



Security Intelligence

Essential Decision Support

for Security, Risk Management, and Compliance Operations

February 2010

Executive Summary

The digital infrastructure used today by businesses and governments is more sophisticated and critical than ever before. It is also under unprecedented attack both from the outside world and from inside the organization. There has been a dramatic increase in cybercrime, and stories detailing large-scale identity theft and other data disasters are making headlines daily. These attacks are costing organizations billions of dollars a year through interrupted operations, data loss, lawsuits, and damage to customer confidence. According to one study, \$1 trillion in intellectual property was stolen online in 2008.¹

The problem is intensifying as cyber-attacks have become much more sophisticated and malicious. Threats are now coming not only from solo hackers, but from a new breed of cybercriminals who are using innovative combinations of hacking, phishing, social engineering, and botnet schemes to make money. Brian Grow, cybercrime reporter for *BusinessWeek* magazine considers cybercrime “the fastest growing crime in America and in the world.”²

Organizations today face huge challenges in preventing and defusing these threats. Thus the need for protection against cybercrime is greater than ever, especially considering the volume of personally identifiable information (PII) and financial transactions that corporations and financial institutions manage daily—information that is specifically targeted by cybercriminals, organized crime rings, and potentially foreign governments as well.

The threat is also increasing from inside the organization. Disgruntled or displaced employees can exploit inside access and conduct malicious attacks, either for personal gain or to damage the organization’s information networks. In a 2009 survey conducted by the Computer Security Institute (CSI), 42 percent of respondents reported experiencing losses attributed to malicious insiders.³ According to a study from McAfee and Purdue University, malicious insider attacks appear to be growing. This study also suggested that the economic downturn is further increasing the security risk; 42 percent of respondents reported that displaced workers were the biggest threat to sensitive information on their networks.⁴

Nonmalicious insiders—average well-meaning users who disclose data unwarily—pose an even greater insider threat. In the CSI study, 66 percent of respondents reported losses attributed to nonmalicious insiders. In addition, 41 percent of those respondents felt that either the majority of or *all* of their financial losses were attributable to non-malicious actions by insiders.⁵

Compounding the problem is the fact that the volume of event data managed by organizations is doubling every year. Regulatory agencies and business imperatives now require that organizations capture and retain multiple years’ worth of data, not just for regulatory compliance

¹ – “Google and China: the new era of cybercrime,” Editorial Board, January 26, 2010, Christian Science Monitor: <http://www.csmonitor.com/Commentary/the-monitors-view/2010/0126/Google-and-China-the-new-era-of-cybercrime>

² – “Media Challenged by Changing Nature of Cybercrime,” Jane Applegate, WEIS 2008 (Workshop on the Economics of Information Security): mba.tuck.dartmouth.edu/digital/Programs/.../WEIS_media.pdf

³ –CSI (Computer Security Institute) Computer Crime and Security Survey 2008 Executive Summary, p.12: <http://www.gocsi.com/2009survey/>

⁴ – “Laid Off Employees Turning to Cybercrime,” Lidija Davis, February 1, 2009, ReadWriteWeb website: http://www.readriteweb.com/archives/laid_off_employees_turning_to.php

⁵ – CSI (Computer Security Institute) Computer Crime and Security Survey 2008 Executive Summary, p.12: <http://www.gocsi.com/2009survey/>

but also for fraud detection, forensics and investigations, law enforcement and security agency requests, and operations troubleshooting.

Organizations have lacked the necessary framework to manage this huge volume of data and derive knowledge from it to improve related operations. Preventing and minimizing cyber-attacks requires the precise analysis of multiple, complex data sources in real time and over long time frames. Much, if not most, of this data is event data, which is produced from virtually every form of information technology. Expanding regulatory compliance requirements and audit challenges make it even more essential for organizations to know what all their data and computing assets are, where they are, who has access to them, when they are accessed, and how they are secured.

There is a critical lack of database, knowledge management, and business intelligence applications to help organizations gain this knowledge. Professionals and public servants in the field of digital security are doing their best to safeguard digital assets and institutional reputations. But they need better tools, and they need them now. When asked what solutions are most needed, CSI survey respondents cited better log management, security information and event management, security data visualization, and security dashboards. They also want these tools to be thoroughly interoperable and able to show what was happening in an organization's entire environment, not just on a few devices.⁶

The many point products currently being used to manage event data have proven inadequate:

- Traditional data warehouses lack a security context and struggle with the unstructured nature of event data.
- Traditional security information and event management (SIEM) systems do not scale to support the sheer volume and long-term storage requirements of an event data warehouse.
- Traditional log management systems lack the real-time monitoring functionality necessary to keep pace with critical operations such as security incident response.
- Both SIEM and log management systems lack the sophisticated analytics necessary to detect and investigate state-of-the-art cyber-threats.

It is quite clear that a new approach is required, one that leverages the power of scalable data warehousing and flexible information analytics but in the context of security management. Just as Business Intelligence solutions leveraged data warehouses to facilitate decision support for business management, now Security Intelligence solutions must leverage the power of event data warehouses to facilitate decision support for security management.

SenSage[®] is at the forefront of this new technology, offering the world's only Security Intelligence solutions specifically developed to address the essential decision support requirements of security, risk management, and compliance operations. Based on patented, proprietary technology, SenSage solutions provide organizations with a scalable means to centrally aggregate, efficiently analyze, and dynamically monitor massive volumes of data. In addition, SenSage solutions substantially reduce the cost of deployment and ongoing management associated with IT monitoring, investigation, and compliance. Over 450 organizations and government agencies worldwide are currently using SenSage solutions to safeguard their data in today's cyber-threatened environment.

⁶ – CSI Computer Crime and Security Survey 2008 Executive Summary, p.1

Event Data: the Challenge and the Opportunity

Virtually every form of information technology produces event data. Sometimes referred to as log data, audit trails or the system of record, event data is a set of chronologically sequenced data records that capture information about what happens in the digital infrastructure.

Event data differs in many ways from transactional data that is stored in traditional data warehouses:

- Cumulative volume – Event data accumulates rapidly and often must be stored for years; many organizations are managing hundreds of terabytes and some are managing petabytes.
- Format – Because of the huge variety of sources, event data is unstructured and semistructured.
- Collection – Event data is difficult to collect because of broadly dispersed systems and networks.
- Time-stamped – Event data is always inserted once with a time-stamp and never changes.

Event data sources include:

- Network and security devices
- Physical access systems
- Identity management systems
- Workstations, servers, and operating systems
- Database activity
- Enterprise applications, including shrink-wrapped, customized, and homegrown
- Banking transactions such as online, ATM, and debit card use
- Historical prices of stocks and other instruments
- Telco call detail records (CDRs)
- Internet protocol detail records (IPDRs) of web-based access and transactions
- Updates to shipping status in RFID records
- Email, Windows, network, and other systems management activity events
- Manufacturing sensor data

When this data is captured and analyzed broadly (across all relevant technologies), deeply (to convey sufficient detail about what happened) and over a long time horizon (to isolate real-time incidents as well as long-term trends), it provides tremendous perspective on security operations.

