Research Brief

Aberdeen Group
A Harte-Hanks Company

March 2008

The Role of Security Information and Event Management (SIEM) in Security Governance, Risk Management, and Compliance (GRC)

Organizations of all sizes are compelled to demonstrate compliance with industry regulations, government regulations, industry standards and best practices, or internal policies related to information security. By more effectively allocating their IT resources for these activities based on business objectives and acceptable levels of risk, Aberdeen research has shown that organizations with top performance improve security, sustain compliance, improve leverage from existing IT resources, make faster decisions, and optimize business processes. In this Research Brief, additional analysis reveals that current users of Security Information and Event Management (SIEM) solutions exhibit superior capabilities in security Governance, Risk management and Compliance (GRC).

Current SIEM Users Exhibit Superior Capabilities

Aberdeen research has consistently shown that compliance, taken in all its dimensions, continues to be a leading driver of investments in information security. Although their capabilities are still developing, in our research on *Security Governance and Risk Management* (November 2007) we have seen clear evidence that companies with top performance are taking proactive steps to ensure that their investments in security and compliance controls directly support their strategic objectives for the business. Policies, as the explicit expression of their business objectives and their appetite for risk, provide the foundation for the most effective security GRC programs.

But policies without actions are dead. Many organizations are leveraging SIEM solutions to track, analyze, and manage how the requirements expressed by their policies are (or are not) being satisfied, and to drive appropriate actions and behavior by the relevant stakeholders. Our research shows that current SIEM users are in fact achieving superior results in security GRC.

As part of its benchmark process, Aberdeen analyzes the aggregated responses of all companies surveyed to determine whether their performance ranks as Best-in-Class (top 20%), Industry Average (middle 50%), or Laggard (bottom 30%). In addition to having common levels of performance, each maturity class also shares common characteristics with respect to current capabilities in the following areas:

- Process – the approaches taken to execute daily operations
- Organization – corporate focus on the topic, and collaboration among stakeholders

Research Brief

Aberdeen Research Briefs provide a more focused look at the principal findings derived from primary research, including key performance indicators, Best-in-Class insights, and vendor insights

Fast Facts

Compared to the Industry Average, the research shows that current SIEM users rate their performance:

√ **15% higher** at prioritizing security and compliance-related investments based on defined business objectives and acceptable levels of risk

√ **11% higher** at speed of decision-making regarding security governance, risk management, and compliance

√ **18% higher** at optimizing business processes related to security governance, risk management, and compliance

www.aberdeen.com

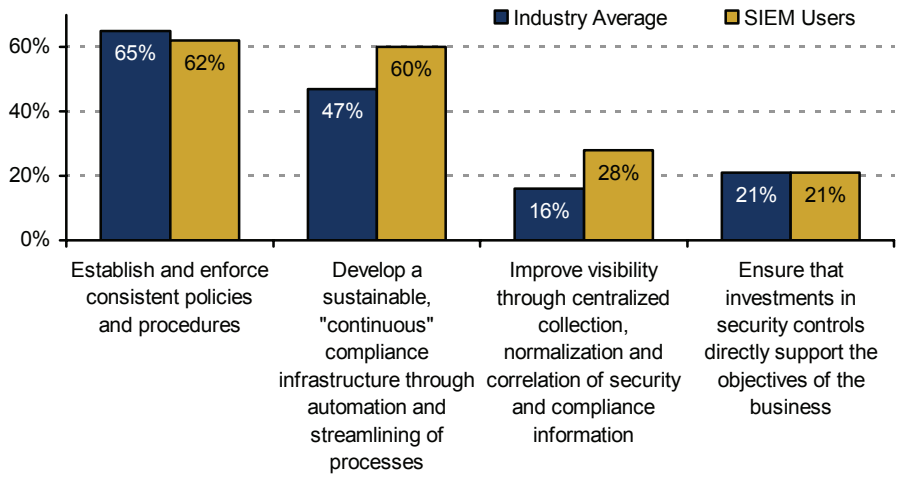
Telephone: 617 723 7890
Fax: 617 723 7897

- Knowledge management – putting data in context, and exposing it to key stakeholders
- Technology – the selection of appropriate tools, and the effective deployment of those tools
- Performance management – the ability of the organization to measure results as a means to improve the business

These characteristics serve as a guideline for best practices, and correlate directly with Best-in-Class performance. An analysis of current users of SIEM solutions shows that **SIEM users exhibit superior capabilities in all five of these categories**.

