INFORMATICA®
The Data Integration Company™

Informatica RulePoint

The Event Detection and Response Challenge

WHITE PAPER

This edition published March 2010

Table of Contents

Introduction

Situational awareness, cost containment, risk mitigation, and growth: these operational imperatives require timely detection of and response to key business events. Organizations must be able to effectively respond to opportunities and threats represented by events continually occurring across disparate sources of information that relate to their missions. Several key event detection and response capabilities, including detection of complex events as they occur, real-time contextual alerts, end-user managed rules, subscription management, and automated response handling, are all required for an organization to be able to effectively manage business events with minimal impact on existing processes.

Individual events such as a new order, a 911 call, a customer service request, a geographic position update, or an updated investigative report represent the foundation of new and changing data throughout an organization that must be continually monitored to identify opportunities and threats. Individual events, if not already detected by existing business systems, can be quickly harnessed using event detection and response capabilities. Complex events, comprised of related individual events, traditionally go completely undetected by both users and existing systems. These events may have internal and external informational components, and may occur at different times. Following are three real-world examples of normally undetected complex events, along with potential responses.

Example 1: Vessel Tracking

A vessel is entering port in 24 hours. It is carrying cargo, crew, and passengers. The vessel is traveling from a Middle East port, and is registered in Panama. More importantly, the vessel is carrying a passenger whose name matches an individual on a watch list, and one cargo item that looks questionable. The complex event is the occurrence of a vessel that is calculated to be of high risk, based on data derived from the vessel's position, travel history, cargo, and passenger manifest. Effective response would be to alert appropriate watch officers who may request interdiction of the vessel prior to its entry into port so that the crew, passengers, and cargo can be properly inspected.

Example 2: Customer Satisfaction

A salesperson has a meeting scheduled with a key customer in three days. The customer has an order due to arrive the day after the meeting, but it will be late. In addition, product returns from this particular customer have increased, and its customer service calls have become more frequent. The complex event in this scenario is a planned sales meeting that may have higher priority issues than the sales person has planned for discussion. Upon receiving an alert about this complex event, effective response would be for the software system to research the cause of the increased returns and customer service calls, to determine the cause of the late order arrival, and to seek prospective resolutions prior to the meeting. These topics can then be addressed proactively during the sales meeting.

Example 3: Interaction Tracking & Analysis

An analyst is utilizing a link analysis tool to track interactions between individuals and organizations within a particular social network. Interactions such as communications, meetings, and transactions form the basis for analysis and assist in identifying additional associative links. Separately, a case file system is updated with a new report that discusses individuals that the analyst has recently added to a chart within her link analysis tool. The complex event is the detection of entities of interest in the analyst's link chart that match data repositories (e.g., the case file system) to which she might not otherwise have the time to check for updates, let alone run hundreds of queries daily against, each query representing a particular individual or organization of interest displayed in her chart. Effective response in this situation is to alert the analyst that new information has been detected about key individuals or organizations that she is tracking. This complex event alert dramatically improves her situational awareness and perhaps results in the definition of additional linkages.

Complex events like the examples above are not typically detected in a timely manner today. The high-threat vessel may proceed directly to port, the salesperson would go to the meeting unprepared, and the analyst would be unaware of critical data that ties to individuals that she is tracking.

This paper discusses the Event Detection and Response capabilities needed to address the challenges presented in the above examples. Included is a discussion of critical business requirements necessary to deliver an effective event detection and response system as well as specific solution examples.

Effective Event Detection & Response

An effective event detection and response solution must have several key attributes. The first of these attributes is the automatic rules-driven detection of complex business events in near-real time, from any information source, without compromising security or data integrity. The second attribute is the correlation of current and historical information sources, sensors, as well as internal and external data feeds. The ability to extend knowledge about detected events to discover additional facts for in-depth correlation is necessary to ensure a complete picture of event details prior to triggering an alert or a process. Finally, responses to detected events must be targeted, specific, and automatic. Appropriate responses include delivering information-rich alerts to appropriate subscribers, automatically triggering business processes, and kicking off existing analytic tools.

A graphical interface for creating and modifying event detection and correlation rule sets is necessary for defining information sources, analytic rules, and relevant response actions. This interface must be usable by business users and domain experts, and not require systems development personnel for changes and additions to business rules. In addition, end-user management facilities must be available to allow users to define personalized domain-specific rules for monitoring and alerting.

A robust complex event processing (CEP) engine must serve as the core for detecting and responding to events, and it must be capable of using detection and correlation rule sets in real time as they are defined. As events are asynchronous in nature, the CEP engine must operate through the use of server-based processes generated from rule set definitions. CEP allows for correlation of people, locations, things, time, and actions, and provides for detection of interrelated informational events.

