

## Customer: Large Broker-Dealer

**Target Application:** Information Security Monitoring / Anti-Money Laundering & Loss Prevention  
**Compliance Applicability:** Securities Exchange Commission / Sarbanes-Oxley

### Overview:

Customer is a large financial services company with a requirement to monitor security, operational, and trading transactions on the network in order to correlate events between each category. The Customer must adhere to compliance guidelines set forth by the SEC and Sarbanes-Oxley regulations. As an added challenge, the Customer has a driving desire to implement a single event monitoring and correlation engine for this analysis, rather than multiple traditional products in silos (SIM, BAM, AML, etc.). By correlating such a large volume of disparate data sources within the SIM system, the Customer is looking to monitor several key patterns in real time, such as those listed below.

- Information Security and IT Control Monitoring
  - Access to critical files (trading models, development code, etc.)
  - Access to databases that house customer-specific information.
  - Privileged-user access to production computer systems (especially during trading hours.)
  - Unauthorized access attempts to multiple computer systems.
- System health / overload monitoring
- Fraud and AML identification and prevention

Long-term storage of the normalized event data is not a requirement for this project, as the source data is already being stored by the individual devices.

### Environment:

The Customer environment contains a large number of devices such as Cisco PIX, Checkpoint, and VPN, ISS Real Secure and Dragon sensors, User Desktop Logs, Custom Application Server logs, RSA SecureID, CA e-Trust and ClearTrust, Antivirus, FTP, Verdasys, SpySweeper, CyberArmour etc. The Customer's server environment is a heterogeneous mix of Windows, Linux, AIX, and Solaris.

### Solution:

The proposed solution for this project is to integrate all security, operational and transaction data into a central SIM platform. Leveraging the extensibility of the SIM product to collect and categorize a broad array of events, the SIM system will correlate and report upon anomalies and suspicious activity for all event categories. In conjunction with this effort, the Customer is building an enterprise event bus for the transport of all events to the SIM or other preliminary aggregation points. Listed below are examples of custom, use-case driven correlation rules and reports that have been designed to meet the Customer's requirements for this project.

### Custom Rules:

- **High Rate of IDS Events** – Monitor IDS events looking for a high number of signatures coming from a single host in a specific time range
- **Internal Port Scanning** - Port scanning where the Target IP is in the Customer's internal network
- **External Port Scanning** - Port scanning from the Customer's internal network to the internet.

- **Database Access Violations** – Users/IP's performing unauthorized database access attempts
- **Network Access Violations** - Non-standard machines accessing the production environment.
- **Account Transaction Monitoring (AML)**
  - Funds are moved from account to account with little or no activity actually occurring and then funds are withdrawn.
  - Funds deposited domestically and transferred or withdrawn internationally.
  - Large number of small deposits being made in short period of time.
- **Account Activity Monitoring (Fraud)**
  - Market manipulation - Open Buy/Sell orders from the same account and/or Buy/Sell during Pre-Session and Extra-Session Trading.
  - Match Trading - user buys or sells at same price or number of shares with no change in beneficial ownership.
  - Spoofing - Small offer to buy a stock at price that splits the Bid/Ask market value which is then revoked after a sell is issued.
  - Fraudulent ACH/Check transfers - Account funded by a fraudulent ACH Transfer/Check where the trades go through immediately.
- **Infrastructure Monitoring**
  - Alerts generated when server CPU goes above 98%.
  - Alerts generated when server memory usage spikes are detected – deviating x times from the average mean in a specific time range.
  - Alerts generated when by web servers when maximum number of connections exceeded.
  - Alerts generated when devices stop reporting events.
- **Business Intelligence Monitoring**
  - Dashboard that tracks daily revenue by multiplying total number of shares executed by average profit per trade.
  - Alerts generated when server memory usage spikes are detected – deviating x times from the average mean in a specific time range.
  - Dashboard tracking various types of trades executed.
  - Dashboard showing daily number of accounts opened/closed.
  - Dashboard showing daily number of ACH executions.
  - Real time offerings based on account activity.

#### Custom Reports:

- **Executive Summary Report** – (High level bar/pie chart)
- **Revenue Generation**
- **User Activity Violations**
- **Capacity Planning**
- **Business Monitoring**
- **All Violations by User ID**
- **All Violations by Source IP / Source Hostname**

#### **Summary:**

The customer's specific requirements for Operational SIM, IT Control, Business Activity and AML monitoring will be met through the implementation of a single, enterprise SIM platform. Upon completion, the Information Security business unit will be able to monitor network infrastructure, user policy violations, and network traffic anomalies. The Customer's AML/Fraud group will track suspicious account transactions, revenue generation, and funds circulation. The Business Intelligence group will monitor account activity and proactively prevent account loss. In addition, the customer will be able to readily demonstrate that they are in compliance with guidelines set by the Securities Exchange Commission through the use of custom audit reports created above.