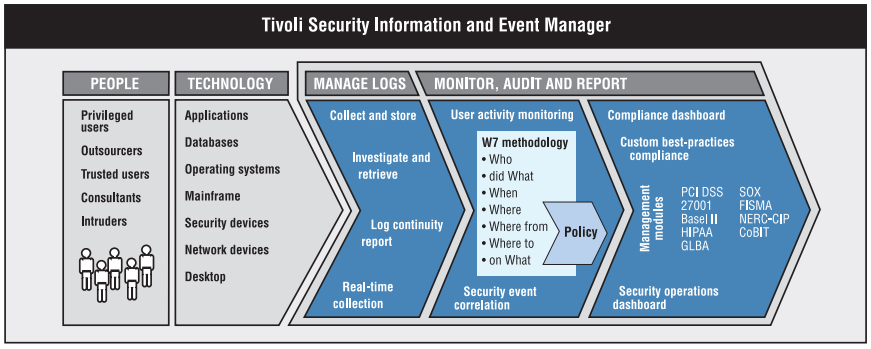
Manage logs and monitor privileged users for insider threat, audit and compliance initiatives

Tivoli® software

IBM Tivoli Security Information and Event Manager

Highlights

- ***Facilitate compliance efforts with centralized dashboard and advanced reporting capabilities***
- ***Efficiently collect, store, investigate, report from and retrieve native logs***
- ***Understand and alert on insider threat using near real time analytics***
- ***Monitor and audit privileged user activities with easy-to-understand reports***
- ***Jump-start compliance reporting with regulation-specific Compliance Management Modules***



IBM Tivoli Security Information and Event Manager allows for end-to-end, holistic security information and event management.

In the last few years, security risks posed by external sources have received significant media attention. While these high-profile attacks pose a very real threat to organizations, internal security incidents perpetrated by privileged users often pose an even greater threat. Whether inadvertent or malicious, the impact can include anything from lengthy outages to lost business to legal liability.

Compliance management is another challenge facing today's business, as preparation for audits, in the form of log management, policy definition and reporting, requires significant resources, and failed audits result in fines and significant rework.

IBM® Tivoli® Security Information and Event Manager helps IT and compliance professionals overcome insider threat and compliance-related challenges. An automated solution for monitoring, investigating and reporting on user and security activity across the enterprise, Tivoli Security Information and Event Manager can provide continuous, non-intrusive assurance and documentary evidence that your data and systems are being managed in accordance with company policies as well as alerting in near real time for specific insider threat type activities.

Tivoli Security Information and Event Manager provides an easy-to-use security compliance dashboard. Through this dashboard, you can quickly gain an overview of your security compliance posture, understand user activities and security events in comparison to acceptable-use frameworks, and monitor privileged users and related security events. Optional Compliance Management Modules allow you to jump start compliance reporting activities with regulation-specific policy recommendations and report templates.

Tivoli Security Information and Event Manager can also help you securely and reliably collect, store, investigate and retrieve logs across the enterprise for compliance and investigative use. Reporting on the log content allows for an expedient time to first report, thereby showing immediate value from using Tivoli Security Information and Event Manager.

Capture audit data with automated enterprise log management and analysis

Most organizations have thousands of systems across the enterprise generating event logs, all of which must be captured and retained. Automating and centralizing the collection of log files can make the process more efficient, saving time and money. Tivoli Security Information and Event Manager can help you securely and reliably collect, store, investigate, report on and retrieve logs across the enterprise for compliance and investigative use.

