

---

# IT Security Event Management



[Yahya Mehdizadeh](#)  
CISSP, GSEC  
June 2004

**Abstract:** This white paper addresses the emerging technology of IT security event management, also referred to as IT security information management. The functional architecture of SEM system is discussed along with features to consider when selecting a SEM system. The audience for this document is technologist that either what to know more about SEM or are in the process of evaluating a SEM system.

# Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>1.0 BACKGROUND .....</b>	<b>5</b>
<b>2.0 INTRODUCTION .....</b>	<b>5</b>
<b>3.0 ARCHITECTURE .....</b>	<b>6</b>
3.1 Monitored Elements .....	7
3.2 Event Collection .....	7
3.3 Core Engine .....	8
3.4 User Interface .....	8
<b>4.0 EVENT WORKFLOW .....</b>	<b>9</b>
<b>5.0 SEM FEATURES .....</b>	<b>10</b>
<b>6.0 CASE STUDY 1 .....</b>	<b>12</b>
<b>CASE STUDY 2.....</b>	<b>13</b>
<b>7.0 COST/BENEFIT .....</b>	<b>13</b>
<b>8.0 CONCLUSION .....</b>	<b>14</b>

---

## Executive Summary

Enterprise IT Security Event Manager (IT SEM) focuses primarily on the tools, technologies and services that are needed by IT security operations to manage security devices and the security of IT infrastructure, applications and transactions. The value proposition for such technology is the correlation of security data from multiple devices and systems to enable better security assessment and support appropriate remedial action. The motivation behind this technology grew out of the failure of intrusion detection systems (IDSs) to separate real threats from the background noise of ineffective probes, false alarms and normal system changes.

### 1.0 Background

At one time IT security staff responsible for security operations faced a significant challenge when it came to protecting the security infrastructure of an organization. Faced with excess instrumentation for networks, servers and security devices that produced a flood of data and false alarms, security personnel had to sort through the data to determine if a security event was taking place, substantiate the criticality of the event and finally initiate an appropriate response.

It was in this environment that IT security management market emerged to meet the need to improve the efficiency of intrusion detection systems, consolidate information about enterprises' general security postures and support enterprises' efforts to consolidate security operations. In addition, companies are turning to centralized security event management tools to help them make sense of crucial security information.

Furthermore, according to Forrester Research Inc, new and proposed government regulations are also requiring companies to constantly monitor their networks for security incidents which is increasing interest for Security Event Manager systems.

### 2.0 Introduction

IT Security Event Manager provides an enterprise-wide security monitoring and administration solution that collects data on events, analyzes the data, and provides a suitable response to threats on enterprise assets. It is positioned as a security information management tool that can be used by an enterprise-class network management centers or managed security service providers with interest in protecting physical and/or logical assets.

The following IT environment has been crucial in giving momentum to this technology:

- The necessity to consolidate the security operations of heterogeneous environments.
- The requirement to decipher useful information from the flood of raw data and alerts that are generated by security devices.

- The need to provide a timely action to threats and vulnerabilities identified.

### 3.0 Architecture

A typical SEM architecture consists of three modules – a user interface, the core engine, and event collection. The event collection module interfaces with the monitored elements that are already installed in an enterprise. The core engine module processes information from the flood of raw data and alerts that are generated by security devices into an intelligent interrelated format for proper analysis and correlation. This module also provides the capability to integrate with third party applications to extend the functionality of the SEM engine.