Driven by changes in security threats, compliance mandates, and risk management initiatives, organizations are collecting event data from more sources and storing it longer, and they have been trying to piece together systems to enable them to analyze this data more deeply, more broadly, and more frequently.

Security Intelligence solutions deliver the profound benefit of managing vast amounts of security and business event data while comprehending what it means. Over 450 organizations and government agencies worldwide have solved major event data warehousing problems by employing Security Intelligence solutions from SenSage.

Here are five examples of how different organizations have leveraged SenSage Security Intelligence solutions to address their critical security, risk management, and compliance requirements:

- A large U.S. government agency consolidated its SIEM and log management operations to better protect customer data through real-time alerting, forensic investigation, long-term event data analysis, and FISMA compliance reporting. This project required scaling to support 1,000 Microsoft Windows servers, custom dashboards, out-of-the-box compliance reports, and flexible query capabilities.
- A large European country's national health service consolidated SIEM and log management services for clinical and nonclinical data for over 77 million patients. Key criteria included advanced threat detection, correlation, forensic analysis across vast amounts of critical data including electronically protected health information (ePHI), and extensive role-based access and controls required by mandates to separate clinical and nonclinical data.
- A large U.S. government agency focused its log management effort on insider threat detection and then expanded it to include SIEM to enable both real-time and historical analytics for individual analysts.
- A large U.S. government defense agency complemented its existing Cisco SIEM solution (MARS) with support for heterogeneous event data coming from multiple sources, comprehensive security monitoring, and long-term analysis to improve its insider threat detection and analytics capability.
- A large European national telecommunications company implemented a corporate-wide cyber-security and log management solution for law enforcement, internal fraud detection, and internal security monitoring. This system collects and correlates log data from over 180 sources, including 1.5 billion call detail records (CDR) per day, to enable more immediate and expansive cyber-threat detection and response. Other key requirements included flexible and precise querying and correlation capabilities and the ability to support a virtualized (private cloud) implementation to reduce operating and capital expenses.

These examples reflect the growing trend towards a more holistic approach to security, risk management, and regulatory compliance operations. By providing expanded scope and visibility into the organization's entire IT and data environment, combined with powerful analytics and reporting capabilities, SenSage solutions are uniquely able to deliver Security Intelligence to these operations, just as Business Intelligence has delivered essential decision support to business operations over the last two decades.

SenSage Security Intelligence Solution Architecture

All SenSage Security Intelligence solutions have three primary components: the Interactive Analytics, the underlying Event Data Warehouse, and the Administration Console. These SenSage components can be deployed in the form of software, hardware appliance, and/or virtual machine, and each may support a variety of storage technologies including on-board storage, storage area network (SAN), network attached storage (NAS), and content addressable storage (CAS). Together, these SenSage and third-party components comprise a Security Intelligence solution (see Figure 1).

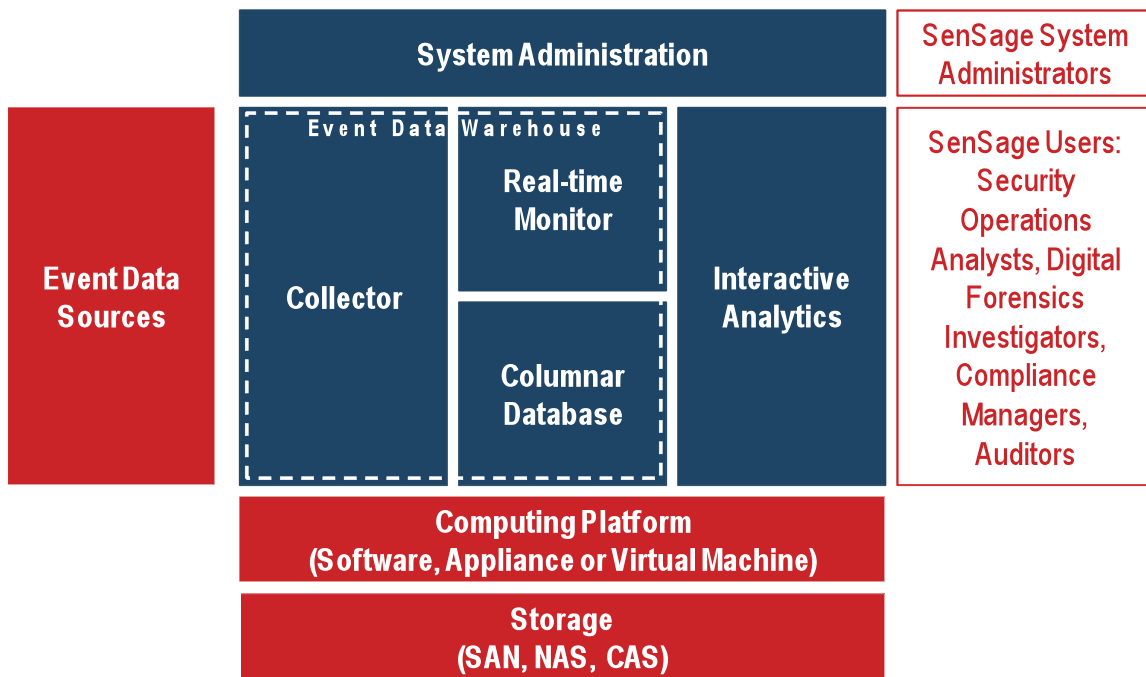


Figure 1. SenSage Security Intelligence Solution Architecture.

Interactive Analytics

The Interactive Analytics component is an analytics environment that can be completely customized. It performs three operations: real-time monitoring, contextual investigation, and reporting. Real-time monitoring is done using supplied and customized dashboards tailored to the specific Security Intelligence solution. For example, the SenSage Continuous Monitoring and Auditing for ERP product includes supplied analytics for fraud monitoring in the order-to-cash process (among many others) that can be edited or supplemented with custom analytics and dashboards built by the customer or by SenSage Professional Services.

Contextual investigation is enabled by a query wizard embedded with all of the organization’s collected event data elements or accessed through contextual links from any dashboard, report, or prior query result.

The reporting capability includes supplied reports, ad hoc reporting, and compliance reporting. Supplied reports are available for many of the popular SenSage uses (e.g., SAP Monitoring and

Auditing, Database Activity Monitoring, Windows). Ad hoc reporting is aided by a report-generating wizard and allows a range of formatting options for any custom query. Compliance reporting formats the event data and associated summaries into specific regulatory compliance formats such as ISO 17799, PCI, HIPAA, Sarbanes Oxley, FISMA, DCID/3, and NIPSOM.

System wizards enable nontechnical users to create new reports, dashboards, and ad hoc queries in seconds using a drag-and-drop interface. Exact-match querying across any data column enables the user easily to create data aggregation, trending, business, and technical reports through bar, line, and tabular charts. Unlike solutions that use “Google-style” searches, only exact matches are returned.

Technical users can use underlying SQL code to further fine-tune reports and queries. SenSage IntelliSchema provides cross-source and cross-vendor reporting capabilities, and new data sources can be easily added with no SQL changes. IntelliSchema was designed to give customers the ability to expand their solution capabilities on the fly, adding new sources, new reports, and analyses without changing their data schema. IntelliSchema easily incorporates custom data sources in both the collection and reporting processes. Organizations can adapt to new threats and new regulations without major upgrades or service engagements, and there is no need to involve DBAs.