In Figure 1 we see that compared to the Industry Average, current SIEM users are more committed to a strategy of automating and streamlining processes to develop a sustainable, "continuous" compliance infrastructure. In addition, current SIEM users are 75% more likely to make investments around the strategic objective of improving visibility through the centralized collection, normalization, and correlation of security and compliance information.

Figure 1: Leading Strategies Driving Current Investments in Security GRC Initiatives

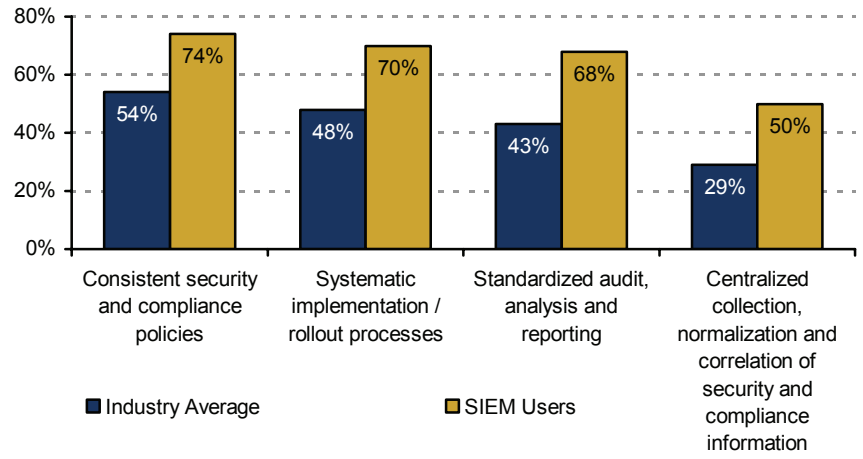


Source: Aberdeen Group, November 2007

While current SIEM users are comparable to the Industry Average in identifying the need to "establish and enforce consistent policies" as their top strategic objective, they are distinctly better at actually implementing it. As shown in Figure 2, SIEM users report more consistent policies (74% versus 54%); more systematic implementation (70% versus 48%); and more standardized audit, analysis, and reporting (68% versus 43%). Not surprisingly, SIEM users are also more effective (50% versus 29%) at achieving their strategic objective of centralized collection, normalization, and correlation of security and compliance information and events.

Aberdeen Group
A Harte-Hanks Company

Figure 2: Current Capabilities (Process)



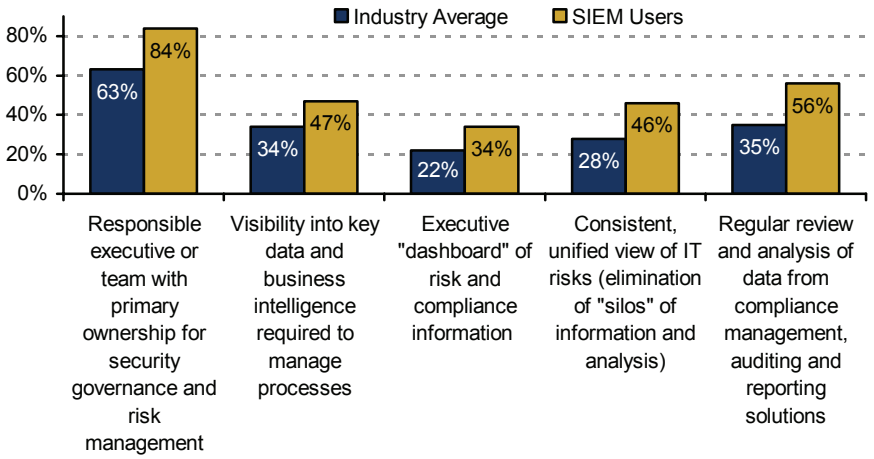
Source: Aberdeen Group, November 2007

"Our initial focus was on building, not on measuring ... but now that we have built the workflow, we can look at more than ever before, and take action faster."

