IBM India Software Labs

Tivoli Security Information and Event Manager

Installation of TSIEM, Fix packs, Agents and Compliance modules

Aslam Siddiqui

Boudhayan Chakrabarty

Introduction to TSIEM

- **IBM® Tivoli® Security Information and Event Manager (Tivoli Security Information and Event Manager) is an enterprise-wide auditing program for monitoring internal computer activity.**
- **Tivoli Security Information and Event Manager provides continuous, non-intrusive assurance and documentary evidence that data and systems are being managed in accordance with and comply with company policies.**

Components of TSIEM

- Tivoli® Security Information and Event Manager is composed of two modules, three types of servers, event sources.
- Log Management
  The Log Management module collects log data that is relevant to security auditing and compliance monitoring. It stores the data on a central server, the Log Management Server.
- Security Information Management (SIM)
  The SIM module evaluates and reports on user-oriented events and evaluates them against predetermined policy.

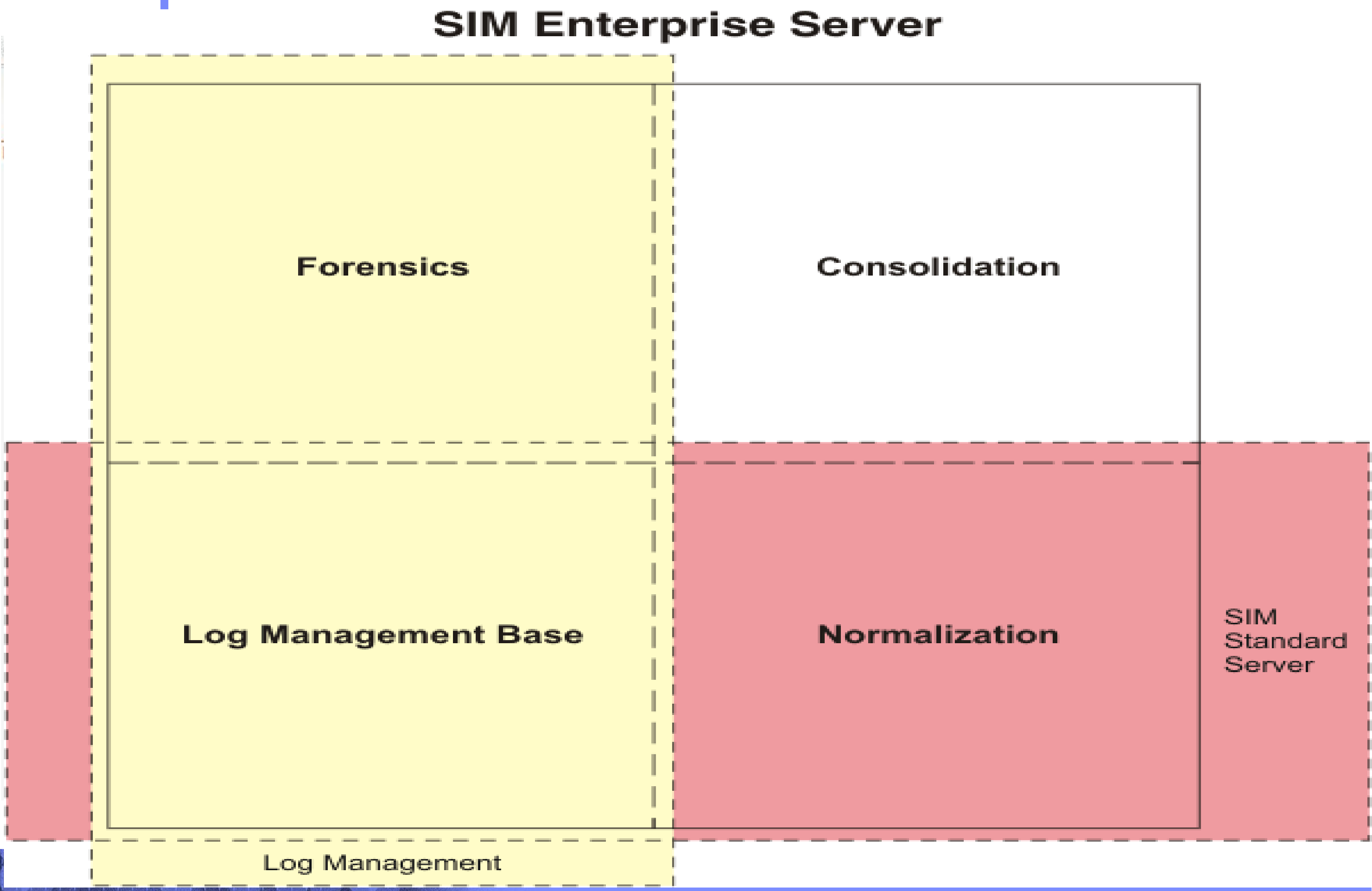
Server types and their functions

- **1.Log Management server**
- **It provides all Log Management functions, including log collection, log storage, log retrieval, forensic search, and log management reports.**
- **This server type is deployed to manage log data for which SIM functions, such as W7 normalization and compliance reporting, are not required.**
- **If you did not purchase the Security Information Module, you can deploy only Log Management Servers**

Continued..

- **2.SIM Standard Server**
- **It provides log collection, log storage, log retrieval, W7 normalization, and compliance reporting, but no forensic search or log management reports**
- **3. SIM Enterprise Server**
- **It provides all Log Management Server functions as well as all SIM functions such as W7 normalization and compliance reporting.**
- **Also provides a consolidated view of normalized W7 data on the attached Standard Servers , forensic search and log management reporting.**

Example


SIM Enterprise Server
Forensics
Consolidation
Log Management Base
Normalization
SIM Standard Server
Log Management

Event sources

- Tivoli® Security Information and Event Manager provides event sources (end points) to obtain and process activity data from various applications, devices, and operating systems
