Security and Identity Management Auditing Converge

Earl L. Perkins, Mark Nicolett, Ant Allan, Jay Heiser, Neil MacDonald, Amrit T. Williams, Ray Wagner, Roberta J. Witty

Security information and event management (SIEM), as well as identity and access management (IAM), have required different information security approaches. Indeed, implementing and maintaining systems for them have often been run first as separate projects, then as separate services by different organizations. However, they are integrating at their respective functional layers for auditing. Compliance efforts are the major catalyst driving them together. Clients can prepare for this integration by evaluating common audit needs of their enterprise from those systems.

This document outlines the case for planning the future of IT security auditing in IAM and SIEM together. There are synergies to be realized in the way auditing works together and, hence, opportunities to save time, money and effort when deploying the tools that support those approaches.

Key Findings

- Don't expect SIEM audit solutions to be a replacement for detailed IAM audit solutions. Robust SIEM logging and reporting are often addressed in the aftermath of audit results, and identity and access audit needs are often already in place.

- Don't expect IAM audit solutions to be a replacement for SIEM audit solutions either. They are focused primarily on identity-centric events and do not include the effective handling of IT-environment-based events. Consider them necessary but insufficient to a SIEM audit strategy;

- SIEM provides visibility into resource access attempts that are not normally visible to IAM audit functions. For example, SIEM would capture a root login by a privileged system user, followed by access to sensitive resources. An IAM audit function may not capture such an access because IAM audit functions focus on administrative changes that are made through IAM or enterprise directory interfaces.

- SIEM solutions (to be effective in regulatory compliance monitoring) need the user and resource context provided by IAM, and they need IAM policies as a reference point for monitoring.

Predictions

- Short term (2005 and 2006) — Expect detailed audit log and reporting capabilities of IAM products and services to be crucial, particularly as a result of regulatory compliance concerns.
• Long term (2006 through 2008) — For innovative enterprises, prepare for integration with SIEM product implementation or initiatives, resulting in the ability to view IAM audit logs in conjunction with other SIEM logs for a holistic view across IT security systems. This will result in a new level of detail in forensic detection because of the combination of identity and environment events.

Recommendations

• Incorporate IAM context into SIEM approaches (for example, regulatory compliance data collection, analysis and reporting). Expect the need to customize some SIEM filtering, correlation and reporting functions as a result of the methods and variety of IAM requirements for collection.

• The audit implications of compliance ensure that high record levels will be required to correlate real people with real events. This will be true for forensic investigations in IAM long after compliance is not a priority.

• Establish a three-year deployment planning horizon beginning in 2006, with process re-engineering resources required first to map out a converged view of potential common collection sources, collection points and reporting. This is followed by a skills set inventory for use in training and organizational preparation necessary to support common audit infrastructure. This will include IT operations among other teams.

• Expect an additional 3 percent to 5 percent across IAM and SIEM budgets during the first year for labor and possible tools to initiate audit convergence. New investment in SIEM capabilities may also be needed, after basic IAM auditing is in place. The investment will be partially recovered as process and organizational efficiencies are realized, but a substantial portion of the SIEM investment must be positioned as necessary to improve operational monitoring capabilities.

• Long term, some IT organizations can expect to move to a centralized audit repository for IAM and SIEM for event logs for simplified reporting and forensics, as some technology providers are already offering early editions of tools that support such an environment. This will depend on the infrastructure distribution of event logs and the ultimate organizational structures charged with the responsibility of managing and using them.
TABLE OF CONTENTS

1.0 IT Security Auditing .............................................................................................................. 4
   1.1 Current State: SIEM Auditing .................................................................................. 4
   1.2 Current State: IAM Auditing..................................................................................... 5
2.0 Issues ................................................................................................................................... 6
   2.1 Issues for Clients..................................................................................................... 6
   2.2 Issues for Technology and Solution Providers ......................................................... 6
3.0 Bottom Line........................................................................................................................... 7

LIST OF FIGURES

Figure 1. IT Security Audit Process ............................................................................................ 4
1.0 IT Security Auditing

A formal definition of the IT security auditing approach has been established (see Figure 1 and Note 1), and there have been a number of product and service attempts at implementing elements of IT security auditing in IAM and SIEM, with varying degrees of success. While IAM and SIEM tools may share common scan and collection approaches to data, the evaluation criteria for data capture, the application of security policy as demanded by controls for that criteria, the nature of the data collected and the organizations managing the environments can vary today. While SIEM monitoring and audit tools, for example, may focus on recording real-time network events and may offer immediate analysis and alerting for some event time, IAM audit tools frequently exhibit more security information management (SIM) characteristics of storing information for reporting for later historical analysis and forensics.

Figure 1. IT Security Audit Process

Source: International Organization for Standardization (ISO)

1.1 Current State: SIEM Auditing

SIEM is a combination of real-time collection, correlation and response to IT-environment-type security events as well as a heavily indexed, long-term repository optimized for query and reporting of security events.

Significant SIEM product deployments are limited to the largest organizations today. Much of the technology required for a generalized, automated audit using output from a SIEM implementation is not available to most enterprises. However, many clients have used SIEM technology solutions
for host and directory server log monitoring, customizing their own SIEM correlation rules and developing reports to meet compliance mandates.

More and more clients are using log monitoring capabilities of SIEM as a component of a regulatory compliance program. In this use case, IAM-type activity is aggregated and analyzed from such sources as:

- Microsoft Active Directory, Novell eDirectory and other directory server logs
- IAM product logs
- Server system activity logs
- Security configuration policy compliance data
- Application logs (most recent additions)

SIEM technology and solution providers are developing initial audit offerings with pre-defined correlation rules and reports for IAM-related events targeted for regulatory compliance. Application layer IAM-type monitoring is nascent but growing (for example, SenSage integration with Cerner medical applications for Health Insurance Portability and Accountability Act [HIPAA] compliance reporting). Tools are also focusing specifically on event and data analysis capabilities for server and application IAM and security configuration policy compliance where applicable.

