KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | October 2016

Securonix Security Analytics Platform

Securonix Platform provides advanced security analytics technology for collecting, analyzing and visualizing a wide range of business and security information, converting it into actionable intelligence and serving as a basis for a broad portfolio of specialized security solutions.

by **Alexei Balaganski**
ab@kuppingercole.com
October 2016

Content

Related Research

Advisory Note: Real Time Security Intelligence – 71033

1 Introduction

Securonix is a privately held security analytics solution vendor headquartered in Addison, Texas, USA. Founded in 2008 by a team of seasoned experts in information security, risk management and identity compliance, the company brought their first product to the market in 2011 and has been steadily growing ever since. Currently, the company has over 250 employees in the USA, UK, Australia and India and a large global partner network. With a strong focus on developing a healthy technology ecosystem, Securonix provides a substantial number of integrations with different security solutions, as well as maintains strategic partnerships with large integrators and consulting companies.

Since the notion of a corporate security perimeter has all but disappeared in the recent years thanks to the growing adoption of cloud and mobile services, information security has experienced a profound paradigm shift from traditional perimeter protection tools towards monitoring and detecting malicious activities within corporate networks. Increasingly sophisticated attack methods used by cyber criminals and even more so, the growing role of malicious insiders in the recent large scale security breaches clearly indicate that traditional approaches to information security can no longer keep up.

Thanks to a breakthrough that led to commoditization of big data analytics technologies, a new generation of security analytics solutions has emerged in the recent years, which are able to collect, store and analyze huge amounts of security data across the whole enterprise in real time. Enhanced by additional context data and external threat intelligence, this data is then analyzed by various correlation algorithms to detect anomalies and thus identify possible malicious activities. Unlike traditional SIEM solutions, such tools operate in near real time and generate a small number of security alerts ranked by severity according to a risk model and enriched with additional forensic details. Thus, they are able to greatly simplify a security analyst's job and enable quick detection and mitigation of cyber-attacks.

Securonix has been focusing on developing such solutions from the very beginning, and currently they are offering a broad portfolio of specialized security analytics products in areas like Privilege Management, Application Security, Network Security, Data Exfiltration intelligence and so on. However, the common underlying technology for all these solutions is the Securonix Security Analytics Platform – an advanced analytics technology for collecting, analyzing and visualizing a wide range of business and security information, converting it into actionable intelligence and serving as a basis for a broad portfolio of specialized security solutions. A unique differentiator of this platform is a broad range of data sources of security information about users, devices, networks, applications and cloud services, which can be consumed and correlated, as well as a large number of integrations with third party IAM, DLP, PAM, SIEM and other security tools.

Currently, the company is primarily targeting large enterprises, with around one third of Fortune 100 companies in verticals like financial services, healthcare, manufacturing and retail using Securonix Enterprise solutions. However, recently the company has expanded towards mid-market companies, being able to offer them a specialized product to address their most critical security issues like fraud detection or risk monitoring. Supported by a global network of technology partners, service providers and consultants, Securonix is steadily increasing their presence outside of their home market towards European, Latin American and Asia-Pacific regions.

2 Product Description

Securonix Security Analytics Platform is the technological foundation of the company’s product portfolio. It is an advanced security analytics technology that has been designed from scratch to be extensible and scalable, capable of supporting a broad range (over 200) of data sources across the enterprise. On premises, it can be deployed rapidly as a prepackaged bundle including the Securonix platform and the Cloudera Hadoop distribution or installed on pre-existing Hadoop clusters. Through the company’s service partners, customers can deploy Securonix as a managed service or run it in the cloud.

A key differentiator of the Securonix platform is its flexibility and extensibility: it provides a broad range of predefined threat models and over 100 out-of-the-box connectors to identity management and security tools to collect identity data, access and entitlements, as well as activities and violations from existing corporate infrastructure. This allows the product to support almost any data source within the corporate IT infrastructure: networks, devices, applications and even cloud services. For each supported data source, the platform automatically applies appropriate behavioral models and analytics. It is even possible to define custom analytical models for specific data sources.

All information consumed by the platform is enriched with additional context attributes, which can be automatically extracted using over 40 predefined operations or custom rules. Also, a key operation is identity attribution – each incoming event is automatically linked to a real identity. The real-time correlation engine is thus able to tie each security event to an entity within the enterprise, be it a user, device or an organizational unit. A behavioral baseline is automatically established and maintained for each such entity.

After a period of initial training, when the platform is adjusting to the particular corporate network and establishing “normal” behavior patterns for entities, the solution can begin identifying anomalies in activities across the company, detecting potential malicious attacks, insider threats caused by excessive privileges and so on. The technology based on peer group analysis and behavior analytics is able to identify such incidents without relying on signatures or predefined rules.

