**Insider Threat Detection**

**Bringing Clarity to Insider Threat**

### Overview

#### Industry
- Cross Industry Solution

#### Securonix Use Cases
- Insider threat detection
- Fraud detection & Prevention
- Data theft detection & prevention
- VIP snooping detection & prevention

#### Business Impact
- Predictive threat detection
- Reduced breach impact
- Comprehensive threat response & investigation
- Quantified, non-subjective threat and risk reporting

#### Data Sources
- Application logs and entitlements
- HR/Identity information
- Proxy logs (optional)
- DLP events (optional)

#### Relevant Compliance & Security Best Practices
- SOX
- PCI DSS
- HIPAA/HITECH
- FARC/NERC

---

**Challenge:** The Wrong Tools for the Job

Employees and contractors have a significant advantage over the organization’s primary security mechanisms (e.g. firewalls, access controls, physical access controls) that are built for the untrusted external attacker and not for the trusted insider. Furthermore, people working for or within the organization are aware of the mechanisms in place and can use this knowledge to circumvent defenses. In order to counter this advantage and realistically address insider threats, organizations need better capabilities in such areas as context-based monitoring, advanced behavior anomaly detection, and link-analysis driven investigation.

**Solution:** Turn-key Insider Threat Detection and Management Platform

The Securonix solution is built to address these challenges by delivering these capabilities in an out-of-the-box solution that does not require a long-term data analytics and discovery project. Using purpose-built data mining, correlation, enrichment, and analytics, the Securonix solution detects not only users with high risk identity profiles but also high-risk activity, access, and events in your organization associated with insider threats. Simply put Securonix produces Insider Risk Intelligence. It does this by mining and analyzing a diverse set of user, system, application, security event, physical access, and even telephone activity to identify abnormal behavior associated with data theft/misuse, fraud, or IT sabotage. Beyond detection, Securonix performs continuous monitoring, scoring, reporting, and advanced investigative capabilities. The solution provides the advanced technology needed for a complete insider threat management program that leverages your existing security programs/investments.

- Purpose-Built Analytics for rapid, consistent and quality analysis across key sources
- Big Data Scale to support real-time data mining and threat detection against large data feeds
- Automated Correlation and Enrichment of identity and threat information across multiple internal and external sources
- Peer Group Analysis of users’ behavior and access against their peers for automated outlier anomaly detection
- Behavior Analysis of users, peer groups, accounts, and systems for signature-less detection of insider threats
- Application & Data Risk Visibility for monitoring insider threats at the targets
- Advanced Scoring & Visualization for effective, efficient, continuous reporting of insider risk and threat levels
**Benefit:** Better Access Control and Efficiency

Securonix provides a rapid entry to actionable insider threat intelligence giving you the visibility into the highest risk users in your environment and the tools to monitor, report on, and investigate them.

- Predictive threat detection
- Reduced breach impact
- Comprehensive threat response and investigation
- Quantified, non-subjective threat and risk reporting

**Solution Tour**

**User Risk & Threat Monitoring**

Securonix continuously builds a comprehensive risk profile of a user based on identity/employment, security violations, IT activity and access, physical access, and even phone records. All identity, activity, and access characteristics are compared to their baseline, their peers, and known threat indicators to identify true areas of risk. All results are scored and presented in interactive scorecards.

**High privileged Account (HPA) Monitoring**

HPAs are a primary source of insider misuse and a platform for attacks. Securonix automatically identifies HPAs such as administrator, service, and shared accounts then monitors them for abnormal behavior associated with an attack while linking the high-risk behavior back to a real user and their risk profile to give the potential threat full context.

**Application & Data Risk Monitoring**

Insiders attack sensitive data, transactions, or the systems and applications that host them. Securonix addresses this threat by monitoring critical applications and systems at the transaction, data set, or sensitive user record level. Similar to a user, Securonix continuously builds a risk profile for all applications and systems that identifies all high-risk users, access, and activity associated with their sensitive data and transactions. All results are scored and presented in application risk scorecards.

**Advanced Enterprise Fraud Detection**

Insider fraud is typically conducted over a long period of time or through complex activity designed to get around the known threat or “signature-based” detection methods. Securonix addresses this blind spot with advanced “signature-less” behavior and peer based outlier analysis techniques that are highly effective at identifying “slow and low” and complex fraud attacks.