In addition, Event Detection and Response servers must be deployed without change to existing systems and processes, without duplication of sensitive data, and without compromising information security.

Event Detection & Response With Informatica

Informatica's event detection and response software products provide the capabilities mentioned above, and serve as the platform for developing and deploying enterprise-class event detection and response solutions. Informatica's products provide an enterprise event service, delivering proven Event-Driven Architecture (EDA) capabilities within a Service-Oriented Architecture (SOA) framework.

At the core of Informatica's event detection and response products is RulePoint. RulePoint is a sophisticated Java-based software product that acts as an enterprise event service, intelligently detecting complex business events as they occur, and automatically initiating responses as required. RulePoint detects complex events across disparate information sources including sensors, EAI, enterprise applications, databases, text documents, and more. Events are automatically detected through execution of user-defined rules, configured via easy-to-use web interfaces and wizards. Rules may leverage over-time correlation, geospatial analysis, automatic cross-referencing against external sources, and more, in order to identify events of interest. Relevant actions, such as process initiation and alerts, are triggered in real time. Any automated action can be initiated, including e-mail and instant message alerts; web service and business process activation; browser alerts through Informatica's Real-Time Alert Manager™, a web-based application for managing alerts received from RulePoint; and instant GIS/link analysis tool updates.

Integration of Any Information Source

All sources of electronic information are supported for detection of complex events. Information can be internal or external, and centralized or distributed. Sources can include traditional databases, sensors, EAI, e-mail, communications streams, message handling systems, Web Services, Lotus Notes, search engines, RSS news feeds, web pages, and more. Information sources can be monitored without duplication of data.

Individual and Complex Event Detection

The ability to detect and respond to individual and complex business events as they occur is a core business competency that drives operational agility. Detected individual events, correlated using analytic rules defined by domain experts, drive identification and subsequent handling of complex events.

Information-Rich Real-Time Alerts

Information-rich and actionable alerts are delivered to appropriate subscribers through instant messaging, email, Real-Time Alert Manager, or custom channels. Alerts are delivered based on detected events in accordance with a user's rules. Users with appropriate permissions may subscribe to receive alerts based on events detected via another user's rule sets. Robust filtering capabilities are also available to prevent alert message overload. Alerts also provide access to detailed information upon which the detected event was based, in addition to actionable links that offer drill down access to additional data and visualization through third-party geospatial and link analysis tools.

Intelligent Business Process Initiation

In addition to alerting people and teams, action can be taken by triggering existing business and system processes. Actions can include triggering Web Services, activating workflow processes, initiating transactions, updating management dashboards/portals, adding database records, and modifying security parameters such as system and physical access rights or network configurations.

Shared Expertise

Rule sets created by domain experts can be easily shared with other users that have appropriate permissions. Shared rule sets serve as a force multiplier, allowing authorized users to work at a level approaching that of domain experts. For example, an analyst may configure a highly filtered rule set to send alerts when new data retrieved from five specific RSS feeds is about any one of twenty related individuals. Another analyst, instead of having to write the same rule to look for those same twenty individuals, can simply create a subscription to the first analyst's rule. In general, complex event processing rules are entered and maintained through easy-to-use graphical user interfaces, and are only accessible to authorized end users. Rules can be configured to detect events using Boolean logic, pattern matching, geospatial analysis (e.g., bounding box), over-time correlation, threshold/statistical evaluations, non-event exception detection, and more. Rules can also leverage 3rd party analysis tools in near-real time such as entity extraction, categorization, and other natural language processing systems.

Knowledge Extension

When an event is first detected, RulePoint has just begun to deliver value. Knowledge of a detected event can be extended in real time through correlation of known people, locations, phone numbers, e-mail addresses, things, time, and other available event data. Knowledge extension is accomplished by initiating automated queries focused on the event's details against available data sources. Knowledge extension enables additional events to be discovered, resulting in highly contextual alerts, and allowing actions to be initiated from a more informed position.

Responsiveness to Change

Rules can be updated in real time as business environments change and as organizations discover new information. RulePoint's ability to be dynamically updated facilitates on-the-fly adaptation to critical situations, organizational learning, and business agility. As organizations learn, users can add new knowledge to the rules base immediately, and changes may be shared immediately with end users who have appropriate access to the system.

End-User Driven

End users share rule sets where authorized, and maintain individual profiles through web-based interfaces. These profiles contain domain-specific rules for targeted monitoring, correlation, alerting, and response management. For example, facilities are available that allow users to quickly point and click on information topics to identify what items they'd like to receive alerts on. Users are also able to rapidly define event detection rules and identify the appropriate event responses that should take place, such as updating a portal, sending an instant message, or triggering a workflow process.

