalous Data Sharing
- Privilege Misuse
- Data Exfiltration
- Unauthorized Login & Access
- External Attacks

Product Features

Entity Context Enrichment

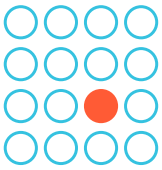
- Build a comprehensive profile of every entity in your environment: users, IP addresses, and hosts.
- Real-time enrichment of events with entity context including identity, asset, geolocation, threat intelligence and data from lookup tables.
- Point in time IP attribution ties dynamic IP addresses to entities.

Behavior Analytics and Machine Learning



Behavior Analysis

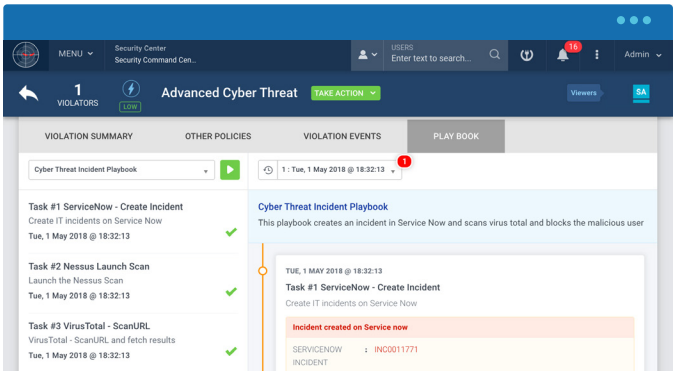
Peer Analysis



Event Rarity Analysis

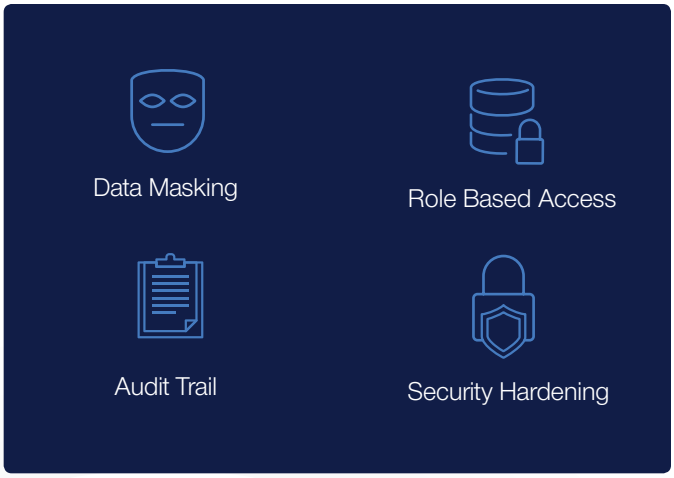
- Apply sophisticated, patented machine learning algorithms to event data in real time to accurately detect advanced and insider threats.
- Stitch together a series of events over time using threat chain models in order to surface the highest risk events.
- Securonix comes with out-of-the-box use cases delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time to value.

Investigation and 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.

Data Privacy



- Robust role based access controls mean that different user groups will only see the data they are entitled to.
- Data masking protects protect an individual's data and privacy and prevents users from accessing sensitive data unless they have a specific need to.
- A full audit trail means that you will be able to track and investigate all activity in the solution.
- Privacy capabilities approved and certified by more than 15 works councils across Europe and Asia Pacific.

For more information about Securonix UEBA
visit www.securonix.com/ueba

SECURONIX™

LEARN MORE
www.securonix.com

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

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