~ Senior Manager, Network Security Engineering Leading Cable, Content and Communications Provider

If the goal of SIEM solutions is to create "actionable" intelligence for security and compliance, Figure 3 illustrates that current SIEM users are in fact better organized to monitor, trigger, and communicate the appropriate actions required to ensure continuous compliance with policy. Worthy of note, 84% of current SIEM users have identified an executive or team with primary ownership and accountability for security GRC – an important capability, given that responsibility for remediation often falls across disparate network, security, and operations teams.

Figure 3: Current Capabilities (Organization and Knowledge)



Source: Aberdeen Group, November 2007

"The data is there now to measure our key performance indicators, and to quantify how we are reducing our risk."

~ Senior Manager, Network Security Engineering Leading Cable, Content and Communications Provider

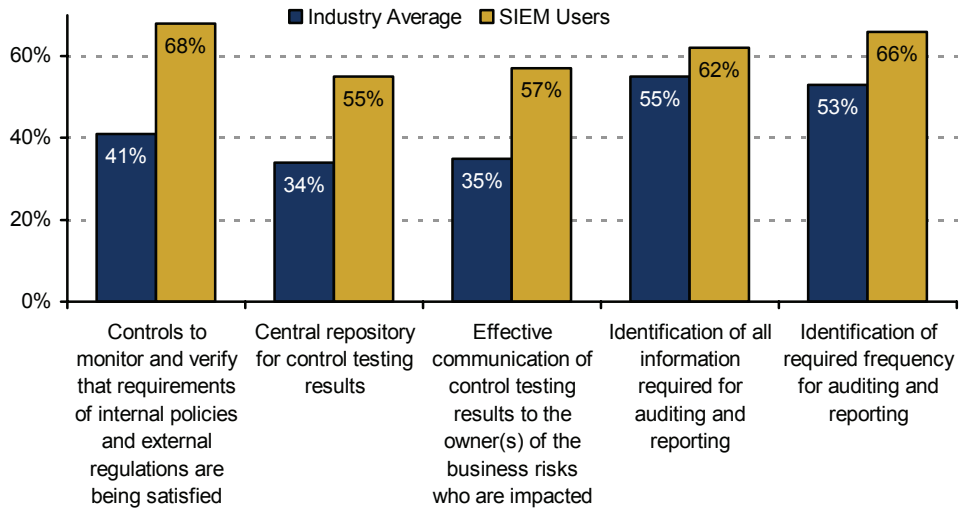
As shown in Figure 4, SIEM users also:

- Exhibit superior use of technical controls to monitor and verify that policy requirements are being met (68% versus 41%)

- Store control testing results centrally for mining and analysis (55% versus 34%)
- Communicate results more effectively to the owners of the business risks who are impacted (57% versus 35%)

Finally, SIEM users are more likely to have identified the type and frequency of information required for auditing and reporting. Finding out what they like and how they like it, and giving it to them just that way, is always a sound approach to satisfying key stakeholders.

Figure 4: Current Capabilities (Technology and Performance)



Source: Aberdeen Group, November 2007

"Sometimes, it's more difficult to agree on the management and reporting aspects of the solution than on the technological implementation."

~ Senior Manager, Network Security Engineering
Leading Cable, Content and Communications Provider

Case in Point

Take, for example, the case of a leading national provider of cable, content and communications products and services, serving more than 20 million cable customers, more than 10 million high-speed Internet customers, and nearly 5 million digital voice customers in 39 states. With the majority of its services being Internet-facing, the company sees a continuous stream of security-related issues that potentially impede the availability and reliable delivery of real-time services to its subscribers. "Our primary focus is service delivery," comments the company's Senior Manager for Network Security Engineering. "We're responsible for the availability and reliable delivery of voice, video, and data services – if we're not doing our jobs, you're not getting your service."