- Event sources have a Log Management component and an optional SIM component. The Log Management component allows raw events to be stored into the Log Management Depot and allows Log Management reports to be created. The SIM component provides full W7 support.

Hardware requirements for AIX systems

- Any system from the POWER® family of processors (64-bit)
- 8 GB RAM (+ 0.5 GB for each Reporting Database)
- The swap space must be at least equal to the amount of the RAM on your system, or slightly more (such as 1.25 times the amount of RAM).

Hardware requirements (continued..)

- **Ensure that the following directories have at least the minimum amount of space:**
- **1 GB in /**
- **1 GB in /usr**
- **1 GB in /var**
- **2 GB in /tmp**
- **1 GB in /home**
- **10 GB in /opt**
- **A minimum of 200 GB of free hard disk space is required. Specific requirements depend on log volumes and types of log data**

Hardware requirements for Linux Systems

- **Quad Core Intel Xeon 3.0 GHz processor (64-bit)**
- **8 GB RAM (+ 0.5 GB for each Reporting Database)**
- **Temp directory: 100 MB for the /tmp directory (during installation). The temporary directory is the working directory for the installation program**
- **A minimum of 200 GB of free hard disk space is required. Specific requirements depend on log volumes and types of log data**

Hardware requirements for Windows systems

- Quad Core Intel Xeon 3.0 GHz processor (64-bit)
- 8 GB RAM (+ 0.5 GB for each Reporting Database)
- Temp directory: 600 MB (during installation)
- A minimum of 200 GB of free hard disk space is required. Specific requirements depend on log volumes and types of log data.
- Note: For Standard server you may can use Duo Core Intel Xeon 3.0 GHz processor (64-bit)

Software requirements for AIX systems

- One of the following operating systems:
- AIX 5.3 Service Pack 5300-04-01 (64-bit)
- AIX 6.1 (64-bit)
- Ensure that the sudo and seq utilities are available by installing the following packages:
- sudo-1.6.7p5-3 coreutils-5.2.1-2
- For the forensic search function, the AIX Fast Connect component must be installed on any AIX Log Management Server or AIX Enterprise Servers
- For SSH collect, OpenSSH for AIX must be installed on the AIX agent, AIX Servers, and AIX Log Management Server involved in the collect operations