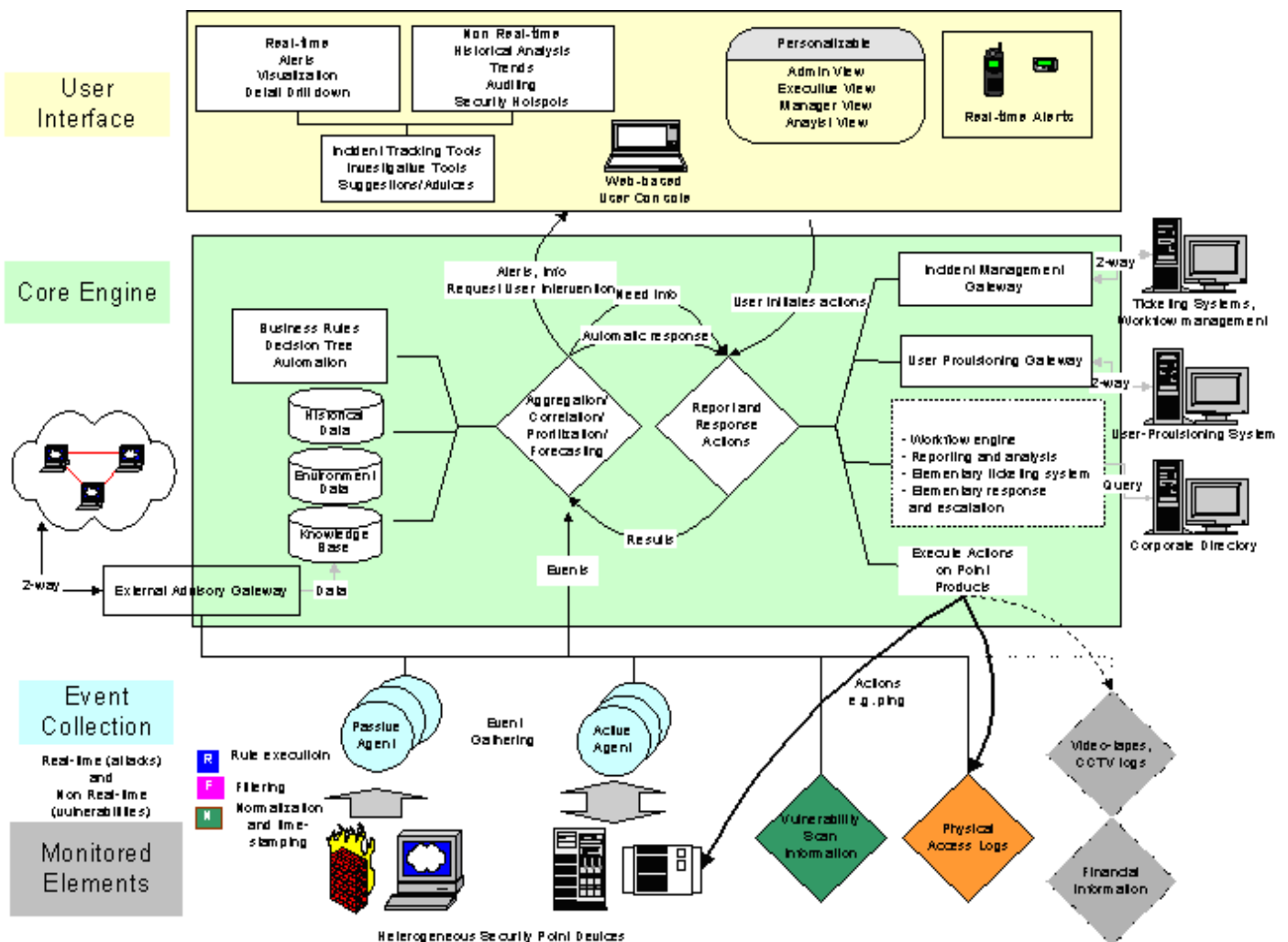


Figure 1: Architecture

### **3.1 Monitored Elements**

Monitored elements are security point products such as intrusion detection systems (network-based or host-based), firewalls, anti-virus software packages, VPN, routers, web servers, databases, and host operating systems. The products generate security events that can be collected by collector agents and forwarded to the Security Event Manager. A security event is defined as a single or collection of actions that violate the security policy of an organization. For example, an intrusion detection system reports a network attack and firewalls report rule-set violations which are consolidated and sent back to the core engine for processing.

There are currently several software packages on the market that manage different types of point products. These products often consolidate events from multiple point products of the same type. For example Checkpoint use Provider-1 to manage multiple firewalls, Netscreen uses Global-Pro and Nokia, Horizon Manager. This manager software is part of the monitored elements module of a SEM system. The manager software may aggregate and correlate events from the point products, and then forward these events to the SEM system, which would act as a consolidator of managers.

Some enterprises may already have a network management system (ie Micromuse) in place that is responsible for monitoring network health. The events collected by the NMS application could be forwarded to the SEM for security processing.

