Transforming data2knowledge

D2k Secure Solution Brief

Problem: The Inside Threat

The global financial industry loses billions of dollars through fraud and system tampering. Maintaining system security requires constant surveillance and monitoring of systems to detect unauthorized or unlawful usage. Even with sophisticated surveillance systems, theft often goes unrecognized until it is too late. This is because over 65% [1] of electronic fraud is committed by expert insiders with an intimate knowledge of the systems and their weaknesses.

The success of preventing fraud depends on the capability to detect and recognize suspicious system usage patterns. Audit records are generated rapidly in real time, often by several systems in different log file formats, making it is extremely difficult to view them in a parallel and recognize patterns across sources.

Solution: d2k Secure

D2K Secure transforms the contents of an unlimited number of log files into a single structured database. Instead of masses of irrelevant data, security analysts are able to view relevant patterns with full links to the original audit trail sources. D2K Secure generates real time alerts when suspicious usage patterns are recognized in the logs.

D2k Secure utilizes the full power of the core D2k Integrated Structuring Platform [2] with Transaction Log specific data source configuration templates and GUI's.

Features and Functionality

- Ø Reads transaction log information from system log files generated by any system in a wide range of any formats
- Ø Interprets and transforms specified log files into a unified data structure
- Ø Specialized GUI's allow users to define patterns of interest
- Ø Transaction log data filtered so only data relevant to the predefined conditions is presented
- Ø Automatic alerts in real time when defined conditions met
- Ø Previously unspecified source files can be defined and processed at any time following initial set up through a specialized GUI
- Ø Archive and query historical data
- Ø Recognizes if the requested data is not in an active database and alerts the user which data tape is required.
- Ø Extends beyond Audit logs to monitor the logs of network security devices (firewalls,etc.) to identify systematic threats & attacks, enabling preventative action.

How does d2k secure work?

System & audit logs generally consist of lines of text composed of several fields, this text correspond to events within a bank's system. The description of any event within a system, written to a log file for example an error message, log-on message or a transaction description in a report, are all referred to as messages. Transactions in a table are also considered to be messages. Often several lines together form a logical unit or the contents of a field needs to be further divided to interpret the events in the

system.
D2k secure automatically defines the static attributes of events class, source, etc, within the bank's systems. Then allows the user to select, decompose and regroup individual messages. In this phase several messages may be grouped to a single higher-level object and as the process is iterative, these higher-level objects may be grouped again into a next higher-level structure. This hierarchical structure is known as the General Data Model; a relational model behind transactions like money transfers, credit card use and the activities of different users such as logging in to different systems and authorizing transactions of different users (system administrators, cashiers, other clerks etc).

Through specialized wizards D2k secure allows the user to quickly define the semantics of a message. For example the parameters it contains and how it fits into the general data model, to which message group in the hierarchy does it belong and what parameters does it add to, or modify within the group. During the generation of the General Data Model, D2k Secure maintains the links between the objects so it is possible to identify the sources for each object, down to the level of individual log entries.

Why Chose D2k Secure?

Automatic systems are available on the market but none has the flexibility to integrate and analyze logs from several platforms, and non-standard proprietary systems. Leading database vendors have Log Analysis Tools for their database management systems. However they are purpose designed for a specific type of application log. The alternative is manual searching of logs, a very laborious and costly process. D2k secure provides the only cost effective solution to recognizing suspicious usage patterns, in real time, across different systems.

For more information please contact Data2Knowledge:
US: +1 (0) 201 626 4842
UK & Europe: +44 01763 836916
Email: info@d2k.com
www.d2k.com

---

[1] KPMG eFraud report 2000

[2] See d2k technology white paper for more information