Before their implementation of a SIEM solution, the company had numerous tools and multiple solutions, "but we were spending too much time managing multiple systems. We didn't have a tool that did normalization, and we were able to do virtually no correlation of information and events. The data was there; we just couldn't look at it because it just wasn't feasible in a timely way."

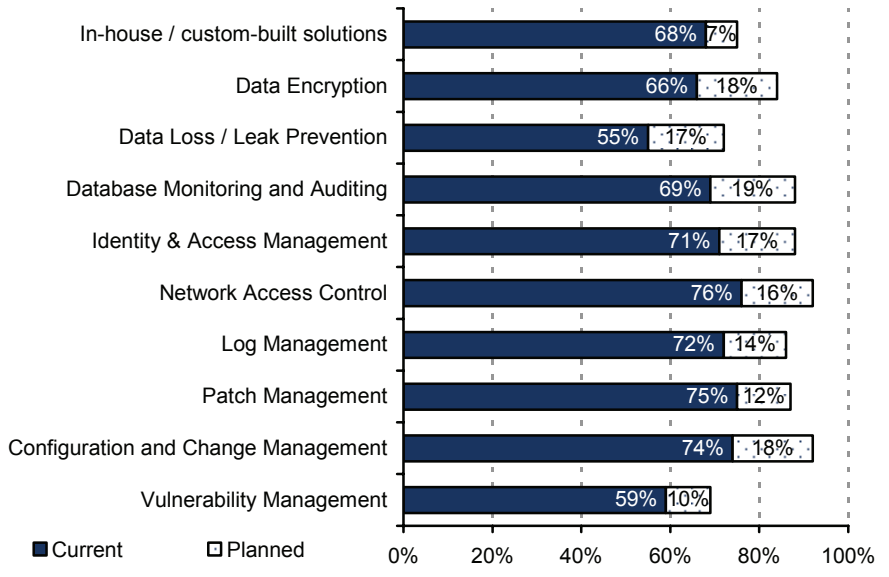
Today, a common information and event management system enables the company's operators to manage out of a single view, across multiple shifts and 24x7 coverage. "In our operational philosophy, what's key is that the operator should be presented with every piece of information they need to understand, analyze, and respond to issues," he notes. "In the past, they would have to go into two or three different systems, and the time it took to go from detection to mitigation could be several minutes – by then it's too late. Now, it's within seconds."

Widening the Scope of Applications Supported by SIEM

Most companies have already deployed a diverse suite of technologies in support of their security and compliance initiatives, as shown repeatedly in Aberdeen's security research. A growing portfolio of tactical, project-oriented point solutions has typically meant that organizations must absorb the operational inefficiencies of integrating and managing a hodge-podge of discrete systems – or leave them for the most part to be managed separately within their respective silos. To address this issue, leading SIEM solution providers are building out a "platform" or "ecosystem" approach, starting with a consistent architecture to facilitate integration and interoperability for collection, archival, correlation, analysis, monitoring, auditing, and reporting on security and compliance-related data. This approach is consistent with the Best-in-Class view of security GRC as a strategic, sustainable program, as opposed to a series of one-time events.

Analysis of current SIEM users shows that they are also supporting a wide variety of IT security solutions, as illustrated in Figure 5. This creates a premium for SIEM solution providers that can integrate easily with security information and events from disparate data sources.

Figure 5: Use of Other Security Solutions by Current SIEM Users



Source: Aberdeen Group, November 2007

"Integration is key. We selected a SIEM system that is open and extensible, and from this point forward we will select and deploy new selected solutions that are easily integrated."

~ Senior Manager, Network Security Engineering
Leading Cable, Content and Communications Provider

Physical security infrastructures are also an important source of security information and events, as detailed in Aberdeen's *Logical / Physical Security Convergence: Is it in the Cards?* benchmark report (December 2007). That research shows that by collecting and correlating information and events from both logical security and physical security infrastructures, companies improve overall management visibility and progress towards a common, enterprise-wide view of risk.

Solutions Landscape

An illustrative list of leading SIEM solution providers is compiled in Table 1.

