



# Building the Better Mousetrap:

*An Analysis of Security Management Systems*

*By Darwin Herdman  
Chief Technology Officer, RedSiren*

*RedSiren White Paper  
February 2003*

1.877.360.7602  
info@redsiren.com  
www.redsiren.com



## Table of Contents

<b>Executive Summary</b> .....	3
<b>Identifying the Challenge</b> .....	4
Silent Intruders.....	4
Interdependent Systems.....	5
Finding Real Incidents Within the Noise.....	5
<b>Management Technologies</b> .....	6
Comparing Security Management Technologies.....	7
<b>The Security Knowledge System: The Better Mousetrap</b> .....	8
Level 1: Data Collection and Custom APIs.....	9
Level 2: Data Management and Secure Transport.....	9
Level 3: Enterprise Knowledgebase.....	10
The Importance of Data Mining.....	10
Building Knowledge.....	11
<b>Deploying Security Management</b> .....	11
<b>Conclusion</b> .....	12
<b>About the Author</b> .....	13
<b>About RedSiren</b> .....	13



## Executive Summary

The increase in computer security-related incidents, losses and reliance on interconnected systems demands that new measures and strategies be applied to information security, not only to better protect the enterprise, but also to sustain business operations.

Many of these strategies and concepts are unfolding as developers and scientists continue to work to build the perfect defensive product. A number of recent announcements and activities have been focused on security management as an attempt to reach a state of *information integrity*.

**Information Integrity**—A state of operations where business systems are protected continuously, warnings and alerts are accurate and responses are meaningful and pertinent to the business.

The positions presented in this white paper are:

- Threats to information integrity are constantly changing and require continuous investment, vigilance and management.
- Information security will continue to fail as long as security technology and service activities are coordinated independently.
- Traditional vendor management solutions and enterprise management systems are incapable of bringing the entire security picture together.
- Security Information Management (SIM) systems fall short of what is truly needed to deliver information integrity.
- Security Knowledge Systems (SKSs) define a higher order of service and ability that shall become critical to mitigate new threats and continuously improve operations.
- Outsourcing security management to a managed security service provider (MSSP) that utilizes a security knowledge system offers the best return on investment across costs, security and value.

The positions presented in this paper are the result of RedSiren's performance and experience as an MSSP and developer of incident response systems. The Security Knowledge System concept and technology was born out of studies of RedSiren's internal business process reengineering, quality management and enterprise application integration, conducted from 1999 through 2002.



## Identifying the Challenge

Meeting the challenge of sustaining information operations is a progressive and forever-changing task for chief information officers, security officers and designated parties. On a daily basis, each officer must grapple with the risks posed by new information technology threats—and the costs to mitigate and avoid their success.

To date, individual product approaches have been ineffective at avoiding attacks and reducing security incidents. While the technology works as stated, the number of new vulnerabilities and incidents are nearly doubling year-to-year, according to 10-year studies<sup>1</sup> of vulnerabilities and their attempted use. Driving growth is the vast accessibility of complex attack tools that may be executed by any novice PC and in some cases, gaming systems<sup>2</sup>.

Risk to information operations is further affected by the business's reliance on interconnected systems and applications. Malicious code introduced to a PC in Malaysia may rapidly invade suppliers and private network links around the globe.

As a result, many businesses face the difficult question, "How safe should an organization's network be against intruders?" According to the 2002 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI)<sup>3</sup> survey, 90 percent of respondents (primarily large companies and government agencies) said they had experienced successful security breaches within the last year. The silent entry in which one penetrates, steals and leaves while disturbing little is the most worrisome breach. While much press is focused on defacing pages, industrial espionage may not be discovered for days or months, if at all.

A disturbing example of this occurred at Microsoft Corp.<sup>4</sup>, where hackers broke into the company's network and accessed the company's most valued intellectual property—source code. The intruders were apparently inside the network long enough to copy the code, and Microsoft's security experts detected the breach only after they discovered their passwords being e-mailed to Russia.

