SECURONIX
Security Analytics. Delivered.

DATASHEET

Securonix UEBA 6.0

The #1 Analyst Rated UEBA Solution

Modern threats are complex, often executed with compromised credentials or with the help of insiders with legitimate credentials, and carried out over long periods of time. Predicting, detecting and containing these threats is near-impossible using traditional signature- based solutions that were not developed to protect organizations from modern day cyber or insider attacks. Securonix UEBA 6.0 is purpose-built to rapidly detect any threat, anywhere, leveraging machine learning and behavior analytics that analyzes and cross-correlates all interactions between users, systems, applications, IP addresses and data to detect advanced insider threats, cyber threats, fraud, cloud data compromise and non-compliance.

Light, nimble and quick to deploy, Securonix UEBA version 6.0 is faster and smarter. It comes with a new, ultra-modern user experience based on design concepts that provide intuitive visualizations of enterprise risk and one-click actions for threat management and incident response. New enhanced analytical and machine learning capabilities have been added to detect ransomware and advanced cyber-attacks. Securonix UEBA 6.0 has 350 out-of-the-box connectors and over one thousand one-click deploy threat models that immediately deliver tangible value.

WHAT'S NEW IN SECURONIX UEBA 6.0?

Advanced Behavior Analytics

Events that can look harmless in isolation often map into high-risk threats when analyzed in context over time. UEBA 6.0 correlates and analyzes events from multiple sources such as user, device, asset, application, and network segment to predict, detect and contain slow-and-low attacks that are invisible to legacy solutions. 200+ new threat models have been added to this release in addition to tuning of existing models for further risk refinement.

Quick Time-to-Value

Getting UEBA 6.0 up and running is even faster and more automated than ever before. With built-in data connectors and pre-packaged use cases, implementation is swift and results are immediate.

Adaptive Learning Framework

UEBA 6.0 uses adaptive learning and supervised classification algorithms to provide real-time feedback to the system based on the findings and remediation patterns. This improves threat fidelity, threat detection and operational efficiency by cutting out the need for security analysts to manually tune the system.

More Packaged Applications For Fraud, Trade Surveillance and Patient Data Analytics

Securonix uses packaged solutions to provide out-of-the-box use cases for specific threats and industries, plus use case models, dashboards and reports. UEBA 6.0 comes with new line-of-business use cases, dashboards and reporting for fraud, trade surveillance and patient data analytics.

Threat Model Exchange

UEBA 6.0 comes packaged with The Securonix Threat Model Exchange®, 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.

Enhanced User Experience

Securonix 6.0 has a new user interface with elegant visualizations of enterprise risk and intuitive, easy-click actions to mitigate threats and risk. The solution also provides data insights and fully customizable dashboards. The entity risk view have been updated to provide a full 360-degree perspective on an entity's risk profile.

Securonix UEBA Cloud

Securonix UEBA Cloud delivers the solution as a turn-key cloud-based service. Customers get all the benefits of UEBA 6.0 without the hassle of managing and maintaining the platform. The solution is highly scalable and secure and is ideal for organizations that are looking for rapid deployment and quick time to value.

LEARN MORE
www.securonix.com

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

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

Insider Threat

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

Cyber Threat

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

Fraud

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

Cloud Security

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

- **Privileged Account Analytics**
- **Data Security Analytics**
- **Cyber Threat Analytics**
- **Cloud Security Analytics**
- **Applications Security Analytics**
- **Access Analytics**
- **Patient Data Analytics**
- **Fraud Analytics**
- **Trade Surveillance**

KEY PRODUCT FEATURES

Real-time Behavior Analytics

Patented unsupervised and supervised machine learning and statistical algorithms profile normal activity and detect anomalies. Some of the key signature-less techniques include mix-max clustering, peer analysis, event rarity analysis, predictive learning, fuzzy correlation, robotic pattern detection, DGA detection and sequential learning.

Connector Library

350+ out-of-the-box connectors integrate with a variety of structured and unstructured data sources including enterprise applications, identity systems, and non-technical data sources such as badge readers and social media that are not supported by typical log management solutions.

Packaged Applications

Out-of-the-box content in the form of packaged applications specifically designed for insider threat, cyber threat, fraud, and cloud security analytics is delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time to value. Key packaged applications include: data security analytics, privileged account analytics, cyber threat analytics, application security analytics, cloud security analytics, fraud analytics and patient data analytics.

Predictive Learning

Algorithms analyze patterns of behaviors to predict future risks associated with a user or entity. For example, a user whose behaviors indicates an intention to quit would be flagged for the elevated risk of data theft associated with employees who plan to leave their jobs. Predictive analytics can also inform decision automation such as access blocks or increased authentication requirements.

Investigation and Response

Full incident management capabilities investigate and respond to threats including link-analysis with drag-and-drop graphical representation for ad-hoc investigations, reviews and analysis. Plus, case management capabilities with out-of-the-box, dynamic workflows based on industry best practices are built into the platform. Case management workflows are fully customizable based on client need.

Data Privacy

A critical capability for UEBA solutions that leverage contextual user behavior patterns, UEBA 6.0 provides complete data masking and encryption capabilities to protect user identities while still enabling robust analytics on their activities. With granular, role-based access control, access and entitlements to data can be limited by business needs. Detailed logging capabilities are available to ensure a full audit trail of all activities within the solution.

Cyber Threat Hunting

Securonix Spotter threat hunting product 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.