Table 1: SIEM Solutions Landscape (illustrative)

Company	Solution(s)	Description
Intellitactics www.intellitactics.com	Intellitactics SAFE Intellitactics ISM Intellitactics SAM Intellitactics Advanced Analytics	Intellitactics parses, normalizes and stores logs collected from any device or data source and offers these capabilities on an appliance (SAFE) or as a software product (ISM). Users retrieve, view, and report on raw and parsed logs, events and alerts to investigate and then act on threats, breaches and policy violations to decrease security- and compliance-related incidents. Intellitactics SAM displays key performance indicators (metrics) on a configurable management dashboard; Advanced Analytics provides data mining and advanced threat detection.
RSA, The Security Division of EMC www.rsa.com	RSA enVision	RSA enVision collects and protects data from any IP device without filtering and without the need to deploy agents. Comprehensive management and analysis capabilities help transform security information and event data into actionable intelligence for security and compliance.
ArcSight www.arcsight.com	ArcSight ESM ArcSight Logger	ArcSight ESM centrally collects and analyzes events from devices, systems and applications across the enterprise. The ArcSight ESM console provides comprehensive, real-time information analysis and remediation capabilities to help organizations discover risks, correlate relevant information, assess vulnerabilities and communicate with stakeholders. ArcSight Logger is a turnkey appliance which captures and analyzes enterprise log data, acting as a universal event log repository and hub within a broader system.
eIQnetworks www.eiqnetworks.com	SecureVue	SecureVue is an integrated platform that combines enterprise security management (ESM) and IT governance, risk management and compliance (GRC) to detect security breaches, speed remediation, and support best practices and regulatory requirements. SecureVue collects, correlates, archives, analyzes and reports on critical security and compliance data, transforming volumes of log, vulnerability, configuration, asset, performance and network behavioral anomaly data into actionable intelligence. A comprehensive compliance library maps directly to specific regulations, best practices and standards.
netForensics www.netforensics.com	nFX SIM One nFX Data One nFX Log One	nFX SIM One helps to transform large volumes of complex security-related data into understandable, actionable information to respond to security events in real time. nFX Data One protects against data breaches by monitoring databases and applications and alerting on any hostile and unauthorized activity. nFX Log One delivers automated, easy-to-use log management for collecting, documenting, and storing log data for compliance audits.

Company	Solution(s)	Description
Symantec www.symantec.com	Security Information Manager	Symantec Security Information Manager provides the foundation for automating the continuous monitoring of IT controls and helps organizations to identify, prioritize, and respond to incidents and threats as part of a comprehensive incident response program. By automating this multi-discipline process, organizations can assure that critical assets are monitored, prove due care as part of a policy-based compliance program, and establish a documented and repeatable process for measuring, responding to and reporting on IT risks.

Source: Aberdeen Group, March 2008

Summary and Recommendations

The role of SIEM solutions in security GRC comes down to creating an active, continuous, self-adjusting linkage between policy and behavior:

- GRC is based on policy, which is the expression of the organization's business objectives as their view of the optimal balance between protection, compliance, and profit.
- SIEM solutions provide the link between policy and behavior, in the tracking, analysis, and management of how a company does (or does not) satisfy the requirements expressed by policy.

In practical terms, the typical starting point is a collection of existing implementations of specific security controls. SIEM solutions can then provide centralized integration, analysis, and prioritization of behavior based on policy. Best practice is to establish policy to address a specific problem, then to generalize the policies and expand security GRC initiatives incrementally over time.

For more information on this or other research topics, please visit www.aberdeen.com.

Vendor Checklist

Items to consider when evaluating SIEM vendors include:

√ Ease of collecting and correlating information and events from a wide variety of data sources

√ Solutions should address a specific problem today, leveraging the controls and information already in place

√ Architectures should provide flexibility from which to address additional problems over time

Related Research	
Trusted Computing; February 2008 *Logical / Physical Security Convergence*; December 2007	*Security Governance and Risk Management*; November 2007 *Sustaining Compliance*; September 2007

Author: Derek E. Brink, Vice President and Research Director, IT Security (Derek.Brink@aberdeen.com)