## Silent Intruders

Patient and persistent attackers systematically breach network defenses without setting off commercially available single-point security products. Such attacks, either from outside or inside the network, come from skilled intruders who break into systems for any number of purposes—to show how smart they are, to pull pranks, to navigate inside a network or to steal information. Their presence has potentially harmful outcomes. A single attack can irreparably damage a company's reputation or its ability to do business. Sophisticated attackers have the skill to blend in with a network populace and are consequently hard to detect. They often use unknown or forgotten "back-doors" to access networks.

<sup>1</sup> From the CERT® Coordination Center. See [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html) for more information.

<sup>2</sup> As presented by Chris Davis, CISSP, and Aaron Higbee, CISSP in their presentation, "DC Phone Home," at the 2002 Black Hat USA Conference. Visit <http://www.blackhat.com> for more information.

<sup>3</sup> Visit [www.gocsi.com](http://www.gocsi.com) to download a free copy of the report.

<sup>4</sup> As reported by Ted Bridis and Rebecca Buckman, "Microsoft Hacked! Code Stolen?", Wall Street Journal, Oct. 26, 2000.



Skilled attackers present network security managers with two challenges. The first is to find out whether an attack is occurring, and the second is to figure out what is under attack. Without the right knowledge or tools, searching could be a useless and expensive exercise—especially if a breach is nearly invisible. The sophisticated intruder knows how to hide deep within the mountain of data that comprises the modern network-driven organization. A mid-sized network moves billions of bytes daily and a global network moves trillions. As such, it is easy to disappear among billions of 1s and 0s.

Attackers can take advantage of published procedures on how to evade systems and slip past the very technology devoted to their detection. Because security technologies are often in multiple locations and poorly maintained, they can leave gaps and therefore miss evidence of potential threats. Skilled attackers consistently study commercially available intrusion detectors to learn how to bypass them, much like a sophisticated thief knows how to defeat home security systems. Finally, these intruders know how to burrow into networks through numerous entry points, whether by modem, PDA, computer, masquerading as another person, password cracking and more.

### **Interdependent Systems**

Until the rise of the Internet with its complex interlinking of networks, there was little need to worry about skilled attackers. Networks were isolated inside the organizations in which they were built. If there was an attack, it most likely came from an insider who was a skilled programmer working in the information systems department and often was contained within the enterprise. Controlling sophisticated attacks meant screening programmers thoroughly before hiring them and keeping an eye on them while they worked. Since the arrival of the Internet, skilled attacks can come from anywhere—and do. The nature of connected systems allows attacks to spread beyond single systems to suppliers. That is why several analysts advocate and stress the importance of an all-encompassing network security system. To discover and deter these intruders, all security detection systems and processes in an organization must work together.

### **Finding Real Incidents Within the Noise**

The open availability of attack scripts creates a volatile environment. As "would-be" hackers try these attack scripts, they collectively create a constant noise at detection points. The result is your firewall and IDS continuously identify security events that may or may not have significant intent. Several factors make detection difficult:

*Random Attacks*—Many attack scripts now begin to alter their execution so they do not follow a predictable pattern. The goal of these scripts is to evade sequential pattern signatures.

*Polymorphic Attacks*—Some new attacks randomize the internal contents of each packet as to not present a repeatable data pattern that can be matched. The goal of these scripts is to evade pattern recognition used within an individual transmission.



*Distributed Attacks*—Using the concept of a Trojan horse, remote control platforms enable attackers to use multiple methods—often not belonging to them—to execute an attack. The goal of these attacks is to distribute the sources of an attack, as to not arouse suspicion.

*Blended Attacks*—This type uses a variety of attack methodologies; several attack types may be combined to reach higher levels of compromise or wider distribution.

The common theme among new attacks is deception and evasion. In this never-ending battle between intruders and defenders, stopping skilled attackers requires new methods and technologies.

## Management Technologies

Management technologies have been around for some time. While much of their work has been around control, performance and availability, management systems have continued to expand in an attempt to address the issues of security management. Security management technologies can be classified into four levels. Two of these technologies are traditional, while the other two are emerging technologies seeking to solve the shortfalls of the earlier two. This paper introduces one of those new technologies: the Security Knowledge System.