A scalable log collector helps ensure the reliable and verifiable collection of native logs from virtually any platform. And while many solutions only collect syslog and Simple Network Management Protocol (SNMP) logs, Tivoli Security Information and Event Manager captures much more and delivers:

- *Operating System depth, including IBM System z®, IBM System i®, IBM AIX®, Sun Solaris, HP-UX, Microsoft® Windows® and Linux®.*
- *Audit trails from applications, whether written to a file or to a database table.*
- *Database depth for enhanced auditing capabilities, including integration with IBM DB2®, IBM Informix® Dynamic Server and Sybase ACE.*
- *Security device logs, through syslog and SNMP as well as native methods, APIs, FTP, ODBC/JDBC, SSH, SSL etc..*

Tivoli Security Information and Event Manager provides an intuitive log management dashboard from which to generate numerous reports directly from the log data, as well as a log continuity report, which allows you to demonstrate to auditors and regulators the completeness and continuity of your log management program. Additionally, with Tivoli Security Information and Event Manager's Log Management Module, you can investigate and query suspected incidents through a

compressed, long-term log depot. The log depot provides easy-to-use search capabilities to help you pinpoint potential security incidents.

An advanced toolkit in Tivoli Security Information and Event Manager simplifies the addition of new log collectors and parsers. These parsers can be used to define indexers that allow log data—collected from log files anywhere in the enterprise—to be included in searches in the depot investigation tool. This capability allows you to quickly perform queries that span all online log data. Consequently, you can get fast answers to enterprise incidents without having to resort to cumbersome, homegrown tools or highly technical query languages. Once incidents are identified, the original log data can be retrieved for use with additional forensic tools or platform-specific analysis tools.

View normalized log data via a graphical compliance dashboard

Tivoli Security Information and Event Manager provides visibility into your compliance posture via its graphical dashboard and using its W7 methodology that translates native log data into easily understood language. Rather than read cryptic logs, you can view normalized data that has been synchronized and classified into logical groupings across systems. This normalized view of data enables you to rapidly verify the seven W's of investigation: Who, did What, When, Where, Where from, Where to and on What. Processing log data at this level means that subject matter expertise is not necessary to understand the events. The automated processing of the event data improves the reliability of reports and reduces the cost of report creation.

With this information at your fingertips, you can:

- *Quickly drill down into user behavior, system activity and security information across all platform types*
- *Compare log entries to baseline policy to help pinpoint and minimize security problems*
- *Deliver reporting to support auditors' evidence requests and security managers' investigatory needs without burdening expensive subject matter experts*
- *Rapidly respond to incidents through the ability to set actions and alerts about privileged user activity*

Exceptional events are flagged according to their risk severity so that you can concentrate on the ones with the greatest importance.

Quickly understand privileged user activity and alert in near real time with insider threat analytics

With access to sensitive and financial data and the ability to make changes that can cause operational outages, privileged users with extensive access across applications and platforms can perform accidental or malicious actions that violate company policies and lead to incidents of intellectual property theft and identity theft.

Increasingly, auditors require you to prove that you can monitor and audit access to critical or sensitive corporate data. At the same time, the work of privileged users is critical to your business success. Your strategy for monitoring, reporting on and investigating their activities should not impede their productivity.

Tivoli Security Information and Event Manager enables you to monitor the activities of these powerful users so that you can verify that your policies are being enforced consistently—without limiting the ability of privileged users to do their jobs quickly and effectively. When audit time rolls around, Tivoli Security Information and Event Manager can help you demonstrate to auditors that your organization:

- *Logs and reviews systems administrator and systems operator activities on a regular basis*
- *Analyzes and investigates security incidents and suspicious activity, plus takes remedial actions*
- *Logs access to sensitive data, including root/administrator and database administrator (DBA) access*
- *Continually maintains and reviews application, database, operating system and device logs*
- *Generates alerts in near real time on specific insider threat scenarios*

Respond to auditor requests via out-of-the-box and customized reporting

Robust reporting capabilities are built into Tivoli Security Information and Event Manager. The solution can instantly produce a series of user- and data-oriented reports, but also offers customizable and conditional reporting to respond with great precision to auditors' requests.

An advanced report definition wizard helps you quickly home in on the relevant specifics. You can also automate report distribution to streamline verification processes and other business workflows.

