SECURONIX

DLP-аналитика

Общее описание

Платформы

- Кросс-платформенное решение

Поддерживаемые приложения

- Symantec Vontu
- McAfee DLP
- Websense

Сценарии использования Securonix

- Выявление и предупреждение кражи данных
- Снупинг VIP-клиентов
- Защита IP-адресов
- Securonix для Vontu
- Securonix для Websense
- Securonix для DLP от McAfee

Влияние на бизнес

- Снижение риска кражи конфиденциальной информации
- Упреждающее определение угрозы данным
- Уменьшение риска необратимой потери информации

Источники данных

- Журналы работы и доступа к приложениям
- Кадровая/идентификационная информация
- Журналы прокси-серверов (опционально)
- DLP-события (опционально)

Соответствие требованиям стандартов и рекомендации по безопасности

- SOX
- PCI DSS
- HIPAA/HITECH
- FISMA
- FERC/NERC

Предотвращение утечки данных при помощи контекстно-зависимой DLP

Проблема: слишком много шума, слишком мало контекста

Today's targeted attacks, whether launched by insiders or by external hackers, are primarily focused on stealing an organizations most sensitive data. The primary defense for organizations is application access controls and in some cases DLP (Data Loss Prevention) monitoring tools. Fully deployed, these controls tend to be defenseless against motivated insiders or outsiders and they generate a continuous stream of false positives. To combat these complex threats effectively, organizations need better context of a user's identity, behavior and their associated peers in order to pinpoint the real attacks and to focus monitoring efforts on what is high risk before it is too late.

Solution: Context-Aware Driven DLP

Securonix addresses this challenge through real time monitoring and analysis of sensitive data access and usage at the source in applications (e.g. SAP, Oracle eBusiness, EPIC, other COTS, custom) and data repositories (e.g. SharePoint, Documentum, etc.). Securonix automatically detects high-risk data access and usage for real-time investigation and access removal thereby reducing the exposure to sensitive data at its source. Meanwhile, if DLP monitoring at the endpoint, egress, or host is being used, Securonix will automatically identify the true high-risk DLP events through advanced identity, behavior and peer group analysis. The combination of these advanced monitoring and detection techniques provides the real user identity and behavior context to rapidly detect the most complex data theft and snooping attacks.

Benefits: Proactive Data Loss Prevention

Whether you have a fully functional DLP program or not, Securonix's DLP Intelligence solution can provide the following:

- Immediately reduce the exposure to sensitive data by users with unauthorized or high-risk access
- Better detection of advanced and targeted data attacks
- Focus DLP monitoring and investigation to true high risk events and people

Solution Tour

Securonix LLC
5777 Century Blvd Suite 838
Los Angeles, CA
90045
Phone: (310)641-1000
Fax: (310)997-3529
Email: info@securonix.com

Sales Office
Sales Information:
Email:sales@securonix.com
Phone: (415)241-9000

For more information visit our Website: www.securonix.com

Securonix provides a wide variety of advanced security analytics solutions including:

- DLP Intelligence
- Identity & Access Intelligence
- Insider Threat Detection
- SIEM Intelligence
- HPA Security Monitoring
- Big Data Security Intelligence
- Cyber Threat Intelligence
- MSSP Solutions
- Continuous Risk Monitoring
- Compliance solutions

To view more solutions from Securonix, please go to the solution section on our website: http://www.securonix.com/security-intelligence-solutions.

Application and System Level Data Risk Monitoring

Sensitive data including trade secrets, product recipes, BOMs, personally identifiable information, sales quotes, proposals, credit card records and other information reside in several formats and data stores across the enterprise. It is not uncommon for this data to be in collaborative business applications like SAP or spread across repositories such as SharePoint or Documentum in unstructured formats. Securonix utilizes identity and access analytics to automatically identify and continuously monitor for high-risk access and activity associated with this data based on abnormal behavior or access compared to the users past behavior or their peer groups' behavior. This "data risk intelligence" allows an organization to dramatically improve their primary data protection control of access by removing unauthorized or unnecessary access while giving them real time continuous monitoring control over sensitive data.

DLP Event Analysis and Prioritization

The Securonix solution analyzes all incoming DLP alerts and quantifies the risk for each alert while drastically reducing the number of false positives. In order to accurately quantify the risk, Securonix uses behavior analysis, peer group analysis, and user-defined threat and risk policies. Using behavior profiling techniques, Securonix identifies abnormal patterns in DLP alerts and assigns them a risk rating, requiring further investigation. This technique considers more than 120 behavioral parameters spanning time windows, frequencies, network sources, and alert metadata. By comparing DLP alerts generated for a user with multiple peers for the user, the solution dramatically reduces the rate of false positives and accurately quantifies the risk for the alerts that pose the most threat to your data. Organizations can use the identity and business context in conjunction with the DLP alert data to generate their own set of policies for continuous monitoring and risk quantification. The risk-ranked DLP alerts that are true threats to your data are shown in a prioritized queue for security professionals to investigate and remediate.