Event Data Warehouse

The SenSage Event Data Warehouse comprises a collector, real-time monitor, and columnar database. The collector performs the externally facing data acquisition functions typically referred to as “extract, transform, load (ETL)” in the data warehouse sector. The extract step is performed by SenSage log adapters, which operate in an agentless mode so that agents need not be deployed on or near the event data source. These log adapters obtain and parse data from over 250 event data sources through a variety of protocols including but not limited to Syslog, Syslog NG, SNMP, FTP, SFTP, SCP, SMB, RPC, SQL*Net/RDBMS, HTTP(S) GET, and PUSH. Customization is easy, and many customers develop their own log adapters. Depending upon the event data source and deployment preferences, SenSage log adapters may operate in streaming or scheduled-batch mode.

The transform and load steps involve two different processes to support the multiple operations modes noted above. As each new event data set arrives through the log adapters, one copy is delivered to the real-time monitor for dynamic parsing, normalization, filtering, analysis, and alerting. A second copy is delivered to the columnar database for tamper-resistant storage in its native/raw format. This unique data forking approach bridges real-time and historic analysis while maintaining the complete event log for forensic evidence. Further, this approach supports instant replay visualization; events may be replayed graphically to review their sequence and interdependency.

The real-time monitor is a highly scalable correlation engine that supports threshold- and scenario-based rules built from logical operations on event data and displayed in dashboards in the Interactive Analytics. The sophisticated scenario based real-time correlation engine leverages a state machine paradigm to correlate events from multiple sources over a sliding time-window. This methodology enables real-time threat detection that goes beyond attack pattern recognition and enables analysis of true threat behavior. Furthermore, the SenSage real-time correlation engine is fully integrated with SenSage historical event analysis. As such, it allows the operator to easily look for historical occurrences of similar events to fine-tune future real-time correlation effectiveness resulting in a virtuous cycle of better security. The real-time engine is scalable and may be distributed across multiple processes (and nodes) for large deployments.

The SenSage Columnar Database incorporates patented technology optimized for event data warehousing applications. Unlike traditional relational database management systems that use a row format, data is organized by column in a single, centralized data repository. While the difference may sound minor, the performance gains are dramatic. Indexes are unnecessary in this configuration, thus reducing storage and maintenance requirements. Data is compressed at a 10:1 advantage over relational databases (and up to 40:1 in practice when you consider the average number of indexes needed by traditional row-wise databases) and is stored in a time-based hierarchical series of folders and flat files. Alternatively, data may reside on a shared storage device such as a SAN, NAS or CAS.

The SenSage Columnar Database supports third-party business intelligence tools through an ODBC/JDBC interface. This enables users to leverage familiar tools and standard SQL to query and report on the event data.

The Event Data Warehouse features a massively parallel processing architecture that scales up or down depending on the number of nodes present in the system. This parallel architecture enables record insertion rates of hundreds of thousands of records per second. Moreover, each node in the parallel architecture may take advantage of advanced hardware features such as multicore processors and faster disk drives, and mixed environments may be configured to leverage nodes of varying power. To maintain constant availability, backup copies of each node's data are stored on another node for data redundancy and automatic failover.

Administration Console

GUI-based administrative screens enable easy management of users, privileges, schedules, and reports. SenSage Security Intelligence solutions offer robust and secure authentication, administration, and access control with multiple security levels down to a highly granular degree of control. Authorized users are assigned roles with specific permissions that determine which features, functions, reports, and data each user may access. Role-based filters support granular permissions where users only see data with specific values (i.e., users only see data related to systems they own). Users can install SenSage clients in any geographic location, and the connection between client and server is secure and encrypted.

A Real-world Example: Leveraging Security Intelligence to Stop Insider Threats and Data Leaks

The following example shows how a SenSage Security Intelligence solution was used to detect previously unnoticed evidence of unauthorized access of critical customer data by an internal user.

On the SenSage Security Alerts Dashboard a real-time correlation rule fires, alerting the analyst to the fact that someone has created a user account and deleted it within a one-hour time frame (see Figure 2).

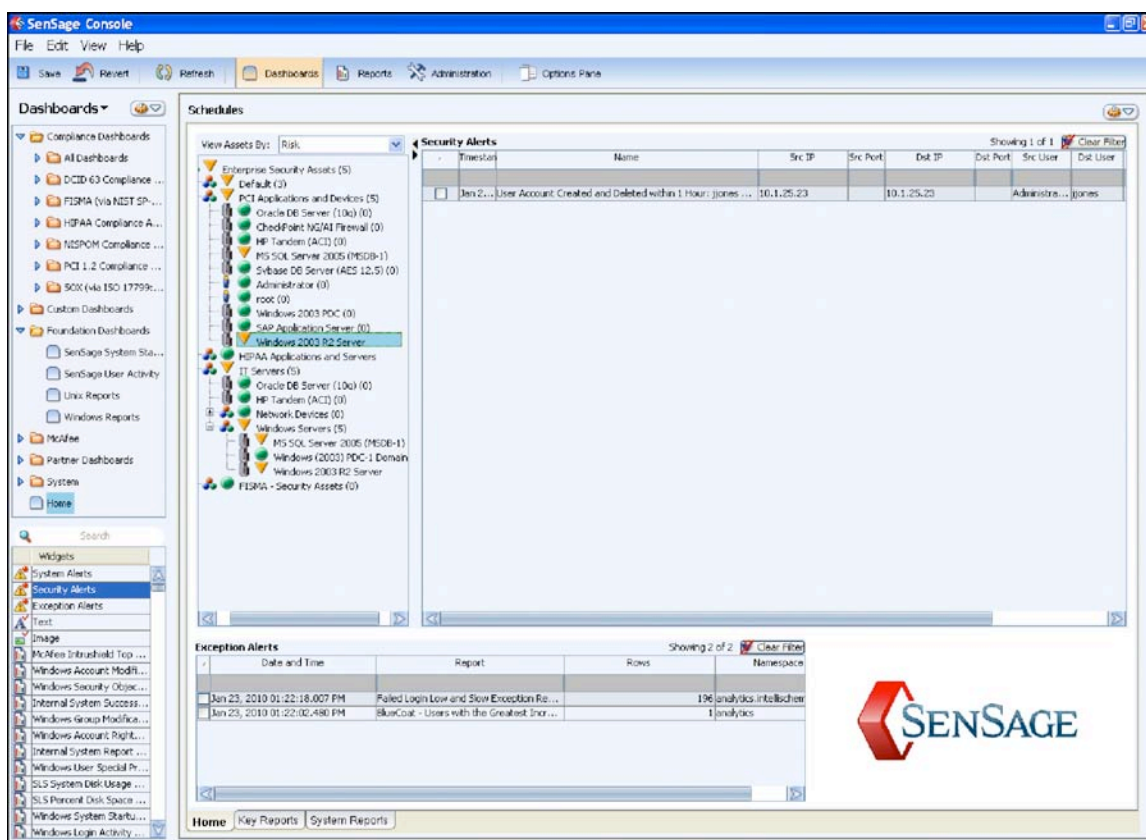


Figure 2. A real-time alert on user account being created and deleted within one hour occurs on PCI-related server. The SenSage Alert Console shows an alert firing on a PCI-related server.

