SOLUTION BRIEF

sgi®
INNOVATION
FOR RESULTS℠

SGI® COMPLEX EVENT PROCESSING SOLUTION

SGI® Complex Event Processing (CEP) Solution

High Performance Continuos Analysis

SGI Protects the warfighter with this Mission Critical Capability

- Persistent analysis of massive amounts of disparate data, real-time events, and data correlation providing real-time alerting
- Continuous exploitation, analysis and detection of critical events
- Rapid and continuous correlation of otherwise disparate data and disparate events
- In-stream detection and alerting when event of interest occur
- Early warning as rules continuously analyze event streams for known indicators and then issue alerts
- Creation of both a detection and workflow environment for system to system-level interactions
- Complimentary to other solutions such as High-Speed Ingest processor, One-way Guard technologies, Rapid Shape Detection, and Full Motion Video management systems
- Increased overall situational awareness and display of a more accurate Common Operational Picture (COP) when deployed in a Network Operations Center (NOC), or Command and Control Center (C2)

Never is the expression “information is power” more applicable than in the case of National Security. To do its job effectively, the Intelligence Community must be able to get information, process it, analyze it, exploit it and share it.

SGI Complex Event Processing (CEP) monitors disparate data sources and rapidly identifies relationships between previously unconnected data, flagging anomalous behavior or events that bear scrutiny as a possible threat to national security and triggering an alert to appropriate systems or personnel.

The system monitors databases, real-time feeds, streams of data across socket connections, JMS queues, RSS feeds, message busses, Web-based streams of email and instant messaging. A correlation engine provides actual event detection in near real-time that sends data to a flexible alerting mechanism.

Uncovering the Information

Threatening events could go undetected if relationships between data elements are not identified. Manually gathering data from multiple servers and databases that may reside across diverse security domains in various formats can result in costly delays or missed information. SGI CEP solves those problems by delivering automated data gathering and analysis across heterogeneous, high velocity data environments to provide unprecedented visibility into information about people, infrastructures, communications, facilities, military and commercial vehicle movement and communication networks. The result is reduced decision and reaction cycle times, with users no longer having to sift through massive amounts of data analysis.

Processing and Analyzing the Information

SGI CEP allows users to create simple "custom rules" that run across all entitled data sources and real-time tactical feeds. The SGI CEP appliance is able to run millions of transactions per second. Complex intelligence events are automatically detected through the application of these user-defined rules, which are easy to build through a wizard process or via a parameterized template that can be deployed across the enterprise. New information such as tips and hunches can also be rapidly correlated against existing data.

SGI CEP analyzes concepts such as event hierarchies, priority, causality and relationships between events based on both temporal and spatial factors. Imagery from GIS data, for example, can be monitored and gathered from sensors, databases and systems, then analyzed against user-defined criteria and geographic areas of interest and correlated temporally against other data sources. The system also supports internal and external analytics for special use scenarios.

Sharing the Information

When content of interest is detected, SGI CEP generates a user alert to the users in the field across multiple networks, including email, SMS or Web-based alerting to portal interfaces and applications. SGI CEP automatically interacts with other downstream targeting or tasking systems. Relevant alerts can support two-way connectivity to databases for updates and set off alerts into situational awareness displays such as existing Geospatial tools, i.e. Google Earth™, ESRI™, etc.

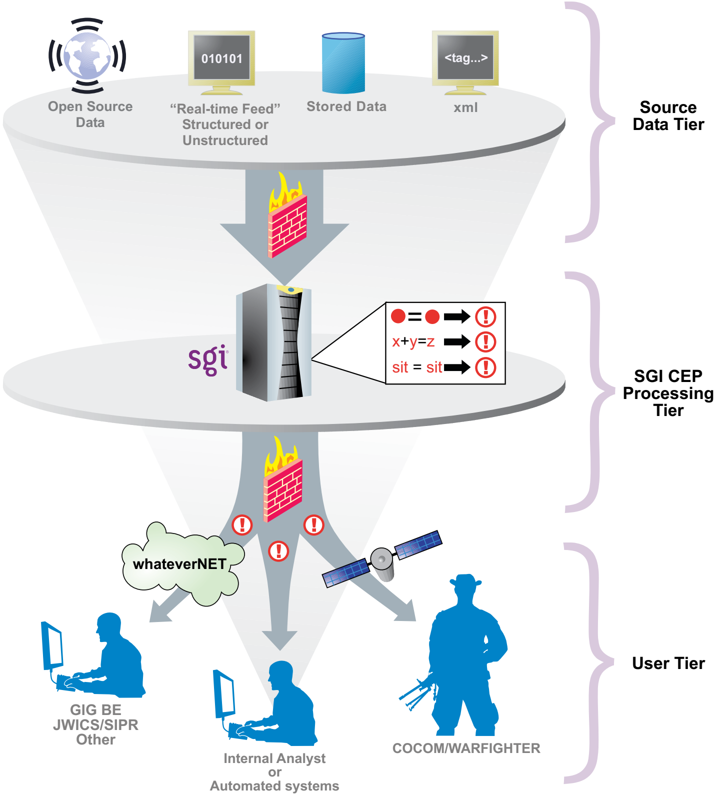
SGI CEP can also issue IM chat alerts or pass data to link analysis applications like i2 Analyst's Notebook or provide system to system alerts like automated targeting and tasking systems.

Easy to Deploy

SGI CEP is non-invasive and integrates with existing data sources. The solution offers out-of-the box connectors for many types of real-time feeds as well as traditional data sources like databases or image repositories. When necessary, SGI can also create customized connectors.

SGI recognizes that detecting and predicting threat events are priorities in the Federal Government. Its CEP solution provides persistent analysis by helping to detect, real-time events related to adversaries, targets and threats.

SGI Complex Event Processing



High Performance Continuous Analysis

sgi®

Corporate Office
1140 E. Arques Avenue
Sunnyvale, CA 94085
(650) 960-1980
www.sgi.com

North America +1 800.800.7441
Latin America +55 11.5185.2860
Europe +44 118.912.7500
Japan +81 3.5488.1811
Asia Pacific +61 2.9448.1463