### **3.2 Event Collection**

The primary responsibility of the event collection module is to interface with the monitored elements and collect events. Software “agents” receive the events and provide them with a time stamp. The time stamp ensures that all events have the same time reference regardless of the time on the individual point products. The agents also normalize the data by parsing the raw information into a common format understood by the SEM system. Before forwarding the events to the core engine module, the agents execute rules and filter the events to select the security-related events. Only these events (defined by business rules) are sent to the core engine.

There are two different types of agents:

- **Passive** agents gather events from point products without direct interaction with the products.
- **Active** agents interact with the point products to gather information, such as issuing a ping or sending an http request.

Agents can be further categorized into **real-time** and **non real-time** agents. The real-time agents gather security events as they happen, while non real-time agents poll the devices periodically to determine vulnerabilities. The protocol of the point product determines how the agent interacts with them.

### **3.3 Core Engine**

The core engine carries out the processing of the collected events and provides a response according to business rules. Event processing includes aggregation, correlation, and prioritization.

- **Aggregation** is the act of gathering similar events and combining them into one event. Aggregation helps the SEM system avoid forwarding/receiving duplicate events.
- **Correlation** security sub-events generated during the data mining stage are linked, which enables to reconstruct a security event.
- **Prioritization** determines the order in which the security analysts should handle the events based on threat assessment.

Event processing depends on the input from the following:

- **Business rules**, decision trees define the rules that govern correlation and response logistics.
- The **Historical Database** provides information on previously collected events.
- The **Environmental Database** provides information on the assets and their configuration inside the enterprise environment. Such as which machine is running what software, how critical they are, what is the associated risk, who are the users and what are their roles.

The core engine also contains a set of tools that can be used to respond to events. These actions are sometimes executed automatically as defined by business rules and other times, the user must initiate the response. At times, the event-processing engine may lack the necessary information to make a decision and needs to execute a tool to gather additional information for correlation and prioritization.

Different types of tools include:

- Actions executed on point products, which include but are not limited to the following: blocking a firewall port, initiating “syslog” backup, or commands such as “traceroute” or “whois.” These actions are executed by running a script or a program.
- Third-party applications such as vulnerability assessment tools that are tied to remediation databases.

### **3.4 User Interface**

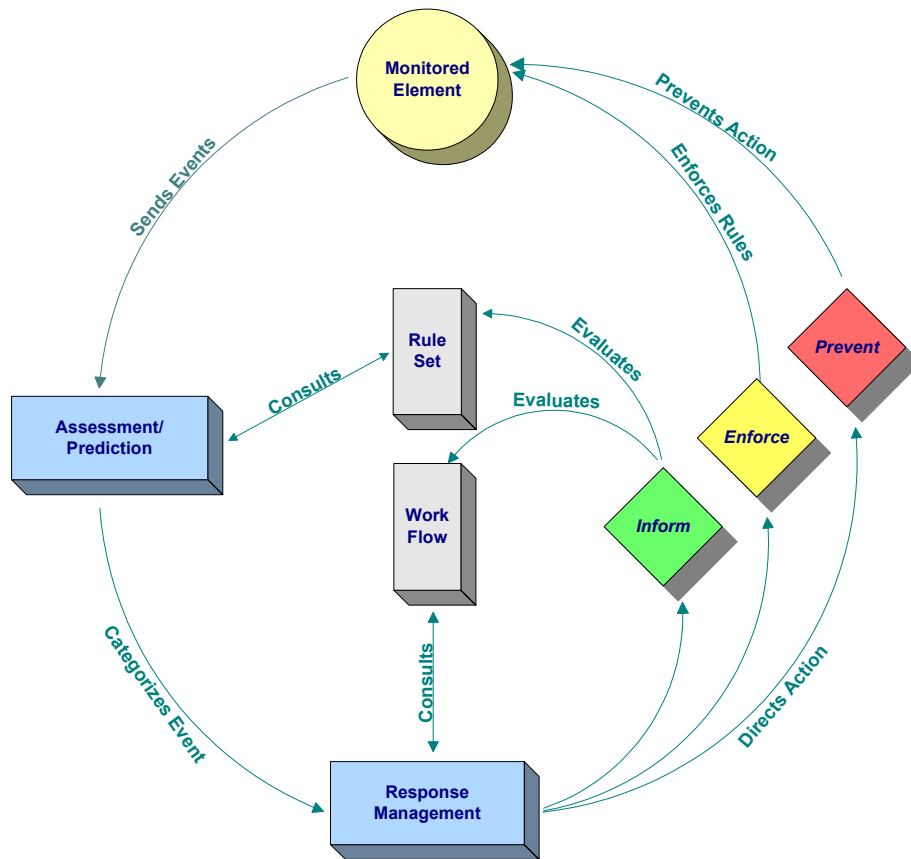
The user interface module describes how the users interact with the system. The interface is used to monitor security alerts, as well as for performing system administration tasks. Additionally, it can interface with other management tools such as HP Openview, IBM’s Tivoli to gather and report some of the same information.

