



>
accenture

High performance. Delivered.

An Enterprise View: Comprehensive Security Information & Event Management Solutions

• Consulting • Technology • Outsourcing

Modern corporations are faced with increasingly complex compliance and regulatory demands that require them to respond quickly and effectively to any information security incidents. Many organizations are unprepared to meet compliance targets due to the many challenges of navigating through compliance laws and interpreting those laws into meaningful technology solutions.

Now specialized assistance is available on an enterprise scale. From a monitoring and management perspective, an effective Security Information & Event Management (SIEM) capability allows organizations to identify and remediate potential security threats across the enterprise.

Business challenges

Compliance and regulatory requirements are placing growing demands on the enterprise to effectively monitor, detect, report and respond not only to new security threats but also to existing vulnerabilities in corporate IT systems and applications. The challenges being faced can be summarized into three categories:

Technology

- Growing size of security logs and events within a heterogeneous environment
- Lack of a holistic view of user behavior and cross-correlation of security events

Process

- Compliance with log retention, monitoring and storage requirements from relevant regulations
- Lack of defined escalation procedures and governance structure which is important to an overall security strategy

Organization

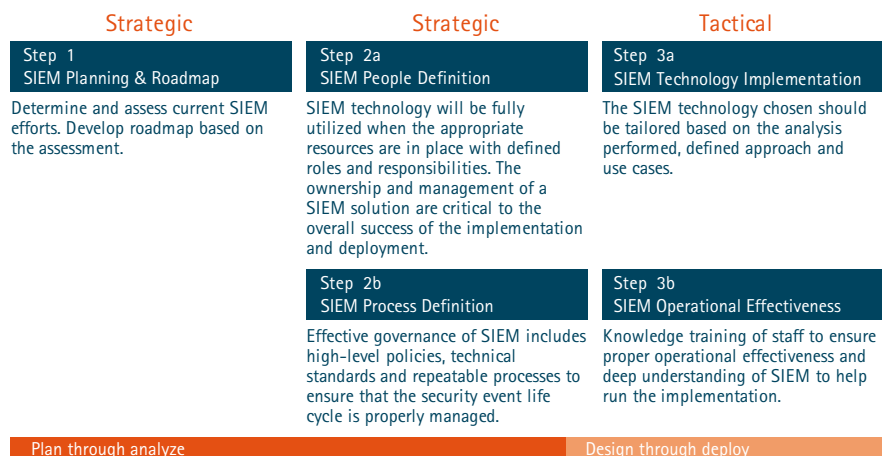
- Staff not properly trained to assess and respond to security events
- Integrating effective communication within various capabilities across the organization

Accenture's approach

Accenture helps enterprises in complex environments reframe the way they think about information security. Most organizations have the tendency to view information security as solely an IT issue. Accenture's experience has shown that high-performing organizations look at security holistically and as a responsibility of all areas of the organization, from a strategic, business-value-oriented level to the technical level. Accenture has developed a distinctive, well-defined and reusable methodology that helps clients determine a comprehensive approach to information security that increases

the value to both their business and IT functions.

Delivering scale, experience and a diverse knowledge base with a global footprint, Accenture provides a comprehensive set of end-to-end SIEM services. With the evolution of SIEM as a consolidated solution for security information and event management, Accenture's approach can assist organizations to better identify threats, simplify administration, perform analysis and respond to suspicious activity:



Success story: Deploying an effective SIEM solution within a retail environment

A good example of high performance in action is Accenture's work to help retail clients adhere to the Payment Card Industry Data Security Standards (PCI DSS). These standards are put in place to require organizations with large retail operations lead the industry in the rigorous protection of personally identifiable information by providing a set of defined security requirements. PCI DSS Requirement 10, which requires the monitoring and tracking of all access to network resources and cardholder data, can be addressed with a comprehensive and customized SIEM solution.