Tivoli Security Information and Event Manager's reporting capabilities can assist you by:

- *Presenting information at a business level, without the individual platform technicalities, thereby reducing the need for SMEs when reviewing logs*
- *Providing easily readable and easy to understand reports via its W7 model that presents data in a common format*
- *Prioritizing events for review by aligning with your businesses priorities*
- *Demonstrating effectively to the auditor that you are reviewing and analyzing log data consistently*
- *Distribute reports automatically to line of business owners for their immediate attention and review*

Jumpstart compliance management efforts with add-on Compliance Management Modules

IBM Tivoli Security Information and Event Manager's Compliance Management Modules are extremely helpful add-on tools that aid you throughout the compliance management lifecycle. These modules include:

- *IBM Tivoli Sarbanes-Oxley (SOX) Management Module*
- *IBM Tivoli International Standards Organization (ISO) 27001 Management Module*
- *IBM Tivoli Gramm-Leach-Bliley Act (GLBA) Management Module*
- *IBM Tivoli Health Insurance Portability and Accountability Act (HIPAA) Management Module*
- *IBM Tivoli Basel II Management Module*
- *IBM Tivoli Federal Information Security Management Act (FISMA) Management Module*
- *IBM Tivoli North American Electric Reliability Council Critical Infrastructure Protection (NERC-CIP) Management Module*
- *IBM Tivoli Control Objectives for Information and related Technology Framework (CoBIT) Management Module*
- *IBM Tivoli Payment Card Industry Data Security Standard (PCI DSS) Management Module*

Each module takes the centralized, normalized data from Tivoli Security Information and Event Manager and works with it in several ways:

- *An asset classification template shows the groups of information, people and other IT assets in your enterprise that are affected–using the vocabulary employed by the regulation or standard.*
- *A policy template measures event data against a customizable, predefined policy that determines who should be allowed to access sensitive data and what each group of people should be able to do with the information.*
- *A report center draws on the asset classification and policy templates to provide dozens of relevant compliance reports geared to the regulation or standard, and the IT controls your organization has in place.*

From a single resource center, you can access all of the management modules you deploy as well as relevant documentation, such as the ISO 27001 Standard, Federal Financial Institutions Examination Council (FFIEC) Handbook for GLBA. You can also access guidelines about using Tivoli Security Information and Event Manager's Compliance Management Modules to facilitate compliance efforts.

By giving you specific views of compliance data from throughout your enterprise, Tivoli Security Information and Event Manager's Compliance Management Modules help streamline compliance management and facilitate efforts to respond to audit requests.

Enhance IBM RACF auditing capabilities

Tivoli Security Information and Event Manager offers optional mainframe plug-ins with enhanced capabilities for RACF® auditing, reducing the cost and skill needed to maintain a secure environment for your business-critical assets. Designed to address the full range of RACF-specific security and compliance challenges, the plug-ins enable organizations to:

- *Quickly analyze and report on mainframe events*
- *Automatically detect security exposures through extensive status auditing*
- *Create standard and customized reports that can be generated in XML format for use in databases and reporting tools*
- *Quickly determine unauthorized logons and attempts, user behavior that violates security policy and when core systems are at risk*
- *Verify RACF commands against your company's policies and procedures, and block or fix the ones that don't comply.*

Benefit from integration across IBM's security portfolio

Tivoli Security Information and Event Manager was built to provide visibility into your organization's security posture, help control the cost of demonstrating compliance, and help reduce the complexity of managing a heterogeneous IT infrastructure. In addition, the solution is seamlessly integrated with other Tivoli security solutions such as IBM Tivoli Identity Manager and IBM Tivoli Access Manager, to help you achieve an end-to-end, closed-loop security and compliance program. Tivoli Security Information and Event Manager can provide the critical monitoring capabilities required when addressing identity and access, application and data security as well as auditing mainframe activity.

For more information

To learn more about IBM Tivoli Security Information and Event Manager, please contact your IBM marketing representative or IBM Business Partner, or visit the following Web site: **ibm.com**/tivoli/solutions/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
October 2009

TID14056-USEN-00