What Just Happened?

SenSage Security Intelligence helps to answer that by providing a graphical representation of the correlated events, allowing the analyst to step through each event to see how they all fit together. This alert deals with a user account being created and deleted.

Is it important?

The asset tree along the left side identifies the machine as a MS-SQL database server used in processing credit card data. Clearly this is an important production asset and so this alert needs to be investigated as a possible breach.

What did that user account do while it was active?

Right-clicking on the value of the created account “jjones,” the analyst is able to choose the appropriate report for this situation from a menu of associated reports (see Figure 3). SenSage software automatically feeds the value of the field into the Investigation Wizard Report, and the analyst chooses a time frame commensurate with the time period when the account was active.

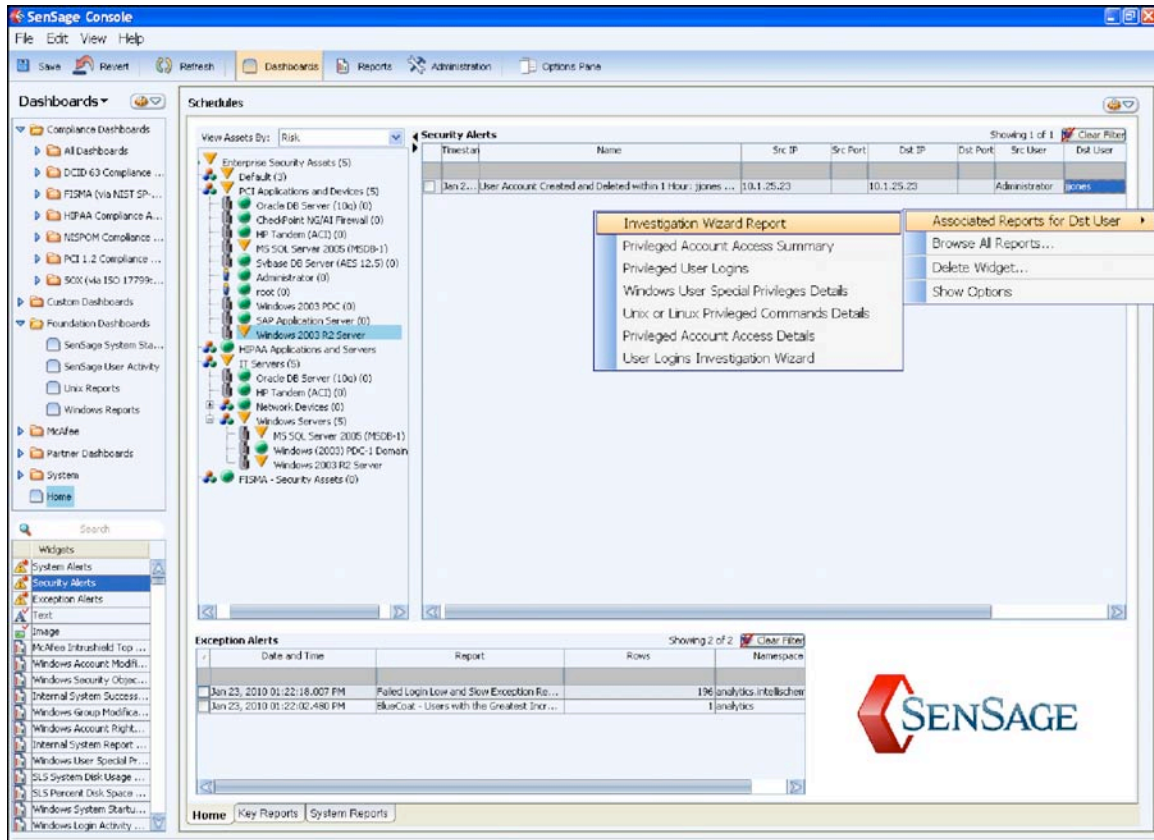
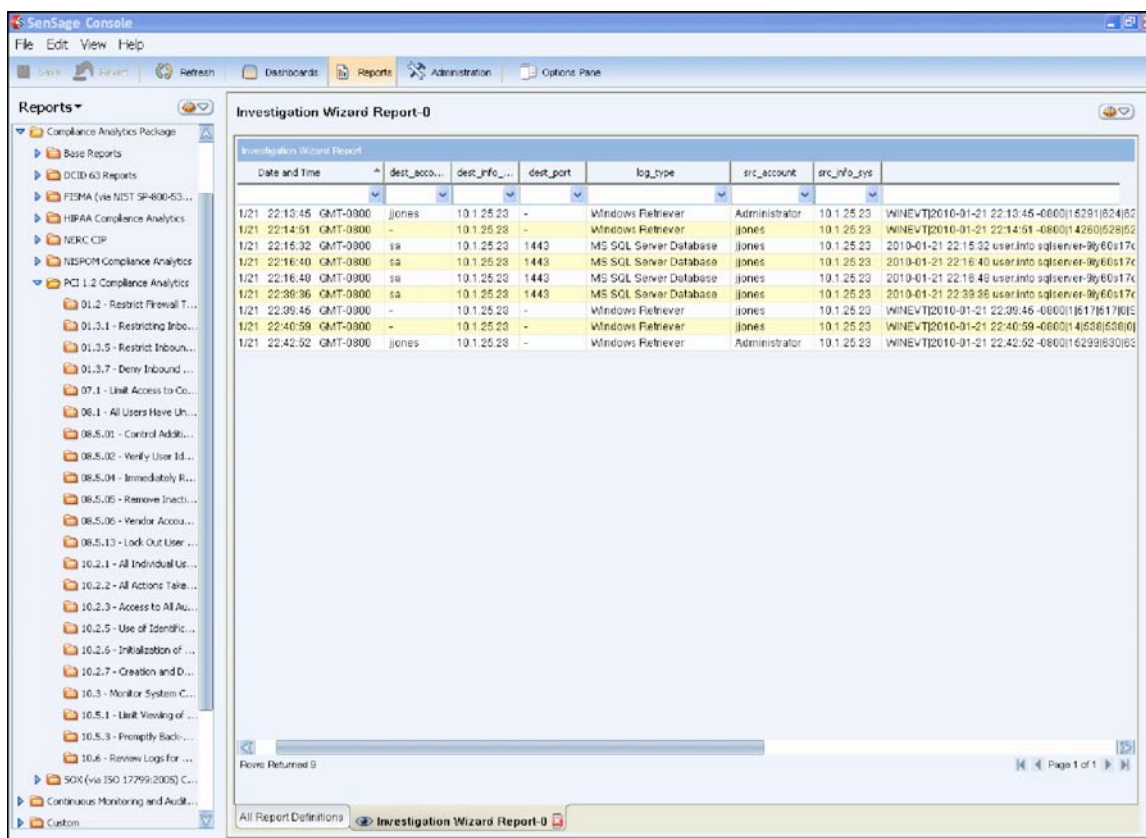


Figure 3. Drilling down directly from real-time alert to investigate user activity and bridging the gap between real-time and historical events.