Seamless Integration and Industry Standards

Standards-based interfaces allow RulePoint to integrate seamlessly with business processes, process-driven applications, and any information source. In addition, RulePoint requires no change to existing business processes and applications.

Informatica products are Java-based and leverage standards including JDBC, Web Services, JMS, EJB, RMI, HTTP/S, POP3, SMTP, IMAP, FTP, and XML.

Power and Scalability

Informatica's RulePoint can be deployed for large and small applications. Deployments can be centralized or distributed, and connected information sources can also be centrally located or distributed. Operational environments include Solaris, Linux, and Microsoft Windows.

Security

RulePoint leverages existing security infrastructure for access, authentication, and authorization. The server allows events to be managed securely by role, while maintaining the integrity of existing information security.

[1] Austvold, Eric, Karen Carter. "Service-Oriented Architecture: Survey Findings on Deployment and Plans for the Future." AMR Research Market Analytix Report: Market Trends Series. 2005. p. 7
[2] Ibid. p. 2
[3] Ibid. p. 14

Event Detection & Response Solutions

Event detection and response solutions support a wide range of missions including law enforcement, financial services, and national security. Solution examples are provided below.

Law Enforcement – Investigative Automation

The Informatica event detection and response solution for investigative automation supports real-time crime centers, investigators, and command centers for incident response, coordination of resource allocations, and management of related investigations across organizational boundaries. Incident reports, 911 calls, patrol officer and walk-in reports are monitored and correlated for commonalities. Correlated information, along with investigative reports and applicable information from other jurisdictions and agencies, is simultaneously utilized to detect critical events and to initiate contextual alerts and effective response. Event detection and response solutions serve as a force multiplier, as rules created by domain experts can be shared and subscribed to by authorized departmental personnel, resulting in improved situational awareness.

For investigative teams, RulePoint for law enforcement detects related investigative information by monitoring existing reporting processes and systems. Correlation is performed among people, locations, things, time, and actions to detect related investigative information. Collaboration is then initiated between investigative teams by alerting all relevant parties when commonalities are detected. Alerts happen in real time as investigative information is entered or updated.

An example process flow for this solution begins with an investigative report being entered through an existing system and process. RulePoint detects the entry based on a user-defined rule, initiates extraction of entities using 3rd party tools if required, and compares the report with past reports, watch lists, MO libraries, and other relevant databases. Information-rich alerts are forwarded to relevant parties with detected correlations. Drill down to the specific information and reports that generated the alerts is available through all notification channels. Alerts are also used to initiate collaboration between investigators and teams.

Battlespace Command & Control

Informatica's event detection and response solution for battlespace command and control allows for fusion of sensor and tracking system information from radio frequency (RF) sources, sensor data, radar contacts, message traffic, and force deployments for situational awareness and targeting. One example of this capability is in the area of radio frequency source monitoring, where disparate sensors are monitored to detect tactical RF events. As new RF data is received, threat assessment rules are automatically initiated to determine if alerts are required by analyzing and comparing frequency, type, location, and other characteristics.

While RF monitoring is occurring, battlefield information, including force deployment positions, is continuously compared to RF source events to determine threat level and available response options. GIS visualization is utilized, along with instant messaging, to deliver actionable alerts. Commanders may create their own personal rules to receive alerts based on threats or target opportunities near their current location based on target attributes as well as on many other criteria.

Link Analysis Event Management and Collaboration

The Informatica event detection and response solution for link analysis event management automatically alerts analysts when changes occur to data within existing link analysis tools, without requiring manual checking for changes to entities and linkages of interest. Alerts are delivered when new linkages are created that match other data available within existing case management systems, search engines, and databases. For example, an analyst may receive alerts when another member of her workgroup creates a linkage between an entity that she's tracking and someone previously unknown: "You requested to receive alerts when any new links occur associated with John Smith. A new link has been created between John Smith and a new individual Sara Doe. There are 10 reports about Sara Doe in the case management system."

The process flow for this solution begins with new entities and linkages being entered into a link analysis tool by an analyst as a part of a normal routine. As data is entered, the Informatica solution detects new entries, initiates correlation against other available data sources, and determines if any analyst has configured rules to receive alerts related to the new information. An analyst may have requested alerts related to any new data, or only specific alerts if the new data is about particular individuals, organizations, or other entities. Information-rich alerts are sent through instant messaging, e-mail, or persistent Web page through the Real-Time Alert Manager, to relevant parties for detected linkages and correlations. Drill-down capability is available through all methods of alerting to view specific linkages and correlated reports.