**Point Security Management Systems** are vendor-specific tools that were built to manage and control a specific security product or set or product within a vendor suite. Providers of these systems are security technology providers of security hardware, appliances and software. These systems are often the best methodology to manage and control a specific product, as they are purposefully built to manage that product. Examples of these systems include Check Point™ Provider/1, Cisco Systems® Works and SonicWall® Global Management Solution.

**Enterprise Management Systems (EMS)** represent a long history of management products that seek to collect all information at a single place. Using network event protocols, they are able to monitor status and visually display results to the user. Specific capabilities include event filtering and forwarding to notify users. However, they often are restricted by the depth of information that is transmitted via event notification protocols, such as Simple Network Management Protocol (SNMP). Classic providers in this category are: IBM®'s Tivoli NetView, Computer Associates™ Unicenter, HP®'s OpenView, Micromuse®'s NetCool.

**Security Information Management (SIM)** systems provide scalable, flexible aggregation of security events from disparate products into a single location. Specific rules may be applied to inputs to reclassify the severity of alerts, producing accurate reports and reducing improper notification for vendor reported events that are actually a lesser priority. This is an emerging technology and is designed to help users manage their security technology investments. The focus, as in the other two cases, remains on the technology and live event information. Representative systems have been introduced by NetForensics®, eSecurity®, Symantec® and Check Point®.



**Security Knowledge Systems (SKS)** represent an innovative management technology that moves well beyond the technology focus of recent SIMs. While SIMs offer the best event aggregation today from live systems, they fail to match an SKS' ability to integrate the vulnerability management and business-level data that enable event classification. An SKS offers advanced correlation, which enables a higher-level analysis. This, in turn, works to greatly increase the accuracy of intrusion detection systems. Representative SKSs include offerings from PentaSafe® (recently acquired by NetIQ®), and RedSiren, which embeds its Security Knowledge System into their managed services. It is expected that SIM vendors will migrate over time to the SKS category, as their systems already lag behind the SKS' advanced correlation techniques.

A review of IDS technology in the June 24, 2002 issue of *Network World* characterized the problem more accurately than any article to date—mainly because it focused on the real-world testing and evaluation of capabilities:

*"By far the biggest problem was a huge number of false positives, with sensors sending alarms for insignificant events—or even worse, for vulnerabilities that didn't exist."*<sup>5</sup>

#### **Comparing Security Management Technologies**

The most effective solution—that which produces the highest level of defense—will carry the following five attributes:

*Alert Aggregation*—Given the number of reporting devices spread throughout a network, it is important to review all information to find the hidden attacker. Alert aggregation brings all events together in a common view.

*Vendor Independent*—Most network sensors come from a variety of vendors and security disciplines. In support of best-of-breed architectures, it is often necessary to integrate events between multiple manufacturers in the same discipline. This gives the customer freedom to address new technology outside of a single vendor.

*Advanced Correlation*—Multiple data feeds through event aggregation often place data on an even priority status by time of occurrence. Finding the attacker amongst the noise requires the ability to compare, sort and analyze data in several ways in near real-time.

*Posture Correlation*—Posture correlation helps to reduce false positives and takes intrusion detection technology to the highest level of nearly 100-percent accuracy. Using these systems, the incidents you respond to are the real ones. Furthermore, these systems use feedback loops to ensure that future incidents are avoided.

*Embedded Response*—Responding to incidents can be one of the more difficult tasks when maintaining computer security. Systems need to provide the necessary step-by-step data to resolve an incident.





---

<sup>5</sup> See "Crying wolf: False alarms hide attacks: Eight IDSs fail to impress during the month long test on a production network," by David Newman, Joel Snyder and Rodney Thayer, *Network World*, June 24, 2002.



As Figure 1 below shows, only the Security Knowledge System features all of these capabilities.