The Investigation Wizard report returns all events for the time frame where jjones was specified (see Figure 4).



Date and Time	dest_accou...	dest_info...	dest_port	log_type	src_account	src_info_sys
1/21 22:13:45 GMT-0800	jjones	10.1.25.23	-	Windows Retriever	Administrator	WINEXT 2010-01-21 22:13:45-6800 16291 824 82
1/21 22:14:51 GMT-0800	-	10.1.25.28	-	Windows Retriever	jjones	WINEXT 2010-01-21 22:14:51-6800 14260 528 82
1/21 22:15:32 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:15:32 user.info sqlserver-96 66s 17c
1/21 22:16:40 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:16:40 user.info sqlserver-96 66s 17c
1/21 22:16:48 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:16:48 user.info sqlserver-96 66s 17c
1/21 22:36:36 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:36:36 user.info sqlserver-96 66s 17c
1/21 22:39:46 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	WINEXT 2010-01-21 22:39:46-6800 11617 6170 E
1/21 22:40:59 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	WINEXT 2010-01-21 22:40:59-6800 14538 638 80
1/21 22:42:52 GMT-0800	jjones	10.1.25.23	-	Windows Retriever	Administrator	WINEXT 2010-01-21 22:42:52-6800 16299 630 82

Figure 4. From alert to details: possible insider abuse.

The resulting report shows that jjones signed on locally to the database server (two Windows events), then switched to the “sa” account (akin to root for databases), issued some select commands to copy the Customers table (MSSQL events), and logged off of the machine (last Windows events).

This is a serious breach, so the analyst starts to document the investigation by exporting the report to a PDF file.

Has this ever happened before and we just didn't know about it?

Using the same Investigation Wizard Report, the analyst expands the time frame of the report to look over the last year (see Figure 5). What becomes immediately apparent is that this situation has happened a number of times using the same pattern—signing on locally as jjones, switching to the “sa” user account and searching through the customer database.

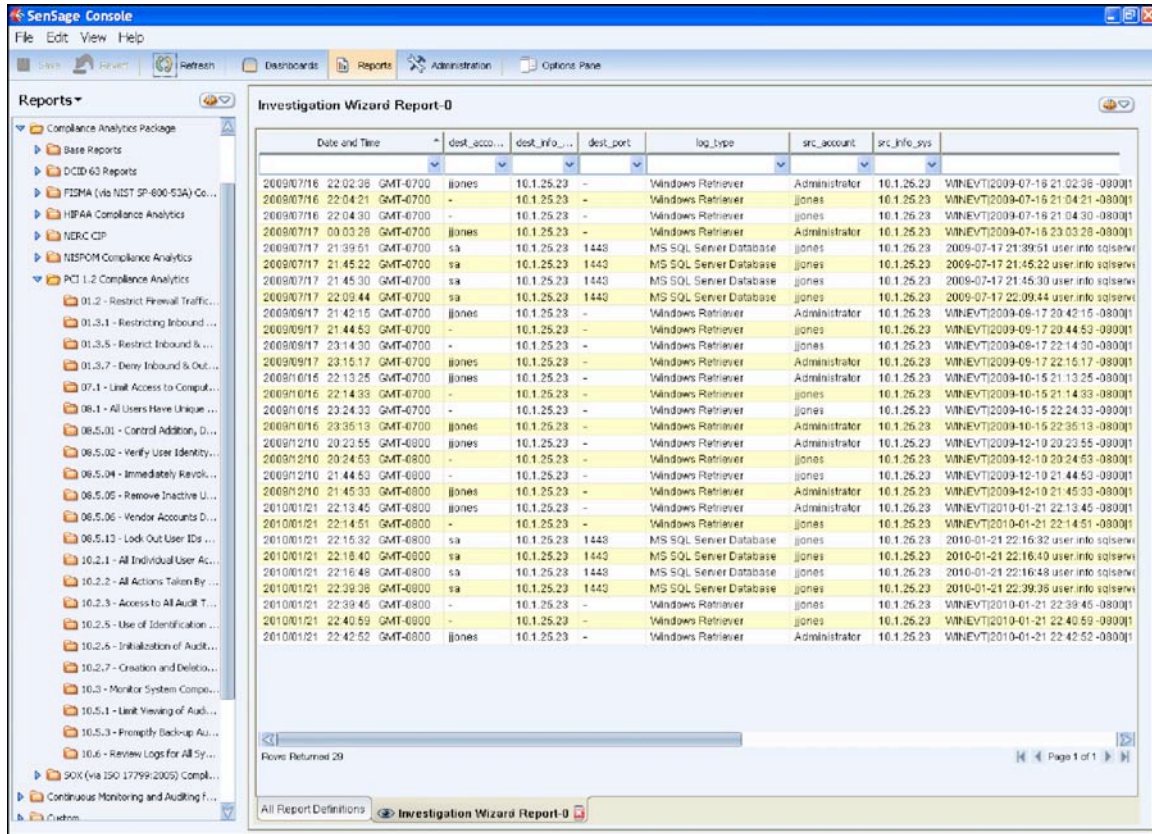


Figure 5. Uncovering a “low and slow” attack.

This situation is showing all of the signs of a “low and slow” attack, where the user has been performing these activities intermittently and trying to avoid detection. This was not noticed before because the jjones account was always active longer than one hour. The user became a victim of his own success; as he got much faster at what he was doing, it triggered the correlation rule. The analyst exports this report as well for documentation purposes.

It should be noted that the advantage of a SIEM product built on top of an event data warehouse is that the data is *always* online and available to query—with no restoration activities and no switching between short-term and long-term databases. SenSage solutions are unique in this regard.

What else happened on that server?