Software requirements for Linux systems

- One of the following operating systems: SUSE Linux Enterprise Server 11 for x86-64 bit
- Red Hat Enterprise Linux 5.5,5.4,5.3 for x86-64 bit
- UTF-8 must be enabled as the default character encoding for the operating system. Ensure that the sudo utility is installed.
- Ensure that the sudo utility is installed.
- The Korn shell, provided in the pdksh rpm package, is required. Install the most recent version available for your operating system.

Software requirements (continued..)

- **Ensure that the following packages are installed. These packages are usually installed by default with the operating system.**
- **compat-gcc**
- **compat-gcc-c++**
- **compat-libstdc++ c**
- **ompat-libstdc++-devel**
- **glibc-devel glibc-headers**
- **glibc-kernheaders**

Software requirements for Windows systems

- One of the following operating systems:
- Microsoft Windows 2003 Server SP1 (or higher) for 64-bit
- Microsoft Windows 2008 Server for 64-bit
- Microsoft Windows 2008 Server SP1 for 64-bit
- Microsoft Windows 2008 Server R2 for 64-bit
- NetBIOS enabled, NTFS file system
- For SSH collect to work, PuTTY must be installed on the Windows agent, Windows Tivoli Security Information and Event Manager Servers, and Windows Log Management Servers involved in the collect operations

Requirements for Web Applications

- One of the following browsers must be installed: Internet Explorer 6.0 SP2 or Internet Explorer 7.0 on Windows systems
- Firefox version 2.0, 3.0, or 3.1 on Windows or Linux systems
- Enable JavaScript and ActiveX
- To view the Tivoli® Integrated Portal properly, ensure that JavaScript and ActiveX are enabled for the web browser.
- If you are using Internet Explorer, ensure that the system where Tivoli Security Information and Event Manager is installed is added to the "Trusted sites" list in Internet Explorer.

Requirements for the Tivoli Security Information and Event Manager agent

- **Ensure that the Korn shell (ksh) is installed on audited machines that are on the following operating systems**
- **AIX, HP-UX ,Linux ,Sun Solaris**
- **Install the Tivoli® Security Information and Event Manager Server before installing an agent.**
- **The agent must have access to the Tivoli Security Information and Event Manager servers through an Internet Protocol network.**
- **Connect the agent to the Tivoli Security Information and Event Manager Servers through an Internet Protocol network.**

Planning TSIEM installation

- Before installing, be sure that you understand the types of servers you are installing.
- Decide which computers you want to designate for the following purposes:
- Log Management Servers
- Standard Servers
- Enterprise Servers
- Ensure that each server or workstation hosting Tivoli® Security Information and Event Manager components meets the system requirements outlined in System Requirements

Installing TSIEM

1.Log on to the system where you wish to install Tivoli Security Information and Event Manager.

On Windows systems:

Log on as a member of the Administrators group , such as Administrator.

On AIX and Linux systems:

Log in as the root user

Installing TSIEM (continued..)

2.Ensure that the host name and IP address of the system can be resolved.

a. Open a command window.

b. Use the host name command to obtain the host name of the system.
For example:# hostname
tsiemserver.example.com

c. If a fully qualified domain name (FQDN) is returned, verify that the host name can be resolved using the ping command.

For example:

Installing TSIEM (continued..)

```
# ping tsiemserver.example.com

PING tsiemserver.example.com (192.168.4.24)
    56(84) bytes of data.

64 bytes from tsiemserver.example.com
    (192.168.4.24): icmp_seq=1 ttl=64 time=0.121 ms
```

d. Verify that the IP address of the system

can be resolved.

```
# ping 192.168.4.24 PING 192.168.4.24 (192.168.4.24)
    56(84) bytes of data.

64 bytes from 192.168.4.24: icmp_seq=1 ttl=64
    time=0.021 ms
```

Installing TSIEM (continued..)

e. Verify that the short name of the system can be resolved.

