SECURONIX

Security Analytics. Delivered.

User & Entity Behavior Analytics For Compliance

securonix.com

info@securonix.com

SUPPORTING COMPLIANCE EFFORTS WITH USER & BEHAVIOR ANALYTICS

UEBA (user & entity behavior analytics) has emerged as the most promising solution to rampant cyber threats and fraud because it allows security leaders to finally get ahead of attackers by rapidly detecting risks to what they're actually tasked with defending: the data!

UEBA tools have proven to be extremely valuable for defending against insider threats, cyber risks and fraud use cases across both private and public sector organizations. UEBA leverages unsupervised machine learning and artificial intelligence capabilities based on a number of technical components including data analytics, data integration, data visualization and source systems analysis.

According to Gartner:

"The understanding of user behavior and management of user access is becoming a fundamental component in the management of enterprise risk. Each user touched by the connections of digital business — customers, third-party contractors and professional consumers (prosumers) — must enjoy proper access to services, but these access mechanisms must also enable the enterprise to limit fraud and to secure operations... Security leaders need to fully engage with technology trends if they are to achieve and maintain effective, efficient security programs that balance digital business opportunities against business risks." (Cool Vendors in UEBA 2016, May 2016.)

There is no question that UEBA technologies are making a large impact in the cyber and insider threat space. So how can we apply machine learning, artificial intelligence and analytics to our compliance efforts?

From access reviews to proving compliance with thousands of control objectives in numerous regulatory, security and risk frameworks, UEBA reduces the overhead and complexity and increases the accuracy of your compliance and reporting efforts while making the process more automated and risk driven allowing your teams to be focused on those areas of effort that are most critical.

What we will look at in this paper is applying UEBA capabilities to assist with compliance efforts. Regardless of the framework you are complying with (GLBA, FISMA, FFIEC, HIPAA PCI-DSS, security frameworks such as ISO or SANS 20, or risk frameworks such as NIST or COBIT), UEBA can support compliance with and reporting on a large number of these controls, making traditional manual, time

onsuming processes redundant. The power of the technology can support your efforts in three ways:

- Allows for very detailed, very specific use cases supporting things like anti-money laundering, trade surveillance, internal and external fraud as well as abuse in financial sectors, VIP snooping, PHI violations in the healthcare industry and improper access to credit card data in PCI-DSS.

- Supports consolidation and harmonization of control sets. Due to the increased number of regulations organizations must comply with, companies are working to consolidate and communize sets of ompliance controls. UEBA technology can be used to fulfill the requirements across all of the consolidated objective sets. Hundreds of use cases can be used to support controls across audit and risk, monitoring and measurement, physical security, human resource management, configuration and records management, privacy protection, third party management, access management including separation of duties, privileged account management and data management.

- Third, UEBA can be used to support access reviews, which are part of numerous regulations. The old method of manually reviewing hundreds of thousands of access permissions is unmanageable and inaccurate. Utilizing analytical capabilities such as behavior base-lining, rarity and peer group analysis, organizations can detect access outliers, detect segregation of duties violations, analyze rogue, orphaned or terminated accounts, drive user self-service access reviews and support risk based access reviews.

Compliance efforts mirror closely your information security and risk programs in that they require fully integrated, people, processes, technologies and governance models. Successful models leverage technology to eliminate silos between the people, process and governance efforts and between various compliance efforts. UEBA technology has been able to do what other technologies have not; support and empower the people, process and governance functions.

For more details on how UEBA can support your compliance efforts, please contact Securonix at info@securonix.com or go to www.securonix.com.

ABOUT SECURONIX

Securonix is radically transforming all areas of enterprise security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately. Globally, customers are using Securonix to address the most basic and complex needs around advanced persistent threat detection and monitoring, high privileged activity monitoring, enterprise and web fraud detection, application risk monitoring and access risk management. For more information visit www.securonix.com.

CONTACT SECURONIX

info@securonix.com | (310) 641-1000