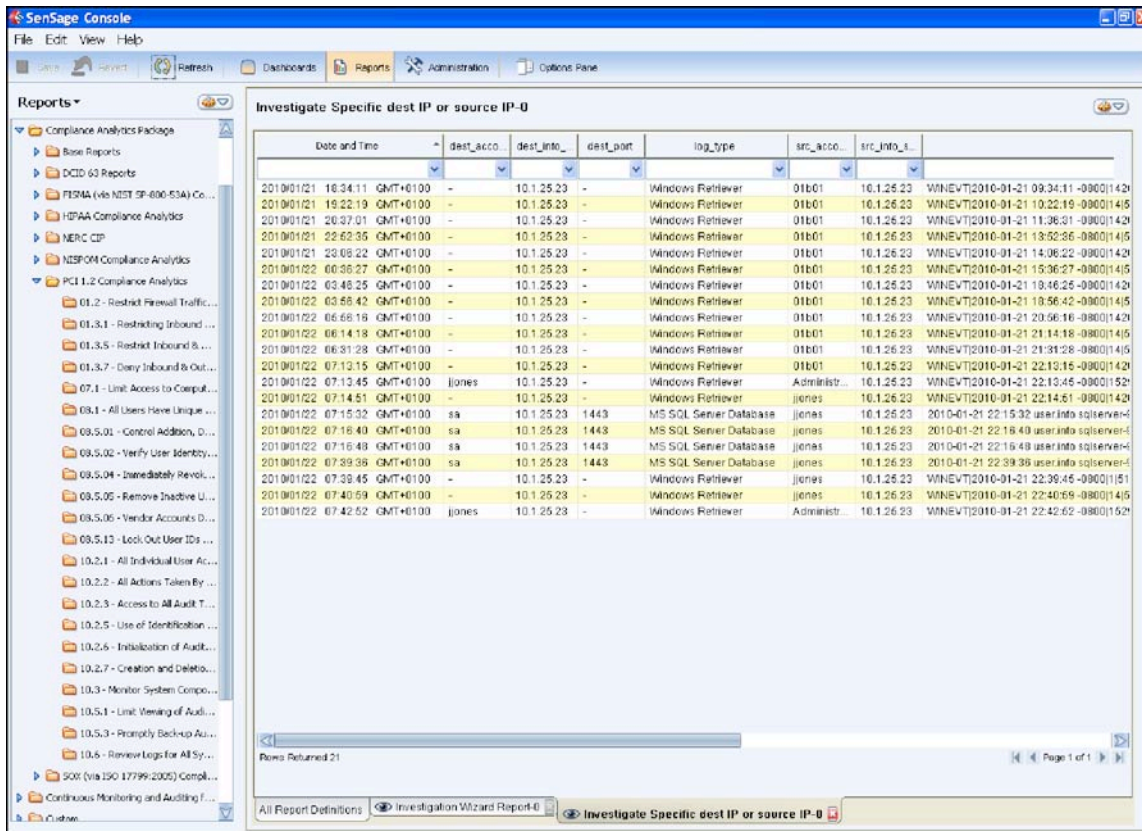
Until now the analysis has been focused on events that contained the user account jjones, but now that there is evidence of unauthorized activity, the analyst must expand the scope of the investigation to look at data from other sources. From the same report result, the analyst clicks on the IP address of the server, right-clicks to see the list of associated reports for drill-down, and selects the Investigate Specific Destination IP or Source IP report (see Figure 6).

The screenshot shows the SenSage Console interface. The main window displays an "Investigation Wizard Report-0" with a table of log entries. The table has columns for Date and Time, dest_acc..., dest_info..., dest_port, log_type, src_account, and src_info_sys. A context menu is open over the IP address 10.1.25.23 in the dest_info... column of the last row. The menu options include "Copy Selected Cells", "Associated Reports", "Browse All Reports...", "Run...", "Export", "Show Options", and "Investigate Specific dest IP or source IP".

Date and Time	dest_acc...	dest_info...	dest_port	log_type	src_account	src_info_sys
2009/07/16 22:02:38 GMT-0700	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-07-16 21:02:38 -0900]
2009/07/16 22:04:21 GMT-0700	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-07-16 21:04:21 -0900]
2009/07/16 22:04:30 GMT-0700	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-07-16 21:04:30 -0900]
2009/07/17 00:03:20 GMT-0700	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-07-16 23:03:20 -0900]
2009/07/17 21:39:51 GMT-0700	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2009-07-17 21:39:51 user info sqlserv
2009/07/17 21:45:22 GMT-0700	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2009-07-17 21:45:22 user info sqlserv
2009/07/17 21:45:30 GMT-0700	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2009-07-17 21:45:30 user info sqlserv
2009/07/17 22:09:44 GMT-0700	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2009-07-17 22:09:44 user info sqlserv
2009/08/17 21:42:15 GMT-0700	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-08-17 20:42:15 -0900]
2009/08/17 21:44:52 GMT-0700	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-08-17 20:44:52 -0900]
2009/08/17 23:14:00 GMT-0700	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-08-17 22:14:00 -0900]
2009/08/17 23:15:17 GMT-0700	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-08-17 22:15:17 -0900]
2009/01/16 22:13:25 GMT-0700	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-10-15 21:13:25 -0900]
2009/01/16 22:14:33 GMT-0700	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-10-15 21:14:33 -0900]
2009/01/16 23:24:33 GMT-0700	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-10-15 22:24:33 -0900]
2009/01/16 23:35:13 GMT-0700	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-10-15 22:35:13 -0900]
2009/01/21 20:23:55 GMT-0800	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-12-10 20:23:55 -0900]
2009/01/21 20:24:53 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-12-10 20:24:53 -0900]
2009/01/21 21:44:52 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2009-12-10 21:44:52 -0900]
2009/01/21 21:45:33 GMT-0800	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2009-12-10 21:45:33 -0900]
2010/01/21 22:13:45 GMT-0800	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2010-01-21 22:13:45 -0900]
2010/01/21 22:14:51 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2010-01-21 22:14:51 -0900]
2010/01/21 22:15:32 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:15:32 user info sqlserv
2010/01/21 22:16:40 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:16:40 user info sqlserv
2010/01/21 22:16:48 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:16:48 user info sqlserv
2010/01/21 22:39:36 GMT-0800	sa	10.1.25.23	1443	MS SQL Server Database	jjones	2010-01-21 22:39:36 user info sqlserv
2010/01/21 22:39:45 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2010-01-21 22:39:45 -0900]
2010/01/21 22:40:59 GMT-0800	-	10.1.25.23	-	Windows Retriever	jjones	10.1.25.23 WINHEVT[2010-01-21 22:40:59 -0900]
2010/01/21 22:42:52 GMT-0800	jjones	10.1.25.23	-	Windows Retriever	Administrator	10.1.25.23 WINHEVT[2010-01-21 22:42:52 -0900]

Figure 6. Investigation pivot: what else happened on that server?

This resulting report shows all events that contain the IP Address of the MSSQL Database server. In addition to the events seen earlier tied to jjones, the report also shows that the user “o1b01” had signed on locally to the server (see Figure 7).



