Gartner

Research

Publication Date: 1 September 2009 **ID Number: G00161012**

SIEM and IAM Technology Integration

Mark Nicolett, Earl Perkins

Integration of identity and access management (IAM) and security information and event management (SIEM) technologies can improve IAM user and role management capabilities, enable SIEM exception monitoring, and provide audit capabilities that are much broader than what IAM alone can deliver. User activity monitoring is important for both threat management and compliance management.

Key Findings

- SIEM provides user activity and resource access monitoring that complements the audit capabilities of IAM. SIEM can also provide identity auditing for applications and platforms that are out of scope of an organization's current IAM technology deployment.
- SIEM requires a basic IAM policy context in order to provide true exception monitoring. In the absence of IAM-to-SIEM integration, organizations can manually instantiate IAM policies within SIEM (at higher deployment and maintenance costs).
- IAM can utilize SIEM event data to drive user and role life cycle management and automate remediation of exception conditions.
- Vendors that have both SIEM and IAM technologies provide some integration that is not available from third-party SIEM vendors.
- For most SIEM vendors, integration of SIEM with specific third-party IAM products is sporadic, still driven by the requirements of large customers. Most SIEM products integrate with Microsoft Active Directory and major network authentication services.

Recommendations

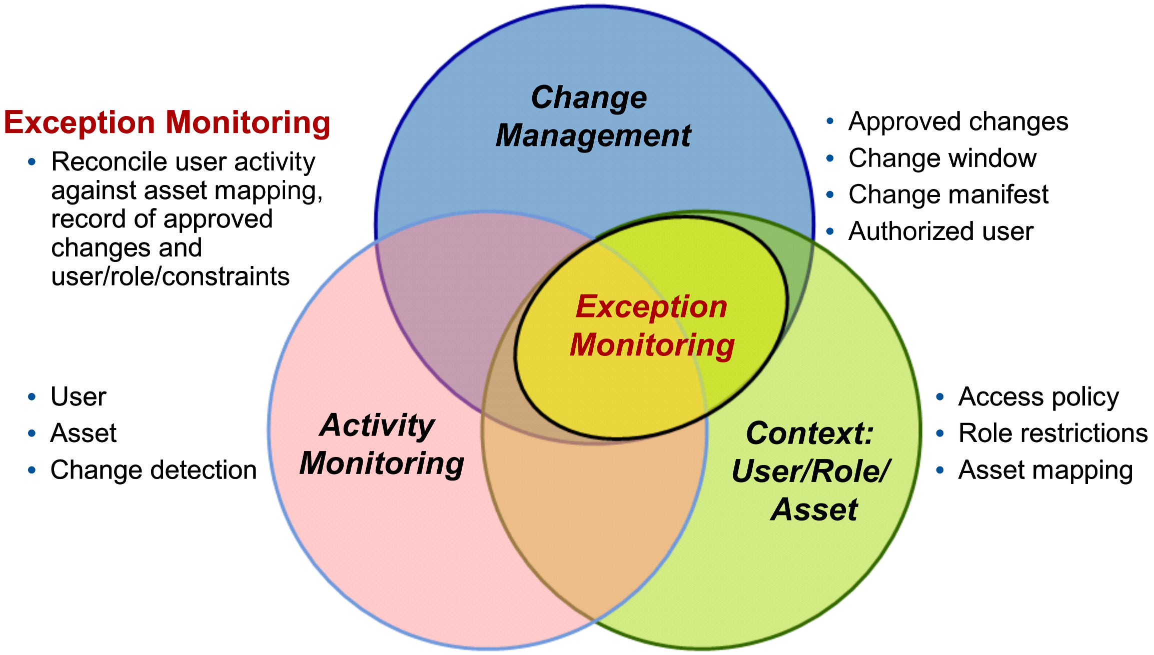
- Implement user activity monitoring as part of a strategy to manage external and internal threats and for regulatory compliance.
- Focus your initial efforts on monitoring the activity of system-level privileged users, followed by those with elevated application entitlements.
- Organizations that wish to employ SIEM for user activity monitoring: Evaluate the level of integration that is provided by the SIEM vendor for the specific event sources in your environment, but plan for extensive customization to implement monitoring for user activity at the application layer.