1.2 Current State: IAM Auditing

In IAM, auditing, logging and reporting functionality as a direct response to regulatory compliance have become the most-significant areas of technology provider improvements over the last 18 months. A primary aim of IAM auditing remains consolidating information about resource access attempts and user administration changes material to regulatory compliance. This is supplemented with the audit capabilities of the audit functions of the IAM products themselves. These functions of innovative technology provider offerings include:

- Simple configuration views
- Flexible, multilayered reporting formats
- Automated and scheduled policy scans
- Automated and scheduled IT control scans
- Notification of violations
- Attestation review and approvals
- Integrated logging (with heterogeneous event logs)
- Identity data correlation with vulnerability management event data

For regulatory compliance, areas such as event tracking include but are not limited to the following events:

- Account creations, modifications and removals, including who approved the request for access and why
- Administrative changes that affect permissions and protections for specific resources
- Privilege escalations
• Normal logins, logouts, dates and times
• Failed login attempts
• Failed resource access attempts
• Inclusion of users into specific groups
• Password resets made from password console tools and target platform environments
• Long-term linked password history, a record of access uses

Key areas of SIEM and IAM overlap include identity audit and security event data correlation for real-time operational alerting as well as templated correlation and reporting oriented to identity and access for server configuration policy compliance.

2.0 Issues

No convergence will be painless. Although at first glance, IAM and SIEM audit share some basic similarities in approach and procedure, there are and will remain fundamental differences in the technology providers for the solutions, the consumers of those solutions, and how those solutions are implemented. A number of issues remain before an effective level of convergence can be realized.

2.1 Issues for Clients

For customers, issues to consider include:

• Changes that SIEM and IAM will have on acquisition evaluation criteria for either technology
• The impact SIEM and IAM integration will have on IT budgets and timelines for implementation
• How organizational roles change and skill sets will be enhanced to accommodate this integration, both for information security and the IT operations group
• Managing a converged infrastructure that will still possess multiple processes, multiple toolsets and a complex database of normalized event data
• How an integrated organization will respond to security breaches

2.2 Issues for Technology and Solution Providers

Technology and solution providers must address a number of concerns for potential customers if they hope to fulfill the request for proposal or tender process. Issues that arise include (but are not limited to) the following:

• IAM providers
  • Incorporation of syslog and security log support within the system
  • Time server synchronization to support log record correlation within the system
  • SIEM closed-loop integration with IAM system
• SIEM providers
IAM connectors for the SIEM products to capture IAM data within the system

- System support for workflow in the SIEM approach for application provisioning; approvals via IAM integration
- Conflicting technology alliances, in which SIEM and IAM technology solutions may provide overlapping functionality in event logging, correlation, reporting or workflow

3.0 Bottom Line

IAM and SIEM are key security environments that enterprises deploy or improve to ensure they meet regulatory compliance needs. Steps should be taken immediately at product acquisition to integrate audit infrastructure and base audit functions of IAM and SIEM where practical, primarily through process integration approaches by IT security planning organizations at implementation or upgrade time for either environment. This will provide improvements to the way compliance is addressed today and how forensic audit processes for IAM and SIEM will be addressed tomorrow.

RECOMMENDED READING

"Identity and Access Management Defined"
"IT Security Technologies Can Address Regulatory Compliance"
"How to Develop an Effective Vulnerability Management Process"
"Use This Eight-Step Process for Identity and Access Management Audit and Compliance"
"Improve IT Security With Vulnerability Management"
"Security Information and Event Management Technology Evaluation Criteria, 1H05"
"Magic Quadrant for Security Information and Event Management, 2H05"
"Hype Cycle for Identity and Access Management Technologies, 2005"

**Acronym Key and Glossary Terms**

IAM identity and access management
SIEM security information and event management
HIPAA Health Insurance Portability and Accountability Act
ISO International Organization for Standardization
SIM security information management

**Note 1**

**Definition of IT Security Audit**

The ISO defines the IT security audit as an "independent review and examination of data processing system records and activities to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy and procedures." SIEM and IAM are significant information security environments that contain discrete auditing...
approaches with these characteristics. For example, SIEM and IAM can be viewed as delivering the following basic process steps:

- **Review** — An independent review of access to information systems using all information security records, activity and event logs generated by security activities. For vulnerability, this may involve device configurations, external threat information and resource access information. For identity, this may include user identity, policy and user access information reviews.

- **Analyze** — An analysis of the use of identity information in authentication and authorization activities, reviewed in the context of information security controls, established security policy and operational security procedures. For vulnerability, this may involve, for example, configuration management and policy compliance analysis. For identity, analysis of application portfolio access attempts over time may be useful as indicators of classification.

- **Test** — Measuring the adequacy of those security controls, policies and procedures through formal testing methods with established tools. For vulnerability, this may result in the use of IT security risk management techniques. For identity, this could involve the use of consulting services to establish baseline metrics for controls and policy measures.

- **Remediate** — Ensuring compliance with the established policies, detecting any breaches in security and taking actions to correct where necessary. From a vulnerability perspective, this could take the form of implementing remediation workflows and then monitoring status. For identity, this might manifest in notification of identity policy violations.

- **Report** — Provide complete reports to appropriate authorities on the appropriateness of compliance by the organization and recommended changes to the controls, policies and procedures of the enterprise. For vulnerability, this may take the form of a vulnerability assessment baseline report. For identity, it may be a list of recommended changes to security controls for identity infrastructure following an audit of the services.

In mid-2005, these auditing processes (where they exist) are managed and administered separately in most IT organizations.