Multi-Source Monitoring for Analytic Centers

Informatica's event detection and response products have been delivering solutions to national security organizations for many years. RulePoint™ provides complex event processing capabilities to address the challenging tasks inherent to threat detection and risk assessment, infrastructure protection, information sharing, crisis management, border control, and intelligence analysis. Event detection and response solutions for analytic centers monitor streams of information from disparate sources, correlate information extracted from these data streams with historical data based on user and organization-defined rules, and deliver alerts in real time for detected items of interest. From centralized, easy-to-use web-based interfaces, users can configure personalized event detection rules, as well as subscriptions to organizationally shared rules that simultaneously leverage many sources including sensors, RSS feeds, search engines, Web Services, databases, custom message handling systems, and more. Event data across many systems is simultaneously processed, filtered, and prioritized, delivering users only actionable data with as little redundancy as possible. Informatica's multi-source monitoring solution for analytic centers not only saves users significant time by automatically watching multiple sources that would otherwise each require extremely tedious manual checking, but also assists with information discovery by identifying correlations and matches among systems that would otherwise be accessed in completely separate ways. Monitoring of information sources and alert delivery is accomplished without compromising source data security, supporting mission needs while maintaining role-based access controls.

National Security – Geospatial Tracking

Informatica event detection and response solutions for geospatial tracking allow analysts, operators, investigators, and threat centers to detect key geospatial threat events from internal and external information sources. Detected threats and risks trigger real-time alerts to relevant parties as new information is correlated by RulePoint, or as new and updated rules within RulePoint are analyzed against existing information.

For example, Informatica's geospatial tracking solution is used to monitor high-risk vessels before they enter ports, or as they pass through shipping areas that are predetermined to be high-risk locations. The process flow for this solution begins with a vessel being detected through an existing sensor network. RulePoint passively listens to messages from a sensor network, continually monitoring for ships that fall within areas of interest as defined by geographic boundary rules created by analysts. When ships are found within particular boundaries, threat assessment is initiated by correlating vessel attributes, cargo manifests, crew and passenger lists, ports of call, watch lists, and more. Information-rich alerts are forwarded to relevant parties via instant messaging, e-mail, or Real-Time Alert Manager when high-risk vessels are detected. GIS visualization is initiated for high-priority vessels. Drill down to the specific information and reports that generated alerts is available through all methods of notification. Alerts also trigger deployment of resources to deal with the detected potential threat.

Business Operations – Phishing and Identity Theft

Informatica's phishing attack management solution delivers phishing attack investigative and adjudicative support for banks, credit unions, online brokerages, and e-commerce companies. This solution enables organizations to efficiently respond to varied phishing attacks by automatically sorting, filtering, prioritizing, and correlating e-mail attack data. In near-real time, the phishing attack management solution processes phishing e-mails relayed by customers, advisory alerts from 3rd party organizations, and phishing emails retrieved proactively via other sources. As new phishing e-mails are fed through Informatica's phishing attack management system, automatic discovery of attack details is initiated to capture relevant data for later search and retrieval, and to deliver information-rich alerts to investigators based on critical trends. The solution's automated discovery process includes running WHOIS queries (host ISP, registered domain owner), network traces (tracert), screenshot captures, and more. Attacks are grouped together based on correlated details and matched to advisories provided by 3rd party services where applicable. Captured attack information serves as the basis for automated correlation, trend identification, management tracking, and evidentiary documentation. This solution allows investigators to focus their time investigating and adjudicating instead of manually researching the details of each attack.

Learn More

Learn more about the Informatica Platform. Visit us at www.informatica.com or call +1 650-385-5000 (1-800-653-3871 in the U.S.).

About Informatica

Informatica Corporation (NASDAQ: INFA) is the world's number one independent leader in data integration software. The Informatica Platform provides organizations with a comprehensive, unified, open, and economical approach to lower IT costs and gain competitive advantage from their information assets. Nearly 4,000 enterprises worldwide rely on Informatica to access, integrate, and trust their information assets held in the traditional enterprise and in the Internet cloud. Visit www.informatica.com.

INFORMATICA®

Worldwide Headquarters, 100 Cardinal Way, Redwood City, CA 94063, USA
phone: 650.385.5000 fax: 650.385.5500 toll-free in the US: 1.800.653.3871 www.informatica.com

Informatica Offices Around The Globe: Australia · Belgium · Canada · China · France · Germany · Japan · Korea · the Netherlands · Singapore · Switzerland · United Kingdom · USA

7107 (03/11/2010)