ANALYSIS

Some of the major limitations of IAM and SIEM technologies can be remedied through integration. IAM technology is very capable in areas such as access and entitlement policy management, but it cannot provide broad-scope user activity monitoring. SIEM technology does provide broad-scope user activity monitoring, but it lacks the user access and entitlement policy context that is needed to identify exceptions. When IAM and SIEM are integrated, SIEM can be used to provide exception monitoring, and IAM can be used to control access in response to the abuse of privileges. There is also the promise of SIEM monitoring, which dynamically adjusts to changes in IAM policies.

SIEM technology provides broad-based monitoring of security events that include user activity and resource access monitoring for servers, databases and applications. User activity and resource access monitoring is needed for compliance reporting, breach detection and fraud detection, but analysis of activity-monitoring reports is labor-intensive. Exception monitoring delivers a substantial reduction in labor, but the move from activity monitoring to exception monitoring requires context about user access rights and policies and reconciliation of detected changes with the record of approved changes (see Figure 1). Some user context is contained in enterprise directories, identity repositories and policies that are defined by IAM systems. SIEM user monitoring can be improved through integration with IAM policy data, and IAM intelligence capabilities in audit and analytics can be expanded through integration with SIEM event data. User-access-based forensic investigations are also enhanced with SIEM monitoring data by providing additional network, server and application resource dimensions to the information used.

Figure 1. Moving From Activity Monitoring to Exception Monitoring



Source: Gartner (August 2009)

SIEM Consumption of IAM Data

Information about entitlements will help organizations implement exception monitoring of user resource access activity as opposed to simple activity monitoring in the absence of policy context. Access policies from role life cycle management, superuser privilege management and other access management technologies define access entitlements that can then be compared with actual resource access.

User provisioning, access management, role management, superuser privilege management, and shared-account password management technologies can provide SIEM with:

- User roles
- User access entitlements
- Cross-referencing of multiple user IDs to a specific identity
- Current account status

Entitlement information can enable SIEM to provide exception monitoring (as opposed to basic activity monitoring). SIEM technology can, by default, provide reports that show all of the resources that have been accessed by a user, or all of the users who have accessed a set of resources. This is activity monitoring. With the addition of user role and access entitlement data, it is possible to build correlation rules and report filters that identify exceptions (i.e., resource access that is out of the normal scope of a role). One example is a rule that flags production database access by a database administrator whose role is to support application development database instances.

User ID cross-reference information maintained by IAM infrastructure can simplify SIEM user activity monitoring. When suspicious user activity is discovered, there is always a need to understand all access by that individual across the environment, and it's common for an individual to have multiple user IDs. Without an identity cross-reference from IAM, SIEM technology would have to dynamically build the user ID cross-reference with long-running correlation rules (or watch lists) that observe multiple logins from a common IP or Media Access Control (MAC) address. IAM integration can provide this cross-reference directly.

SIEM can utilize current-account-status information from IAM to identify resource access exception conditions. A common example is any resource access from a cross-referenced user ID group if one of the user IDs has an inactive or terminated status.

Identity audit and analytics provide a "time machine" of user access and a more definitive "identity" for SIEM data analysis and reporting. SIEM can correlate identity audit information with user resource access events to provide a more complete view of total user access. When identity audit reports are combined with SIEM data obtained from correlated event logs, an additional dimension to "who has access to what" is provided by integrating the circumstances around an access event with the audit report information of the identity involved. It is possible to provide enhanced views of the audit from a network or application perspective. This is particularly valuable when the audit turns to analytics, to determine patterns of access behavior and to employ forensics analysis to deliver comprehensive reporting on a specific access event or events under investigation.

