Decision-Zone
"...from months to milliseconds..."

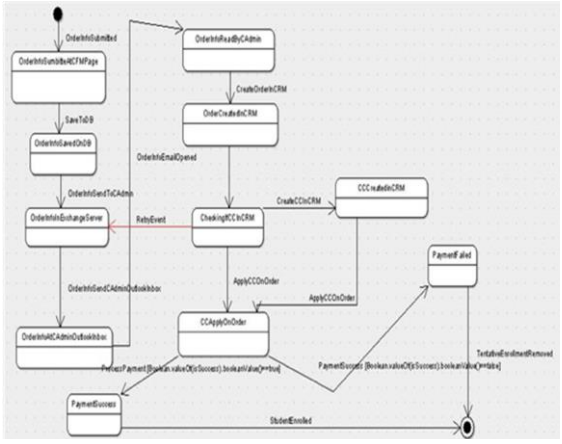
Deep Message Inspection Case Study — Malicious Insider Detected

Historical Investigations

Financial department of an education facility has determined irregularities in their financial statements and is under tremendous pressure to identify the sources of these irregularities. They engaged a reputable data forensics consulting company to work with its IT department to identify the sources of these irregularities. The first step for the consulting company and the IT department was to consolidate terabytes of historical data from many sources, which took over 2 months of effort. In the second step the consulting company subject matter experts performed sophisticated data analytics, lasting over 3 months. The consulting company concurred with the finance department that there were irregularities in the financial statements and *concluded that the sources of these irregularities could be either malware or insiders.*

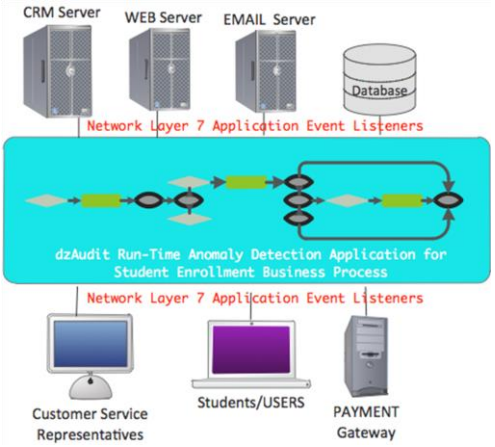
Designing DMI Application

The finance and the IT department engaged Decision-Zone to perform run-time investigations to catch malware or insiders performing non-authorized activities in the act. In the first week Decision-Zone facilitated a workshop working with the client process owners and produced a strawman model of the end-to-end student enrolment business logic. In the second week, DZI facilitated a workshop with the IT department and produced a detailed system event workflow UML map for the student enrolment process.



DMI Application

DZI engineers then created and deployed a run-time deep message inspection app for the student enrolment business logic using the dzAudit platform that listened to system events from multiple sources and checked each event for anomalies against the business logic rules, time and conditions at run-time. dzAudit DMI applications classify output anomalous audit trails into the following categories:



Missing source – in a given process instance a specific activity was not performed.

Timeout – in a given process instance a specific activity or the process instance timed out.

Event Validation Failure – a system event occurred prior to a process instance starting.

No Anomalies – all system events conform to the authorized business process flow.

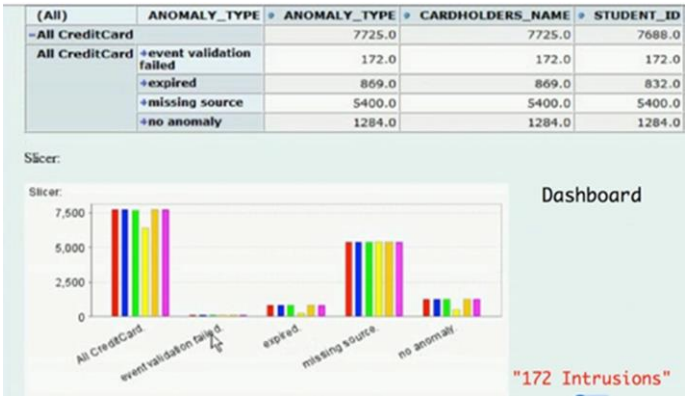
Decision-Zone
"...from months to milliseconds..."

Behavior Anomalies – non-anomalous audit trails are evaluated against adaptive machine learning algorithms for abnormal use of the business process.

SLA Anomalies – specific activity in a process instance that do not meet the service level objectives of the organization.

DMI Output

The student enrollment DMI App was deployed for about a month. The application identified 172 instances of event validation failures, 5400 instances of missing steps, 869 instances of timeouts and 1284 instances with no anomalies.



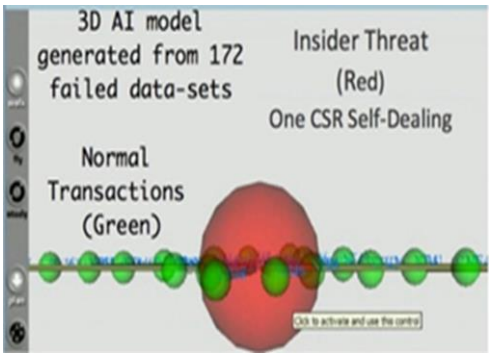
(All)	ANOMALY_TYPE	ANOMALY_TYPE	CARDHOLDERS_NAME	STUDENT_ID
-All CreditCard		7725.0	7725.0	7688.0
All CreditCard	+event validation failed	172.0	172.0	172.0
	+expired	869.0	869.0	832.0
	+missing source	5400.0	5400.0	5400.0
	+no anomaly	1284.0	1284.0	1284.0

dzAudit run-time audit trail results are fed to the dashboard continuously and aggregated into a OLAP database. This allows organizations to visualize the activity in its information assets from many aspects for making informed operational decisions. dzAudit can be integrated to output anomalous audit trails into any commercial dashboards, including Archer, Cognos, Hyperion etc…

Behavior Analysis Identifies Malicious Insider

With the help of DZI, the consulting company and the customer performed behavior analysis on the 172 failed event validation training data sets. Machine learning algorithms were used to perform regression analysis to identify the patterns of causation. An advanced 3D graphical rendering tool was used to visualize the results of the regression analysis.

The visualization revealed that 172 failed event validations were caused by one specific insider. The insider voluntarily resigned when confronted with specific data associated with his/her self-dealing scheme.



With dzAudit, organizations can secure any business process. *The more complex the business process, the more secure organizations become.* With dzAudit complexity is not an issue. However, in a complex distributed environment without dzAudit, enterprises becomes more vulnerable and less secure.