This information gathering and reporting depends on the enterprise security policy and security network operations procedures.

In summary the primary objectives of all the modules interacting together are to reduce the number of alerts that must be evaluated. They do that by automating the evaluation of a significant percentage of security data, and also by reducing the labor associated with security log analysis.

## 4.0 Event Workflow

The event workflow of an security event manager is very crucial in deciphering the right information. Not only does the right information need to be collected but the appropriate rule sets need to be applied to the data to determine action to be taken. The following illustration depicts how a stream of events should flow:



Once the data has been collected from the monitored elements the information is examined by the Assessment and Prediction capabilities of a SEM system. Here the Rule Set is consulted to determine if the event information is of significance. If so, the event information is categorized for Response Management, which consults the predefined work flows to determine what response actions should be taken. The most common response are the following:

At the *Inform* level, response is directed to an appropriate analyst for further review. After review, the analyst may take separate action to amend either the Rule Set or the Work Flow to improve the response of the SEM system should these events re-occur. Hence this is also where the knowledge base is propagated for future reference.

The *Enforce* level, identifies the need to force compliance with the predefined policies of the enterprise and takes direct action to do so. A simple example might be that the SEM system detects that a password or other system secret has not been changed within the prescribed period of time and force a password change.

At the *Prevent* level, a serious risk or threat has been detected by the SEM system. Using the predefined workflow for such occurrences, the SEM rule set reacts to minimize if not eliminate the risk. For example, if a SEM system detected an intrusion in progress on a particular device, it could act to shut the device down pending further investigation by the appropriate analysts.

## 5.0 SEM System Features

Most SEM systems available in the market have common baseline, which should include event collection, aggregation, correlation, analysis and response. A comprehensive selection criterion for a SEM system is listed below. These are features that should be evaluated or considered when selecting a SEM vendor. Appendix A lists some of the more popular SEMs vendors that satisfy these features.

Features
Monitoring of security infrastructure components (hardware and software).
Analysis of information reported by / from security infrastructure components.
Local response to events in spite of network failures.
Guaranteed (but possibly delayed) synchronization of events and responses between local and central components.
Monitoring of network systems.
Monitoring of building control systems such as physical access and fire control.
Monitoring of security systems.
Management of local rules controlling event responses.
Management of central rules controlling event responses.
Management of security workflows.
Management of escalation in workflows.
Post mortem analysis of events.
Secure, real-time and collaborative alternative communications channel with enterprise security personnel in response to threats or attacks.

Features
Threat prediction and forecasting.
Detection, identification and reporting of issues and events.
Collection and correlation (connect-the-dots) of issues and events from sources throughout the enterprise.
Logging of administrative actions.
Management of enterprise assets.
Automated triggering of actions / reactions to protect assets.
Automated, rule-based escalation to insure timely resolution.
Definition and reporting of Key Performance Indicators (KPI's)
Prepared (static) reporting of events.
Ad hoc reporting of events to support forensic analysis and executive decision.
Statistical quality control (SQC) reports.
Visualization (both logically and physically) "reports."
Communication with and real-time control of systems protecting enterprise assets.
Portal to external security and system information.
Reviewing local compliance to security policies.
Incident reports required by regulatory bodies.
Network infrastructure management.
Monitoring attacks and responses in real-time.
Centralized configuration, audit logging and operational logging.
Framework / toolkit for creating agents.
Components that execute on many different enterprise operating systems.
Role-based authorization.
History or roles played by subjects.
Responses based on time horizon (short-term and long-term).
Management of enterprise policies.
Support of custom agents built by the enterprise.
Enforcement of enterprise policies.
Integration with enterprise provisioning systems.
Provisioning of employees.