IAM Consumption of SIEM Data

User activity data that is collected by SIEM could be used to provide information about how users are exercising the access rights that have been granted within the IAM system. SIEM can communicate resource access exceptions to IAM technologies for remedial action, such as account suspension. SIEM systems can alert user provisioning or access management systems on attempts to bypass or circumvent controls or to abuse access, so that the IAM technology can invoke remedial action, such as account lockout.

The development and management of fine-grained entitlements (Web and non-Web) can be refined with critical SIEM information regarding past user access performance. The actual resource usage data provided by SIEM can be used to develop roles based on current access patterns. When role entitlements can be compared with actual access, it is possible to implement finer-grained entitlement policies. SIEM resource access information can be useful in validating whether the granularity of access provided by the entitlement is accounted for and does not contribute to segregation-of-duty violations in situations that are not obvious to other monitoring tools, including identity audit.

Access and entitlement management enforcement actions generate log events, but this information can be enhanced with exception or user activity information available from SIEM. It is possible to build "models" of access that serve as templates for future entitlement assignments in (for example) role management tools by correlating specific instances of entitlement enforcement with the specific access event it occurred in.

SIEM Access Policy Monitoring

SIEM can also be used to monitor and alert changes within enterprise directories, identity repositories, or other infrastructure or application components that are out of the scope of IAM. In cases where fine-grained entitlement management is not possible and users are told to limit activity, SIEM can also be used to monitor compliance with that type of policy.

What the IAM Vendors Are Doing

IAM vendors that also provide SIEM technology are expanding SIEM support for their IAM products. CA, Novell and IBM Tivoli are positioning SIEM technology as an audit component of IAM analytics and the IAM suite itself, and they are selling SIEM into their IAM installed bases. These IAM vendors are further developing access policy-level integration between their SIEM and IAM products.

CA

CA has two products in its SIEM portfolio that are integrated with the CA IAM portfolio and are sold as audit enhancements to CA IAM customers. CA Audit and CA Enterprise Log Manager (released in April 2009) both provide basic log data collection and analysis for host systems. CA has built a large installed base for CA Audit by selling it as a monitoring component of IAM deals. Enterprise Log Manager is intended as a replacement for CA Audit. CA Audit and CA Enterprise Log Manager integration is shown in Table 1.

Table 1. CA's SIEM and IAM Integration

CA Access Control
CA ACF2
CA Directory
CA DLP
CA Federation Manager
CA Identity Manager

CA Role & Compliance Manager
CA Single Sign-On
CA SiteMinder
CA SOA Security Manager
CA Top Secret
IBM Resource Access Control Facility (RACF)
Microsoft Identity Lifecycle Manager

Source: Gartner (August 2009)

CA provides taxonomy-level support for many of its SIEM and IAM technology integrations. CA has also completed user interface integrations with CA Enterprise Log Manager that enable system and user activity investigations launched in context from CA Access Control and CA Identity Manager. Additional integrations of this type are under development.

IBM

IBM has three SIEM offerings. IBM Tivoli Compliance Insight Manager (TCIM) is primarily oriented to user activity monitoring and compliance reporting. IBM Tivoli Security Operations Manager (TSOM) is security-event-focused and primarily oriented to external threat management. IBM Tivoli Security Information and Event Manager (TSIEM) is a loosely integrated bundle of TSOM and TCIM that enables select event sharing and common reporting from TCIM. Additionally, IBM provides IBM Tivoli Identity and Access Assurance, which packages TCIM with the IAM suite in a per-user licensing model. IBM has the broadest support for IAM technology across its SIEM products (see Table 2), as it integrates with the largest number of IAM applications from IBM, CA, BMC Software, RSA and others.