**Figure 1: Comparison of Security Systems**

	Alert Aggregation	Vendor Independent	Advanced Correlation	Posture Correlation	Embedded Response	
 Point Security Management	✓				✓	ISS Cisco Provider/1
 Enterprise Management System	✓	✓				Tivoli NetView CA Unicenter HP Openview/1
 Security Information Management	✓	✓			✓	Symantec SIM Tivoli Risk Manager
 <b>Security Knowledge System</b>	✓	✓	✓	✓	✓	<b>RedSiren</b>

### The Security Knowledge System: The Better Mousetrap

An SKS uses broad, cost-efficient monitoring and analysis to spot and stop network attacks coming through multiple connections. RedSiren security experts and other security professionals have learned that spotting a skilled intruder requires capturing data from many places in the enterprise and analyzing it in several ways to expose the individual or group. The SKS is especially adept at:

- Verifying the existence of intrusion
- Determining the rate of intrusion
- Identifying the intruder
- Identifying the behavior of the intruder
- Providing a situational assessment
- Producing an actionable threat analysis
- Identifying the information manipulated or stolen

Security Knowledge Systems use three levels to achieve these goals.

Level 1: Data Collection and Custom APIs

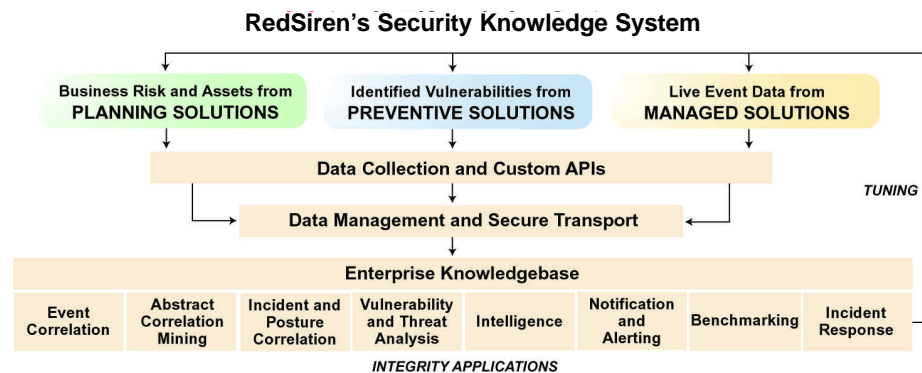
Level 2: Data Management and Secure Transport, which enable the system to safely collect information

Level 3: The Enterprise Knowledgebase, where information is united, analyzed and understood to produce knowledge





**Figure 2: Security Knowledge System Layers**



### Level 1: Data Collection and Custom APIs

Fully functional SKSs monitor and analyze multiple data sources from servers, routers and security products from logs that record data and information requests. These include:

- Firewalls and firewall logs
- Server transactions and server logs
- Web pages and Web server logs
- Host- and network-based intrusion detection products
- Wireless, synchronous servers and server logs for PDAs
- Computer operating systems
- Virus scanning software and scanning logs
- Access control systems

Security Knowledge Systems normalize inbound alert data into a common context. Normalized events are matched and indexed to the knowledgebase. In this way, an event from an ISS sensor can be compared to an event sent by a Cisco router.

Large amounts of security information are securely collected as a first step. While reporting methodologies and protocols vary by vendor and equipment type, the SKS must collect the data from each source. It also must be tuned to collect data that will later aid diagnosis. Custom application programming interfaces (API) are used to support multiple protocols that range from text logs to XML to SNMP traps.

Optimal and accurate SKSs capture two data types in addition to logs and events: Vulnerability Data and Business Data. These additional elements empower additional correlation levels and enable active threat/priority analyses, as the significance of a target is understood within the context of its importance to business processes.

### Level 2: Data Management and Secure Transport

Collecting control flow and detail-level data requires a manageable retrieval mechanism and data preparation. Several of the solutions, such as point security management, do not have the ability to interpret a myriad of data formats and communication methods; therefore, they cannot perform higher levels of interpretation. The SKS, on the other hand, normalizes the inbound alert data to bring it into a common context. Normalized events are matched and indexed to the knowledgebase. In this way, an event from an ISS sensor can be compared to an event sent by a Cisco router.