Incidentally, the platform is not only able to connect to corporate user directories, but to other identity sources, such as HR systems, as well. This provides substantially more advanced capabilities to detect potential malicious insiders by taking into account such information like performance reviews, promotions or even users browsing job sites. This may naturally lead to potential violations of privacy regulations, which is why Securonix incorporates a number of measures to address them. This includes masking and encryption to anonymize employee information, as well as defining separate policies on geographic basis. Only designated legal or privacy officers can expose an employee involved in a security incident. The company claims that their product is currently the only one officially approved by German and Belgian workers’ councils.

Since companies may face different types of threats, for which different teams are responsible, the platform allows defining different threat categories with different threat indicators. Depending on a specific analyst accessing the threat and risk dashboard, they will be presented with a different risk scoring and prioritization of security incidents.

A rich set of out-of-the-box reports is provided, with specialized reports for each supported system, compliance reports, as well as hundreds of filter templates for ad-hoc reporting. Automated scheduled reports are supported as well.

To perform forensic investigations, the solution includes a specialized Investigation Workbench, which provides visualization of connections between users, systems, activities and other relevant data involved in an incident. Recently, the company has added SPOTTER – a natural language search engine – to the platform, which provides instant access to all real-time and historical details of each detected threat.

Each investigated activity is assigned a verdict, ranging from an “approved action” or “exception” to “non-concern” to “confirmed violation”. This verdict will have an effect on similar future incidents, as well as influence the risk score of the user involved. For more complicated investigations, custom workflows can be created, involving multiple steps and several analysts.

A number of remediation capabilities are implemented as well, such as disabling a user account in the corporate Active Directory or blocking the device’s IP on a corporate firewall. These functions rely on integrations with third party security tools, IAM systems, SIEM solutions and other products. Naturally, the platform supports integrations with external threat intelligence providers as well. The company is also encouraging crowdsourcing by allowing customers to share their threat models and other information.

Besides the enterprise version of their platform, which incorporates all available functions, Securonix offers a number of specialized applications for smaller companies to address their specific critical issues. A few notable examples include the following:

- **Data Exfiltration Intelligence**, which provides a proactive, context-driven approach to data loss prevention. By consuming data from already deployed DLP solutions and correlating it with real identities, applying behavior analytics and taking application and endpoint risk scores into account, this solution reduces the number of DLP alerts by at least 90%.
- **Privileged Account Monitoring**, which can automatically identify high-privileged human, service and shared accounts, attribute shared accounts to real identities and rapidly detect anomalous activities using peer group analysis. This solution can operate standalone or integrate with leading PxM solutions to improve protection against malicious insiders.
- **Network Security Analytics**, which provides real-time analysis and correlation of security data collected from network devices to detect malicious activities like malware attacks or advanced persistent threats. By combining current and historical data, it can detect multi-stage attacks as well. Without relying on signatures, the solution can identify zero-day attacks and most sophisticated fraud scenarios.
- **Application Security Analytics**, which integrates with leading ERP, financial, healthcare, document management and other enterprise applications and provides continuous monitoring at the individual transaction level. The solution maintains up-to-date risk profiles for each application and identifies risky activities associated with sensitive data.

Thus, Securonix Security Analytics Platform can be considered one of the most advanced implementations of the Real-Time Security Intelligence concept defined by KuppingerCole.

3 Strengths and Challenges

Securonix Security Analytics Platform provides a truly advanced security analytics technology for collecting, analyzing and visualizing a wide range of business and security information and converting it into actionable intelligence. What sets Securonix apart of many other players in this market is the platform's extensibility and a broad range of connectors and integrations with third party identity management and security products.

The ability to collect and correlate security events across all IT systems, applications and even cloud services, impressive context enrichment capabilities and a powerful correlation engine that is freely customizable ensure that the platform is able to provide a security analyst with the most comprehensive incident investigation tools. This is further enhanced with built-in privacy controls officially approved by workers' unions in several countries. Unfortunately, the solution's active remediation capabilities are rather limited in comparison, relying mostly on custom integrations with third party tools.

Although focusing primarily on large enterprise customers, the company is able to utilize the platform's flexibility to offer a number of specialized security analytics products, which can be interesting for smaller companies looking for solutions for their particular security problems. However, the sheer number of offered products without a clear upgrade strategy may be confusing for some customers.

Strengths	**Challenges**
● A unique platform architecture focused on scalability and extensibility ● Broad range of supported data sources ● Strong focus on identity, including built-in privacy controls ● Large number of out-of-the-box connectors and integrations ● Every aspect of the analytics engine is customizable ● Impressive portfolio of specialized security products based on the common platform	● Threat remediation capabilities quite limited, rely on custom integrations ● Still relatively small market presence outside of North America ● Sheer number of offered specialized products may be confusing for some customers

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com