Table 2. IBM's IAM Integration

IBM OS/390
IBM Tivoli Access Manager (TAM) for e-business
IBM Tivoli Access Manager for Operating Systems
IBM Tivoli Directory Server
IBM Tivoli Federated Identity Manager
IBM Tivoli Identity Manager (TIM)
IBM Tivoli zSecure Alert
IBM Tivoli zSecure Audit
CA ACF2
CA Access Control
CA SiteMinder
CA Top Secret
Oracle Identity Management

Source: Gartner (August 2009)

Integration of TSIEM with the TIM directory allows TIM administrative user names to be included in the TSIEM monitoring model. TIM events are parsed and visible in TSIEM. This also allows administrative activities to be explicitly monitored and reported on from the TIM audit trails. TAM events are also parsed and visible in TSIEM.

Novell

Novell is primarily focused on using SIEM to provide activity monitoring to its IAM customers. The Novell Identity Audit package provides log management and reporting for Novell's IAM portfolio. Novell Sentinel (acquired in 2006) was originally designed for large-scale security-event-focused deployments, but the June 2009 release of SentinelRD, its rapid-deployment option, is intended to provide simplified deployment and support. Novell Sentinel Log Manager was released July 2009, and it provides an option for broad-scope audit data collection and storage. Novell also provides the Compliance Management Platform — an integrated bundle of IAM and SIEM technologies. Novell Sentinel's IAM integration is shown in Table 3.

Table 3. Novell's IAM Integration

Novell Access Manager
Novell Identity Audit
Novell Identity Manager
Novell eDirectory

Source: Gartner (August 2009)

Novell has made changes in its IAM products to produce events that are more usable by its SIEM technology. The integration with SIEM is at the event level. Real-time monitors as well as reports can make use of policy and identity cross-reference data from Novell IAM products.

What the Other SIEM Vendors Are Doing

Organizations do not necessarily need to acquire SIEM and IAM technology from the same vendor. Many SIEM products have specific support for Microsoft Active Directory, and many SIEM products have specific support for the network authentication servers from Microsoft and Cisco. Some SIEM point solution vendors also support a small number of additional IAM integrations that are driven by the needs of their largest customers. Some examples of SIEM vendors' integration with third-party IAM products are given in Table 4.

Table 4. Examples of SIEM Vendor Support for Third-Party IAM Technology

IAM Integration	ArcSight	LogRhythm	LogLogic	RSA	SenSage
ActivIdentity	X			X	X
Aveksa	X				
CA Identity Manager				X	
CA Audit					X
CA Access Control				X	X
CA ACF2		X			X
CA Top Secret	X	X			X
CA SiteMinder	X		X		X
Citrix Password Manager			X		

IAM Integration	ArcSight	LogRhythm	LogLogic	RSA	SenSage
IBM RACF	X		X		X
IBM Tivoli Access Manager for e-business	X	X			
IBM Tivoli Access Manager for Operating Systems		X			
IBM Tivoli Directory Server		X	X		
Microsoft Active Directory	X	X	X	X	X
NetVision NVIdentity					X
Novell eDirectory		X	X	X	X
Novell Identity Manager		X			
Novell Identity Audit	X				X
Oracle Identity Management	X				
RSA Authentication Manager	X	X	X	X	X
RSA Access Manager	X			X	
SailPoint	X				
Sun Directory Server	X	X			X
Sun Identity Manager	X	X			
UpperVision Identity Inspector	X		X		

Source: Gartner (August 2009)

The vendors in Table 4 were selected because they provide good examples of integration with multiple third-party IAM applications beyond network authentication, but many of the 21 vendors that we track in "Magic Quadrant for Security Information and Event Management" offer support for some IAM applications. Since SIEM vendors are constantly updating event source integration, organizations that are evaluating SIEM technology should check with the SIEM vendors they are considering for current information about support for the IAM technologies in use within their IT environments.

SIEM Customization Requirements

Implementation of identity-based exception reporting will require customization to define organization-specific policies for the SIEM technology that has been deployed. Customization efforts can be reduced somewhat by SIEM technology integration with a specific IAM technology, but customization requirements are never eliminated.

RECOMMENDED READING

"Magic Quadrant for Security Information and Event Management"

"Critical Capabilities for Security Information and Event Management Technology"

"The IAM Market: Is There Still Room at the Bazaar?"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509