For example:

```
# ping tsiemserver

PING  tsiemserver.example.com (192.168.4.24)
56(84) bytes of data.

64 bytes from tsiemserver.example.com
(192.168.4.24): icmp_seq=1 ttl=64 time=0.104 ms

64 bytes from tsiemserver.example.com
(192.168.4.24): icmp_seq=2 ttl=64 time=0.015 ms
```

Begin Installation

If the host name and IP address of the system cannot be resolved, the installation fails.

Resolve any name resolution issues before continuing with the installation.

3. Access the installation DVD.

On Windows systems:

a. Insert the *Tivoli Security Information and Event Manager* DVD.

Installing TSIEM (continued..)

b. If the installation program does not start automatically, do the following steps:

Access the DVD drive

Double-click the install.exe icon.

On AIX and Linux systems:

a. Insert and mount the *TSIEM* DVD.

b. On AIX systems,

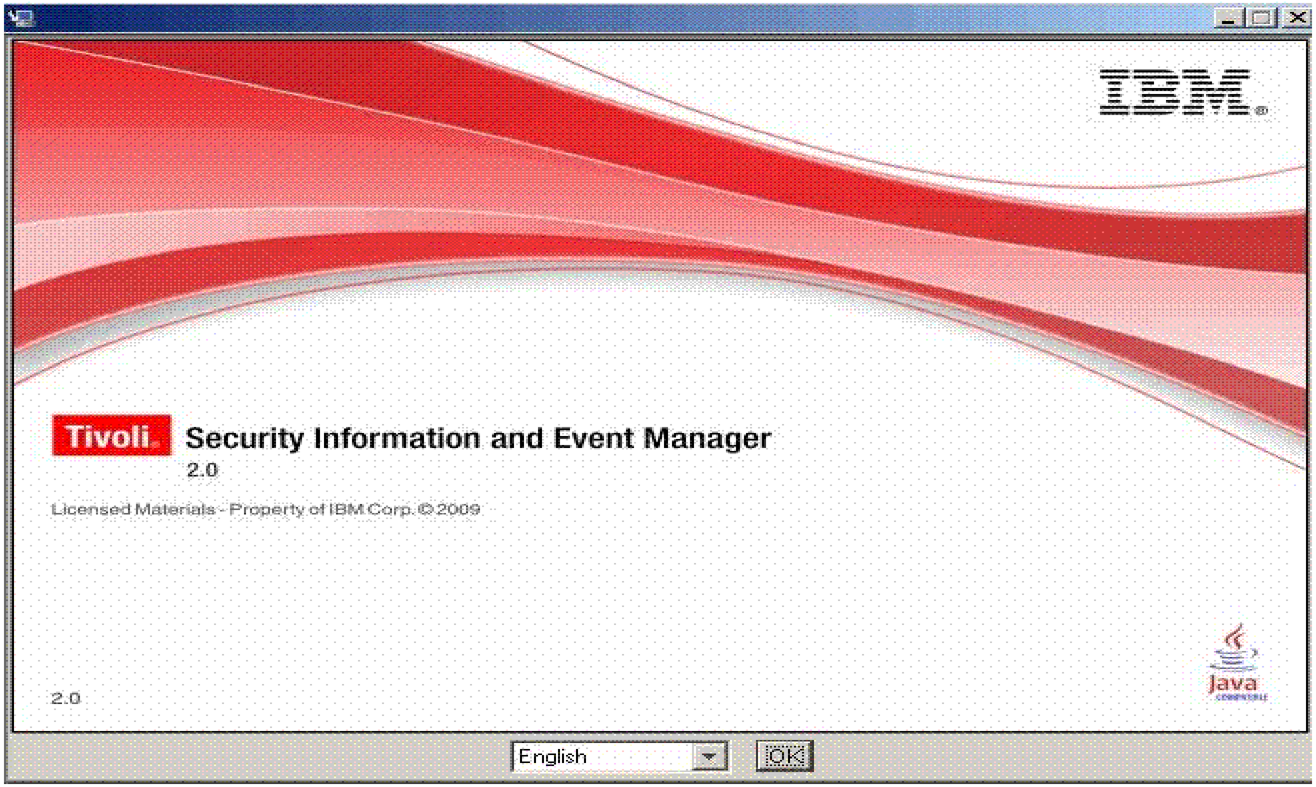
type ./install.aix

On Linux systems,

type ./install.linux

Installing TSIEM Demo

- **The installation program starts and displays the Tivoli Security Information and Event Manager window.**



Tivoli. Security Information and Event Manager

2.0

Licensed Materials - Property of IBM Corp. © 2009

2.0

TSIEM Fix packs

- Individual fixes are published as often as necessary to resolve defects in IBM® Tivoli Security Information and Event Manager.
- In addition, two kinds of cumulative collections of fixes, called fix packs and refresh packs, are published periodically for IBM Tivoli Security Information and Event Manager, in order to bring users up to the latest maintenance level.
- Install these update packages as early as possible in order to prevent problems

Installing the Server fix pack on a Microsoft Windows system

- Extract the files from the 2.0.0-ISS-TSIEM-SRV-Multi-FP008.zip file to a temporary directory on the Windows system.
- It is advised to use the console mode connection when using remote desktop to connect to the server, e.g. mstsc /console
- Install the fix pack by running the Launcher.bat file.

Continued..

- The fix pack installation program determines which Tivoli Security Information and Event Manager components are installed on the system and applies the necessary updates to those components.
- To uninstall the fix pack:
- Go to the <TSIEM_HOME>_uninst\FP008 directory
- Run uninstall.exe

Installing the Server fix pack on an AIX or Linux system