Features
Integrity of application internal data.
Risk analysis
Contingency planning
Security planning
Migration planning or implementation of enterprise system updates, upgrades, or enhancements
Data exchange with Intrusion Detection Systems (IDS)
Automated generation of assurance documentation
Simulated security training
Operational advisories or alerts from monitored elements

However, in addition to the features listed, it is important to note the following constraints: a SEM system is a distributed heterogeneous management system. As such, it shares some of the same strengths and weaknesses of diverse distributed systems. At the foundation it can aggregate events and can improve efficiency and lower security risk. But on the other hand they are complex to deploy, require interoperability of many devices from different vendors and could be expensive to maintain. Furthermore, the human cost to deploy, maintain and use a SEM system is significant. Not only do the systems need to be configured and deployed, but security personnel need to be trained to use the system and at a minimum follow-up on “emergency” alerts. Needless to say, the security analyst is a crucial part of a SEM system and without their involvement; the SEM system would be ineffective.

## 6.0 Case Study 1

To better understand how a SEM system works, two case studies have been presented:

The W32.Sasser.Worm hit the Internet the first week of May 2004. The intent of the worm was to exploit the vulnerability described in [Microsoft Security Bulletin MS04-011](#). It began to infect corporate networks and spread by scanning the randomly selected IP addresses of vulnerable systems.

The way the virus spread was by determining the local machine's IP address. It did this by looping through every address returned by *gethostbyname* for the local hostname. If it found a publicly routable Internet address (non-RFC1918) it would use that address. If none were found it would use any private subnet address (RFC1918 or 127.0.0.1) it found. If no address was returned it would use 127.0.0.1

If successful, the exploit would open a shell on the remote system on TCP port 9996 and attempt to copy the worm via an FTP transfer.

A SEM system would have detected the following:

- Scanning of IP address would have been a violation of most corporate Firewalls and hence would have raised in an alert in the SEM Core Engine.
- FTP connects to remote hosts outside the corporate network would also be deemed as a violation of security policy and recorded as a security event by the SEM core.
- Activity on port 9996 could have also triggered a security incident based on the SEM rule set.

These three events by themselves may have not been interpreted as a malicious attack. But once correlated the IT SEM would have alerted the system admin of a possible attack. It would have observed that the host scanning for IP addresses was also the host attempting FTP connects and all on the same port 9996.

Thus an organization with a SEM deployed would have detected the Saaser worm at a faster pace and stopped the spread of the virus by configuring the Antivirus gateways at the internet router to remediate the attack.

## Case Study 2

The Attack – A hacker scans the public network looking for active systems to attack. The scan detects a firewall and web server as active and responsive systems. The attacker attempts to scan both systems to get a listing of available services in order to identify potential vulnerabilities. Although no vulnerability is found on the Firewall, but the HTTP service is located on the web server. Having access to the HTTP service, the attacker successfully exploits vulnerability and executes a Trojan on the web server which then establishes an outbound connection to the attacker.

The Response – The IT SEM system detects from the firewall logs that an attacker has performed a ping sweep against an internal system. The SEM raises a warning message indicating suspicious activity. Next the SEM system detects several port scans on the internal network. The port scans and pings cause several IDS alerts to be generated which in turn are detected by the SEM system. The port scans are correlated with the previous ping sweep and IDS alerts and conclude that a system has been compromised. The event is escalated to an “emergency” status and responds with an appropriate action by the SEM system which could be either in the form of a notification or a service/port shutdown. Thus in this case the SEM system would have prevented the compromise of an internal system by an attacker.

## 7.0 Cost/Benefit

Estimated budget to deploy a IT SEM system starts from the \$100K range and goes up. The core SEM engine starts in the \$50-60K range for the server software. The agents which aggregate the data from the various devices cost anywhere between \$400-900 per agent. Add an additional \$15K for the hardware with appropriate disk space, memory and bandwidth connectivity for log consolidation and archiving. Next include 7-10 days of professional services at \$1000/per day to design, deploy and customize the SEM system to individual corporate requirements.