Challenges and Key Considerations

Challenges presented with monitoring retail store activity are far from intuitive, and there are many considerations to take into account in order to effectively monitor retail store activity.

One of the main challenges of retail monitoring is how to architect a solution in an effective manner while minimizing costs. Key considerations include collecting, processing and retaining logs. Additional considerations include investment in proactive security, architectural best practices, availability, reliability and overall support cost.

Solution

Accenture's SIEM capabilities help organizations tackle the often-daunting challenge of monitoring the entire enterprise. Our solution reduces the complexity of SIEM, breaking the process down into three simple steps: collection, delivery and analysis.

This three-step process enables Accenture to effectively determine the best architecture to meet an organization's technology environment needs. Further, this process helps define the most appropriate method for collecting, delivery and processing security logs using the appropriate SIEM technology, while minimizing infrastructure resource utilization and limiting bandwidth utilization on the WAN.

High Performance Results

As an integral part of business, a vast majority of organizations are both custodians and brokers of data or information. In these roles, they must also protect the integrity and availability of information systems. The need for mature SIEM services is common across all industries. From regulatory compliance and IT governance to real-time information analysis and overall security best practices, organizations are interested in implementing SIEM solutions that can help reduce the cost associated with log management. Accenture's deep SIEM skills and experience provide clients with the flexibility as well as the capability to plan and implement the solution in a variety of ways.

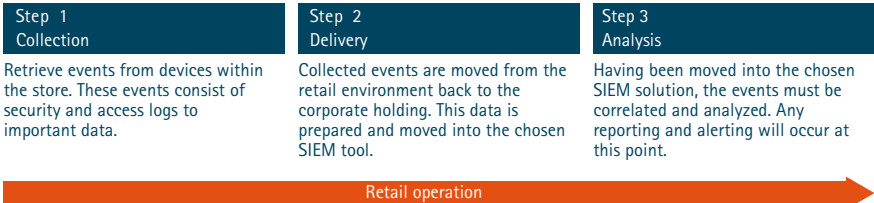
Depending on an organization's needs, Accenture can implement an enterprise SIEM solution as a stand-alone solution (leveraging Accenture's proven delivery methodology) or through its partnerships with leading SIEM vendors. Implementing a SIEM solution has several significant benefits from an IT perspective:

- Improve monitoring effectiveness and efficiency,

- Clarify ownership—establish a clear chain of custody to improve compliance with regulations and standards,
- Centralize the administration and monitoring of multiple components via a single management console, and

SIEM also provides important business value:

- Reduces operational costs associated with compliance monitoring and incident handling
- Helps improve investigations and compliance with regulatory standards
- Helps improve overall security capability within an organization
- Better the ability to understand threat impacts across the organization
- Facilitates a faster response to security incidents due to clear roles and responsibilities within a defined governance structure



Contact

To discuss how your company can benefit from Accenture's Security Information & Event Management services, contact:

G. Christopher Hall
g.c.hall@accenture.com
Security Risk Management Offering Lead

Paul M. Barsamian
paul.m.barsamian@accenture.com
Security Infrastructure & Operations

Yemi B. Saka
yemi.b.saka@accenture.com
SIEM Program Lead

Copyright © 2007 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills and technologies to help clients improve their performance. With approximately 170,000 people in 49 countries, the company generated net revenues of US\$19.70 billion for the fiscal year ended Aug. 31, 2007. Its home page is www.accenture.com.

About Accenture Technology Consulting

Accenture Technology Consulting helps our clients transform their IT to better support a high performing business or government department. With more than 4000 technology consulting experts worldwide, we bring our clients innovative, market-relevant and industrialized technology consulting solutions that enable them to:

- Facilitate business growth by linking IT strategy and technology solutions to business strategy
- Reduce complexity and cost across all layers of the IT Infrastructure to help fund future IT growth and innovation
- Secure mission critical data and information
- Improve employee productivity

For more information on Accenture Technology Consulting, go to:
www.accenture.com/atc