- **To install the fix pack on an AIX or Linux server system:**
- **Extract the files from the 2.0.0-ISS-TSIEM-SRV-Multi-FP008.zip file to a temporary directory on the system.**
- **Modify permission attributes of all extracted files in the temporary directory by issuing the following command : chmod -R 755 <temp_dir>.**
- **Install the fix pack by running the Launcher.sh script.**

Uninstall the fix pack

- **Go to the <TSIEM_HOME>/_uninst/FP008 directory.**
- **Run uninstall**
- **This would uninstall the fix pack and all of its contents**

TSIEM Agents

- Agents, running as a service or daemon on IBM® AIX®, HP-UX, Microsoft Windows, and Sun Solaris systems, collect audit data from event sources and securely transfers that data to Tivoli® Security Information and Event Manager servers.
- The agent for Windows systems
- Install an agent when the audit configuration requires the agent to collect data from Windows systems.
- When you add a computer through the Managing Audited Machines task in the Tivoli® Integrated Portal, you can select one of two ways to install an agent remotely: Automatic or Manual

Automatic Agent installation

- If you select the Automatic installation type, you specify the following information:
- The installation path for the agent software.
- The user credentials under which the agent will run.
- The administrator credentials under which the agent will be installed on the remote system. This administrator must be a domain administrator or local built-in administrator.
- The agent software is installed at that time.

Manual Agent install

- **Installing the agent manually on a Windows system**

1.Log on to the target system as a member of the Administrators group.

2.Insert the CD labeled *IBM Tivoli Security Information and Event Manager v2.0 for Agents* into the CD-ROM drive.

3.Run the Setup.exe program in the x86_nt_4 directory on the CD. The Welcome window of the Setup program is displayed.

4.In the Welcome window, click Next.

Specify Directory

5. In the Target Directory window, do one of the following steps to specify the directory for the Setup program to install the agent components:

- Accept the default value C:\IBM\TSIEM by clicking Next.
- Type the complete path to another directory and click Next.
- Click Browse and navigate to the directory you want to use and click Next.
- A Target Directory window is displayed for confirmation.

Continued..