### **Level 3: Enterprise Knowledgebase**

In this level, information is united, analyzed and understood to produce knowledge. Correlation is the process of combining and comparing two or more data points to arrive at a conclusion. To spot a handful of meaningful serious events in a mountain of data, SKSs use correlation algorithms. The SKS may invoke several types of correlation, including:

- *Time-Based Correlation*, which groups and presents events in relative time order, as many systems are not synchronized. This phase allows sequence analysis.
- *Event Correlation*, which groups events in time from multiple sensor points to validate point of entry.
- *Source Correlation*, which groups origins of attack in time to evaluate serious attack intent and method of attack.

Many more exist and many are the proprietary property of the managed service vendor or SKS vendor. These steps can be combined and are often used as pre-stage elements to Data Mining.

### **The Importance of Data Mining**

Extracting knowledge and understanding information requires custom-built Knowledge Management Infrastructure (KMI). The KMI relies upon several key elements to enable mining and detection of evasive intruders. These include several relational databases that allow multidimensional scenarios to be built upon demand.

Data mining enables businesses to determine trends within their database. This is important because systems that report the same information that security products detect are inherently limited. Such systems see only what detectors see and cannot see what detectors miss. Only data mining can peel away layers to look more deeply by relating various aspects of stored data.

In data mining, network security analysts apply a battery of analytic techniques to look for both simple and complex relationships that will expose attacks. Among the tools they use are:

- Predictive modeling using statistical techniques and neural networks
- Data classification and clustering using decision trees and rules
- Exploration using decision trees and OLAP tools
- Affinity analysis using associations, time-based sequences, frequency, factor and link analyses between code segments

Due to the complexity of these analyses, most of the data mining work is done offline on defined data sets. Only a small amount of adaptive data mining is performed on real-time data. And since finding relationships among millions of transactions requires visualization, graphs, charts and alerts tell analysts the state of the network and the existence of network attacks. When they spot anomalies, analysts drill down into the data and examine it in detail.



### **Building Knowledge**

SKSs gain in effectiveness over time. As they identify attacks and attack signatures, they store them in a growing threat and vulnerabilities database. In the best circumstances, the database captures threats from all sources, as well as from other networks, so attackers who roam from network to network can be spotted and stopped quickly. Furthermore, as threats are identified and evaluated, network security analysts use this knowledge to reconfigure data collectors and sensors to determine the level of organizational threat. As a result, an organization can actually prevent a breach, rather than just react to system damage.

### **Deploying Security Management**

Achieving the benefits of accurate and rapid detection of security incidents may be approached in several ways, from internal development to product licensure. Clients who wish to build their own Security Knowledge System will most likely find it cost prohibitive and minimally effective. The cost to develop an SKS internally typically runs from \$8 to \$10 million.

When considering implementing a security management system, one should examine the following points:

**System Expense**—System expense varies based on whether the system is deployed internally under licensure, developed internally or included as part of a managed service. *Note: Not all managed service providers have SKS capability. Most are using EMS or homegrown SIM functionality.*

**Staffing or Service**—Gartner Group and Forrester Research estimate that the minimum start-up plus first-year costs of building an incident response team to provide 24x7x365 protection can range from \$450,000 to \$750,000, respectively. Managed service providers offer substantially reduced costs, as the provider can distribute customers across staff. For large organizations, these will equalize as a single, large customer optimizes an entire shift. Extremely low service costs are often signs of Alert Forwarding services.

**Knowledge Sources**—Knowledge systems benefit and grow through greater access to data points. As a managed service, the number of sources is significantly larger, allowing earlier warning and prediction. This results in greater accuracy and faster response. Customer-implemented systems have the benefit of only one source.

**Accuracy and Speed**—The value of outsourcing is reflected in the accuracy and speed of response. In the electronic world, where minutes can cost millions of dollars, high capability should be desirable for all enterprises, as it is the most economical.

**Knowledge Build**—The time to build knowledge is fastest in the case of the managed service model using an SKS. The lessons learned in one system are easily applied to other systems. Likewise, the customer begins service at a higher level. In the case of all others, the deficiencies and lack of knowledge management inhibit rapid growth.