Date and Time	dest_ip	dest_port	log_type	src_ip	src_info
20100121 18:34:11 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	WINEVT2010-01-21 09:34:11 -0900 142
20100121 19:22:19 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 10:22:19 -0900 145
20100121 20:37:01 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 11:36:31 -0900 142
20100121 22:62:35 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 13:52:35 -0900 145
20100121 23:08:22 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 14:08:22 -0900 142
20100122 00:36:27 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 15:36:27 -0900 145
20100122 03:48:25 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 18:48:25 -0900 142
20100122 03:56:42 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 18:56:42 -0900 145
20100122 06:68:16 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 20:68:16 -0900 142
20100122 06:14:18 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 21:14:18 -0900 145
20100122 06:31:28 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 21:31:28 -0900 145
20100122 07:13:15 GMT+0100	10.1.25.23	-	Windows Retriever	o1b01	10.1.26.23 WINEVT2010-01-21 22:13:15 -0900 142
20100122 07:13:45 GMT+0100	10.1.25.23	-	Windows Retriever	Administr...	10.1.26.23 WINEVT2010-01-21 22:13:45 -0900 152
20100122 07:14:51 GMT+0100	10.1.25.23	-	Windows Retriever	jjones	10.1.26.23 WINEVT2010-01-21 22:14:51 -0900 142
20100122 07:15:32 GMT+0100	10.1.25.23	1443	MS SQL Server Database	jjones	10.1.26.23 2010-01-21 22:15:32 user.info sqlserven-4
20100122 07:16:40 GMT+0100	10.1.25.23	1443	MS SQL Server Database	jjones	10.1.26.23 2010-01-21 22:16:40 user.info sqlserven-4
20100122 07:16:48 GMT+0100	10.1.25.23	1443	MS SQL Server Database	jjones	10.1.26.23 2010-01-21 22:16:48 user.info sqlserven-4
20100122 07:29:36 GMT+0100	10.1.25.23	1443	MS SQL Server Database	jjones	10.1.26.23 2010-01-21 22:29:36 user.info sqlserven-4
20100122 07:39:45 GMT+0100	10.1.25.23	-	Windows Retriever	jjones	10.1.26.23 WINEVT2010-01-21 22:39:45 -0900 151
20100122 07:40:59 GMT+0100	10.1.25.23	-	Windows Retriever	jjones	10.1.26.23 WINEVT2010-01-21 22:40:59 -0900 145
20100122 07:42:52 GMT+0100	10.1.25.23	-	Windows Retriever	Administr...	10.1.26.23 WINEVT2010-01-21 22:42:52 -0900 152

Figure 7. Another user account becomes part of the puzzle.

It also shows that user o1b01 logged off 30 seconds before the “administrator” account created jjones again. While not a smoking gun, it is suspicious enough to provoke some additional questions.

What else has o1b01 done? Accessed critical files?

Again from the same report result, the analyst clicks on o1b01, right-clicks to see the list of associated reports for drill-down, and selects the Windows Security Object Accessed Investigation report (see Figure 8). This report tracks access to a customized list of critical files the organization wants to monitor, and the results show that o1b01 has been looking at customer-related data. It appears more and more likely that there is an insider taking advantage of his access and that critical customer-related data may have been leaked.

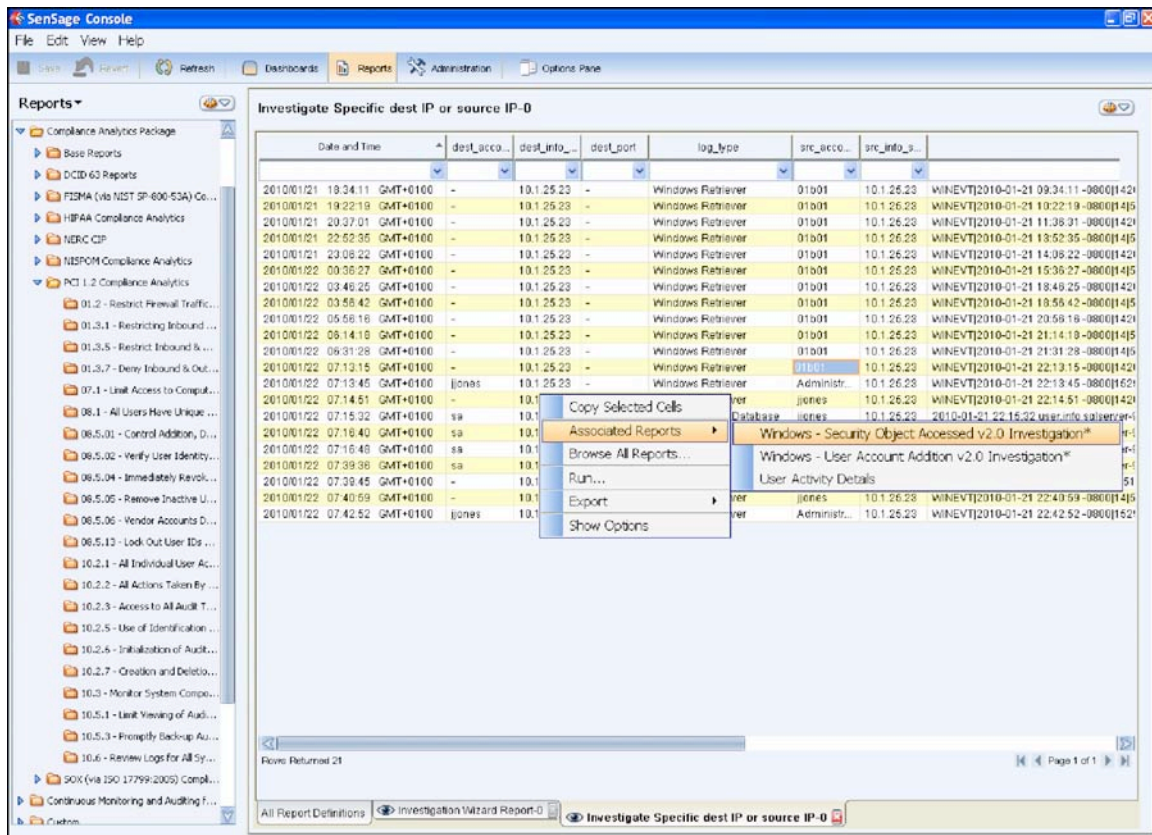


Figure 8. Investigation pivot: what else has the user done?

Notice how the report is returned as another page in this view without deleting the previous report. This allows the analyst to toggle back and forth without having to save or recreate previous work.

From here, the analyst could continue to ask questions (i.e., Did he create a Windows/Unix user? Did he use email to send the data out?), use the reports to get the answers, and then veer off from a returned value onto another investigation path.

SenSage solutions make it easy for organizations to institutionalize these investigation paths. This example made great use of associated reports to further the investigation, and it demonstrated that the available associated reports differed based on the situation. If you review a report and see something unusual you would like to investigate further, right-click and select Browse All Reports. This will present you with all of the SenSage reports in your environment, and you can execute any of them. If the selected drill-down report is something you want to be able to execute regularly from that report, you simply go to the Report Definition for that report and associate the drill-down report with it, and it will be easy to access in the future.

Once a senior analyst has gone through an investigation, the reports that were used can be defined as associated reports. When junior analysts review reports later, they will be guided on how to do an investigation by looking at what associated reports are available. In this way, sound Security Intelligence practices can be replicated quickly and easily throughout the organization.

Comparing the Cost of Security Intelligence Solutions to Traditional Alternatives

SenSage Security Intelligence solutions deliver more benefits at a significantly lower cost than traditional alternatives provided by SIEM, log management, and data warehouse vendors. Figure 9 summarizes the primary advantages of Security Intelligence: deep security context, high scalability, sophisticated analysis, and support for any data source. Traditional data warehouse products can scale and provide sophisticated and flexible data management capabilities, but they lack security context. Traditional SIEM and log management products have security context but do not scale well nor do they provide sufficient data management capabilities. Only SenSage Security Intelligence solutions provide a single architecture that delivers both security context and scalability.