6. Verify that the directory where you want to install the agent is displayed, and click Next.

7. In the Select Configuration File window, do one of the following steps:

   To use a configuration file for the agent configuration parameters, specify the name of the configuration file that the Server created when this agent was configured in the Tivoli Integrated Portal. You can specify the file name in one of the following ways:

a. In the Configuration File Location field, type the complete path and file name and click Next.

Continued..

b. Click Browse and navigate to the directory containing the configuration file and click Next.

8. In the OS Account window, type the name and password for the operating system account that will run the agent, and click Next.

9. If you selected the Manual Configuration check box:

- **a. In the Tivoli Security Information and Event Manager Agent window,**

Specify the following information for the agent and click Next:

Define Agent parameters

- Agent ID
- IP address
- TCP Port
- Password

b. In the Tivoli Security Information and Event Manager Server Information window, specify the following information for the Server and click Next:

- IP address
- TCP Port

Continued..

c. In the HOP Information window, specify the following information and click Next:

- Agent ID
- IP address
- TCP Port
- Installation begins. When installation finishes, the Setup Finished window displays a notification of whether the installation succeeded.
- If the window indicates that installation did not succeed, run the Setup program again.

Uninstalling the agent on a Windows system

- **To uninstall the agent on a Windows system, use the Windows Add or Remove Programs function in the Control Panel**

Compliance management modules

- **Compliance management modules are optional components of IBM® Tivoli® Security Information and Event Manager that can help you monitor your adherence to one or more security and privacy standards.**
- **IBM Tivoli Sarbanes-Oxley Management Module**
- **IBM Tivoli PCI-DSS Management Module**
- **IBM Tivoli HIPAA Management Module**
- **IBM Tivoli ISO27001 Management Module**
- **IBM Tivoli COBIT Management Module**

Continued..

- **IBM Tivoli FISMA Management Module**
- **IBM Tivoli GLBA Management Module**
- **IBM Tivoli Basel II Management Module**
- **IBM Tivoli NERC CIP Management Module**

IBM Tivoli Sarbanes-Oxley Management Module

Detects security violations gainst an organization's security policies, and it records, monitors, and examines user activity in information systems that contain financial data and other sensitive information

Installing the management module

- The IBM® Tivoli® Sarbanes-Oxley Management Module can be installed on any system where the Tivoli Security Information and Event Manager Normalization component has been installed.
- Log on to the system as an administrator or root user.
- Based on your operating system, insert the installation DVD into the DVD-ROM drive.
- Change to the Compliance_Management_Modules directory of the DVD.

Start the Installation program

- On AIX and Linux systems:
  - Based on your operating system, extract the files from the archive file.
  - AIX
  - Sarbanes- Oxley_aix.tar.gz
  - Linux
  - Sarbanes- Oxley_linux.tar.gz
  - Run ./Launcher.sh
- On Windows systems, run Sarbanes-Oxley.exe

Continued..

- Select the language for the installation program and click OK.
- After reading the introduction, click Next. After reading and agreeing to the license agreement, click Next to continue. You must agree to the license agreement to install the management module.
- Ensure that you have sufficient disk space available. Verify the correct management module is being installed. Click Install to begin the installation.
- After the installation is complete, click Done to exit.

Uninstalling the management module

- **Log on to the system as an administrator or root user.**
- **Uninstall the management module.**
- **On AIX® and Linux systems:**
- **Run the uninstallation script, uninstall, located in directory: tsiem_home/_uninst/TSIEM_MM_sarbox**
- **where *tsiem_home* is the directory where Tivoli Security Information and Event Manager was installed**
- **For example:**
- **/opt/ibm/tsiem/_uninst/TSIEM_MM_sarbox/uninstall**

Continued..

- On Windows Server 2008 systems:
- Open the Control Panel in Windows and click Programs and Features.
- Locate the item called Compliance Management Module Sarbanes-Oxley and click Uninstall/Change.
- Click OK to confirm the removal of the management module. The management module is then removed from the system.
- After the uninstallation is complete, click Finish to exit

Questions/Comments!!!!