**Figure 3: Comparative Impact of Various Solutions**

	System Expense	Staffing or Service	Knowledge Sources	Accuracy and Speed	Knowledge Build
Customer Enterprise Internal Development	\$\$\$	\$\$\$	1	Fair	Slow
Customer Enterprise with SKS Vendor	\$\$	\$\$\$	1	Fair	Slow
Customer Enterprise EMS Vendor	NA	\$\$\$	NA	Low	NA
<b>Managed Provider with SKS Bundled</b>	<b>Included</b>	<b>\$\$</b>	<b>Many</b>	<b>Best</b>	<b>Best</b>
Managed Provider with Alert Forwarding	NA	\$	NA	Low	NA

## Conclusion

To be successful, enterprises must keep pace with the rapid appearance of vulnerabilities and deployment of attacks. Sifting through constant attack noise requires the advanced technology that can only be delivered through an SKS. Simply stated, an SKS offers enterprises futuristic business protection capabilities—today.

To restate, the important points to remember are:

- Threats to information integrity are constantly changing and require continuous investment, vigilance and management.
- Information security will continue to fail as long as security technology and service activities are coordinated independently.
- Traditional vendor management solutions and enterprise management systems are incapable of bringing the entire security picture together.
- SIMs systems fall short of what is truly needed to deliver information integrity.
- SKSs define a higher order of service and ability that shall become critical to mitigate new threats and continuously improve operations.
- Outsourcing security management to an MSSP that utilizes a security knowledge system offers the best return on investment across costs, security and value.



Only RedSiren has a complete Security Knowledge System. Our unique SKS is embedded into our Managed Solutions. This eliminates the high expense of software licensure, as well as the high cost of staffing the management and monitoring of the system. It also eliminates delays in activating the system or in collecting intelligence that results from mining the activity and knowledge of multiple customers. As a result, our SKS far exceeds any other capability from traditional management vendors that offer partial implementations that are restricted by service, limited to particular vendors or lacking interpretation. For more information, visit [www.redsiren.com](http://www.redsiren.com).

### About the Author

Darwin Herdman joined RedSiren in June 2002 as the result of its Veritect acquisition and is responsible for the vision and continued evolution of RedSiren's advanced technology solutions. His extensive operational experience and valued lessons learned in the field of information security have played a critical role in the development of RedSiren's highly reliable and scalable managed security services offering. Prior to joining Veritect as a member of the original executive team in 1999, Mr. Herdman managed Veridian Corporation's Applied Technology organization focused on the research, design and development of next generation security focused technologies and solutions for Department of Defense and federal government customers, including numerous CINCs, Services and Agencies. Mr. Herdman has a masters degree in Interdisciplinary Applied Mathematics and is an active member of numerous information security organizations and working groups.

### About RedSiren

RedSiren, the world's largest privately held provider of IT security management, empowers its customers to reduce and manage their business risks, every hour of every day. Backed by industry-leading security knowledge technologies and seasoned security professionals, RedSiren delivers superior customer service and advanced managed solutions to more than 800 mid-tier and Global 1000 companies. Headquartered in Pittsburgh, Pennsylvania, the company is a valued security resource for planning, preventive and managed solutions, including security awareness education, which it delivers through its Information Security University™ (InfoSecU™). RedSiren manages and provides security-related thought leadership and research for the International Information Integrity Institute® (I-4®). The company maintains strategic relationships with security hardware and software vendors, the CERT® Coordination Center (CERT/CC), the FBI's InfraGard initiative, SRI International and the Information Security Alliance.

To learn how RedSiren can help your company achieve a higher level of security, call us today at 1-877-360-7602.

**RedSiren**  
Centre City Tower  
650 Smithfield Street, Suite 900  
Pittsburgh, PA 15222 USA  
[info@redsiren.com](mailto:info@redsiren.com)

**t: 1.877.360.7602**  
**t: 1.412.281.4427**  
**f: 1.412.434.1264**  
**[www.redsiren.com](http://www.redsiren.com)**