SECURONIX™
Security Analytics. Delivered.

DATASHEET

Securonix Security Applications

Extended Use Cases. Delivered.

Securonix revolutionizes security with a security analytics platform that combines log management, security incident and event management (SIEM), and user and entity behavior analytics (UEBA) into a complete, end-to-end platform that can be deployed in its entirety or in flexible, modular components. It collects massive volumes of data in real-time, uses machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response.

Securonix comes packaged with out-of-the-box applications specially designed for insider threat, cyber threat, fraud, cloud security and trade surveillance use cases, delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time-to-value. Threat models are fully customizable from the user interface, providing flexible tuning to your unique needs.

Address a Wide Range of Use Cases

Insider Threat

- Data Exfiltration
- Privileged Account Misuse
- Data Snooping
- Personal Risk Indicators
- Login/Badge Anomalies

Cyber Threat

- Beaconing, DGA
- Lateral Movement
- Ransomware
- Password Spraying
- Covert Channels
- Account Takeover

Cloud Security

- Data Exfiltration in Cloud
- Privilege Misuse
- Unauthorized Configuration Changes
- Suspicious Login/Access Pattern
- Set Up Authentication

Fraud

- Payment Fraud
- Wire Transfer Fraud
- ATM/Credit Card
- Customer Fraud
- Internal Fraud
- Trade Surveillance

Using Threat Chains to Find Advanced Threats

An individual anomaly, when looked at in isolation, may seem innocuous. However, a combination of anomalies over a period of time or in a particular sequence could be an indicator of a sophisticated cyberattack. Securonix threat chains are designed to predict and detect the series of events that indicates an advanced attack. In each pre-packaged application, Securonix provides out-of-the-box threat models that can rapidly scan through historical or real-time data to predict and detect advanced threats. Customers can view and edit the logic built-into threat models or change the risk scores to suit their unique business needs.

Share Best Practices with the Threat Model Exchange

The Securonix Threat Model Exchange™ is an online library of threat models created by the Securonix cyber research team in collaboration with customers, partners, and national security leaders. The Securonix Threat Model Exchange is available exclusively to Securonix customers and is fully integrated into the Securonix solution. Customers can access the online library from their Securonix application interface and download and deploy the latest Securonix threat models with a single click.

Use Your Own Custom Applications

Securonix solutions provide an open-data model which enables you to use raw or enriched data in your own applications. You can add your own custom analytics applications that you build, or acquire from third parties and plug them into the Securonix open data platform.

Securonix Security Applications

Insider Threat Application Bundle
The bundle consists of the Data Security Analytics Application, Privileged Account Analytics Application, and Access Analytics Application. These applications are not available separately.

Data Security Analytics Application
Ingests data from sources such as email, data loss prevention (DLP), proxy, cloud applications, and printers. Baselines normal behavior patterns to detect data exfiltration attempts coming from inside or outside your organization as well as potential data compromise situations. Applies predictive behavior analytics to identify, profile, and monitor users whose behaviors indicate they are at an elevated risk for data theft.

Privileged Account Analytics Application
Ingests data from sources such as Active Directory, UNIX, databases, privileged identity management (PIM) solutions, and privileged access management (PAM) solutions. Baselines and monitors privileged user and service account behavior to detect events such as rare suspicious transactions, login anomalies, credential misuse, account compromise, and credential sharing.

Access Analytics Application
Ingests entitlement data from authentication sources such as Active Directory, enterprise applications, and identity and access management (IAM) solutions and analyzes it using peer comparisons, fuzzy logic, and segregation of duties (SoD) libraries to detect high-risk outlier access. Identifies rogue access attempts and supports risk-based access management and review. Integrates with authentication systems to decommission, block access, or step up authentication for high-risk users.

Cyber Threat Analytics Application
Ingests data from sources such as firewalls, proxy, VPN, intrusion detection systems (IDS), DNS, endpoints, and NetFlow devices. Baselines normal behavior and detects malicious patterns such as beaconing, connections to digitally-generated domains, robotic behavior, rare executables and programs, lateral connections, and unusual web activity. Monitors security logs and network flows in order to detect malware infections (such as zero day attacks and ransomware), system compromise, lateral movement, pass-the-hash, pass-the-ticket, and other advanced threats.

Cloud Security Analytics Application
Monitors your cloud infrastructure platforms and applications for data exfiltration attempts, privilege misuse, advanced external attacks, and access anomalies. Performs data discovery and classification in cloud applications and manages dynamic permissions to critical infrastructure. Supports integration with several cloud services including O365, Google Apps, Box, Salesforce, Workday, Hightail, Netskope, Okta, Ping, AWS, and Azure.

Patient Data Analytics Application
Monitors the activity of users accessing electronic medical records in clinical applications and detects attempts at data snooping and data exfiltration. Contains specific algorithms to detect different types of snooping events including family snooping, co-worker snooping, VIP snooping, self-examination, age-based anomalies, and location-based anomalies. Integrates with several clinical applications including EPIC, Cerner, Medicity, and Allscripts. Provides use cases, built-in reports, and dashboarding capabilities for compliance requirements such as HIPAA and HITECH.

Fraud Analytics Application
Baselines normal transaction behavior based on actor, target, location, time, frequency, and sequence in order to detect fraudulent behavior patterns such as spikes in transactions, misuse of discount or promotional codes, suspicious refunds, fraudulent prescriptions, rogue orders, and suspicious shipping requests. Contains packaged use cases for many types of fraud including healthcare, ATM, online banking, retail, customer, and customer service reps.

Trade Surveillance Application
Ingests any type of structured or unstructured data, including but not limited to: orders, trades, positions, market data, email, chat logs, user activity, know your customer (KYC), and customer relationship management (CRM) data. Sophisticated threat and behavior models coupled with trade and compliance analytics identify and monitor the riskiest traders, portfolio managers, securities, and accounts. Narrows down the entities compliance officers should focus on.

For more information about Securonix Security Applications visit www.securonix.com/securonix-apps/