In addition to the hardware and software, one must also consider the cost of security personnel to monitor and manage the system which in today's high tech market is in the \$80K+ range. Add to this training, replacement, separation of duties and career path concerns and you are well into the \$140K range.

Although these cost combined together may seem high, but the overall cost of deploying a SEM should be gauged against the loss of value resulting from a compromise of corporate information assets and downtime associated with a malicious attack or the prevention of such attacks.

## **8.0 Conclusion**

Information security administrators face numerous challenges today. Rapidly increasing attacks through the Internet, coupled with persistent threat of insider abuse, demand the attention of security staff on a daily basis. However, as corporations deploy more and more security solutions to protect against these threats, the amount of data being generated by these solutions has become overwhelming. In order to adequately protect corporate information assets on a 7x24 basis, information security staff must constantly analyze security data from various security devices, such as firewalls, Intrusion Detection Systems (IDS's), to identify and counteract security attacks in real time.

The IT Security Event Manager market is driven by enterprises' needs to filter, aggregate and correlate security data from heterogeneous sources for real-time monitoring and historical analysis. Primary adopters of this technology tend to be large organizations with a complex IT infrastructure and dedicated IT security staff.

Security Event Manager provides an enterprise-wide solution for security monitoring and administration. It reduces the amount of time security officers need to spend to detect attacks and vulnerabilities on the network by reducing the amount of information that needs to be processed. As a result enterprise assets are better protected against threats.

When selecting a IT SEM vendor it is important to look at functional capabilities with specific focus given to ease of deployment, integrated vulnerability management tools, and monitoring and reporting functionality for regulatory and audit compliance.

In short the Security is an investment, not an expense. The challenge is to get this point across to upper management. Investing in computer and network security measures that meet changing business requirements and risks makes it possible to satisfy changing business requirements without hurting the business' viability.

## **Bibliography**

Technology evaluation of Netforensics, Micromuse, CA, Intellitactics and open service.

[http://www.infoworld.com/article/03/01/10/030113fenexttci\\_1.html](http://www.infoworld.com/article/03/01/10/030113fenexttci_1.html)

<http://www.computerworld.com/securitytopics/security/story/0,10801,83978,00.html>

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

About the Author: Yahya Mehdizadeh, was the director of Managed Security Services for SchlumbergerSema where he had responsibility in defining the tools, technology and processes for implementing an enterprise wide managed security service including the security administration in the 2004 [Athens Olympics](#). He can be reached at [Yahya@mehdizadeh.org](mailto:Yahya@mehdizadeh.org)

## **Appendix A**

- **Arcsight Inc.**  
TruThreat Risk Correlation Engine: Combines threat-severity information with asset data to determine and prioritize risk. Allows administrators to set and monitor policies according to asset priorities. Arcsight is considered to be a leader in vulnerability assessment data integration and visualization.
- **Computer Associates International Inc.**  
eTrust security management software: Product suite comprising of identity management, access management and threat management components. An eTrust security center provides centralized management of these functions.
- **e-Security Inc.**  
eSecurity Security Event Manager: Consists of three modules -- Sentinel, Wizard and Advisor -- for gathering and analyzing and centralized reporting of security event data. e-Security has technology and sales relationships with Hewlett-Packard.
- **IBM**  
Tivoli Security Event Manager: Allows users to automate responses to security events in addition to helping monitor and track security events.
- **Intellitactics Inc.**  
Network Security Manager: Does security event correlation from multivendor security devices and nonsecurity information sources and provides a graphical visualization of threats, anomalies and trends. The company is considered to be a leader in threat visualization and vulnerability assessment data integration.
- **netForensics Inc.**  
Security Incident Manager: Uses a three-tier architecture. Agents gather data from security systems, Engines aggregate and correlate the data, and the Real-Time Console presents the data. NetForensics has a rather large installed base mainly as a result of its strong relationship with Cisco Systems.
- **NetIQ Inc.**  
VigilEnt Integrated Security Management: A product suite for policy and compliance management, administration and identity management, vulnerability and configuration management, and incident and event management.
- **Symantec Corp.**  
Symantec Security Management System: Combines a security incident manager component for consolidating and correlating security information from disparate systems, an event-manager for antivirus software and a security manager policy-compliance tool.