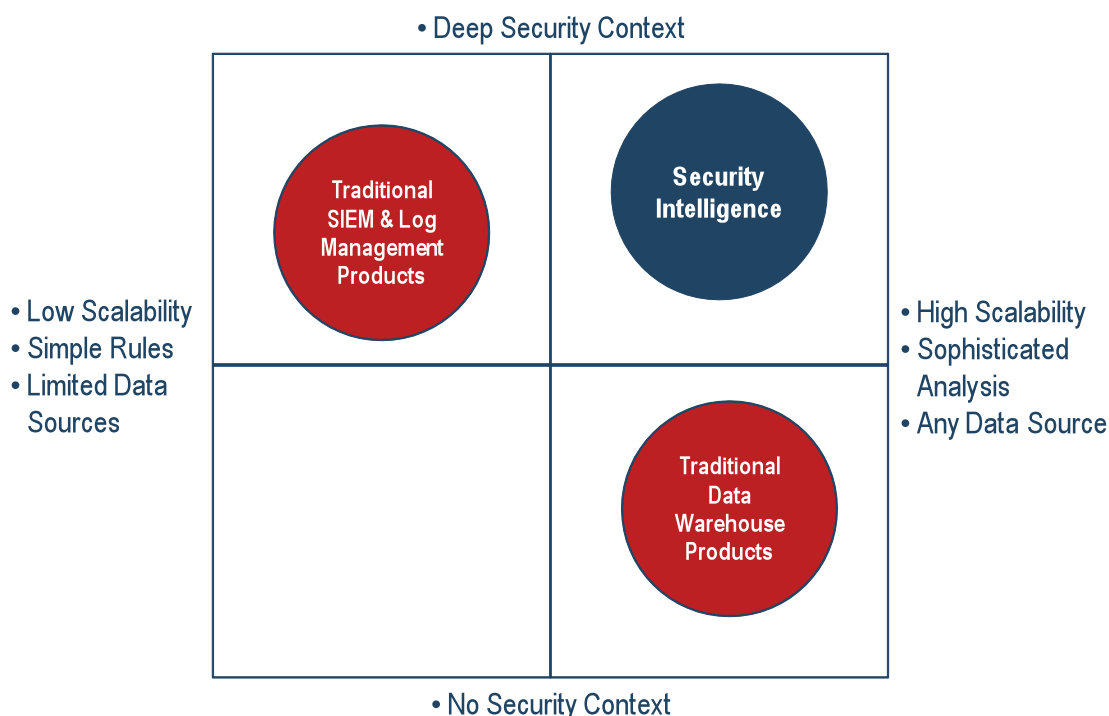


Figure 9. Security Intelligence Alternatives Comparison.

The comparison presented in Figure 10 below illustrates how the three-year cost of a SenSage solution is significantly lower than that of a traditional SIEM solution. The comparison assumes a load of 20GB of event data per day with a CAS device that reduces the cost of long-term retention.

The key areas where the traditional SIEM is more costly include software licensing and ongoing management expense. The latter stems from database administration overhead associated with relational database management systems and the added expense of retrieving event data archives stored in a separate, bolted-on product. Investigations using traditional solutions require users to access two different event repositories (short- and long-term) and use two different extraction methods (SQL and indexed searches) to obtain the necessary information. Investigations that

require accessing data kept on the CAS device would require a very costly and time-consuming process of restoring a number of archived files, querying the data, then flushing the data and repeating the process until all of the archives had been queried.

Investigations with SenSage Security Intelligence solutions involve a single repository and a single, precise method of extracting the data (SQL). The user simply chooses the time range they want the investigation to cover and runs the report query. Investigations involving data on the CAS device are done the same way because CAS devices are treated as on-line storage. In this way SenSage is able to provide the required Security Intelligence in a faster, less expensive, and more precise manner. Larger implementations produce even greater savings with the SenSage solution.

	SenSage	Traditional SIEM
Initial Investment		
Server & Storage Hardware	\$ 20,000	\$ 0
Archive Storage	68,000	68,000
Software/Appliance License	150,000	200,000
Windows Collection Agents	0	50,000
Professional Services	30,000	30,000
Total Initial Investment	\$268,000	\$348,000
Annual Expenses		
System Administration	\$ 35,000	\$ 70,000
Data Retrieval (2 investigations/month)	0	48,000
Software/Appliance Support & Maintenance	33,000	44,000
Hardware Support & Maintenance	17,600	13,600
Total Annual Expenses	\$ 85,600	\$175,600
Total 3 Year Expenses	\$518,800	\$874,800

Figure 10. SenSage Solution vs. Traditional SIEM: Total Cost of Ownership.

Summary

Organizations today are at risk from new security threats that are much more frequent and sophisticated than ever before. In addition, they face the challenge of responding to increased compliance regulations and audits. To protect themselves and to address compliance and audit requirements, organizations need to be able to implement enterprise-wide solutions that enable them to better manage and analyze their data in order to make the best strategic decisions.

While traditional SIEM, log management, and data warehouse point solutions are appropriate for many business requirements, they are unable to address the critical need that organizations operating in today's cyber-threatened environment have for more powerful and more comprehensive decision support. A new category of Security Intelligence solutions is needed to provide the comprehensive data management and analysis tools needed to meet these threats and challenges.

The Security Intelligence solutions from SenSage are the only solutions that provide today's organizations with enterprise-wide, essential decision support for security, compliance, and risk management operations. SenSage Security Intelligence delivers strong real-time threat detection combined with a patented event data warehouse that provides superior long-term analysis and retention—all accessible through an easy-to-use dynamic user interface. In addition, SenSage Security Intelligence solutions provide substantial cost savings. This makes them an attractive and logical choice, enabling organizations to gain higher benefits from the vast amount of data they must save, to protect their valuable and sensitive data, and to respond more easily and fully to compliance and audit requirements.

About SenSage, Inc.

SenSage[®], Inc. delivers Security Intelligence solutions that provide essential decision support to cyber-security, risk management, and compliance operations. These solutions enable the necessary convergence of security information and event management (SIEM), log management, and continuous controls monitoring through a single console and data management architecture. Over 450 organizations and government agencies around the world rely upon SenSage to combine these functions in support of more holistic IT oversight, real-time alerting and investigation, incident response, and compliance reporting. Combining a patented event data warehouse platform and interactive analytics environment, SenSage Security Intelligence solutions are more scalable, flexible, and affordable than traditional SIEM, log management, and data warehouse point products. SenSage goes to market with industry-leading OEMs and strategic alliance partners including Cerner, Cisco, EMC, HP, McAfee, and SAP. Visit www.SenSage.com for more information.

SenSage, Inc.
www.SenSage.com

Corporate Headquarters

SenSage, Inc.
55 Hawthorne Street, Suite 700
San Francisco, CA 94105 USA
Phone: +1.415.808.5900
Fax: +1.415.371.1385
Email: info@sensage.com

EMEA Headquarters

SenSage, Inc.
Venture House,
Arlington Square,
Downshire Way,
Bracknell, RG12 1WA
United Kingdom
Phone: +44 1344 741 053
Fax: +44 1344 741 001
Email: emea@sensage.com

© Copyright 2010 SenSage, Inc. All rights reserved. SenSage is a trademark of SenSage, Inc. in the United States.