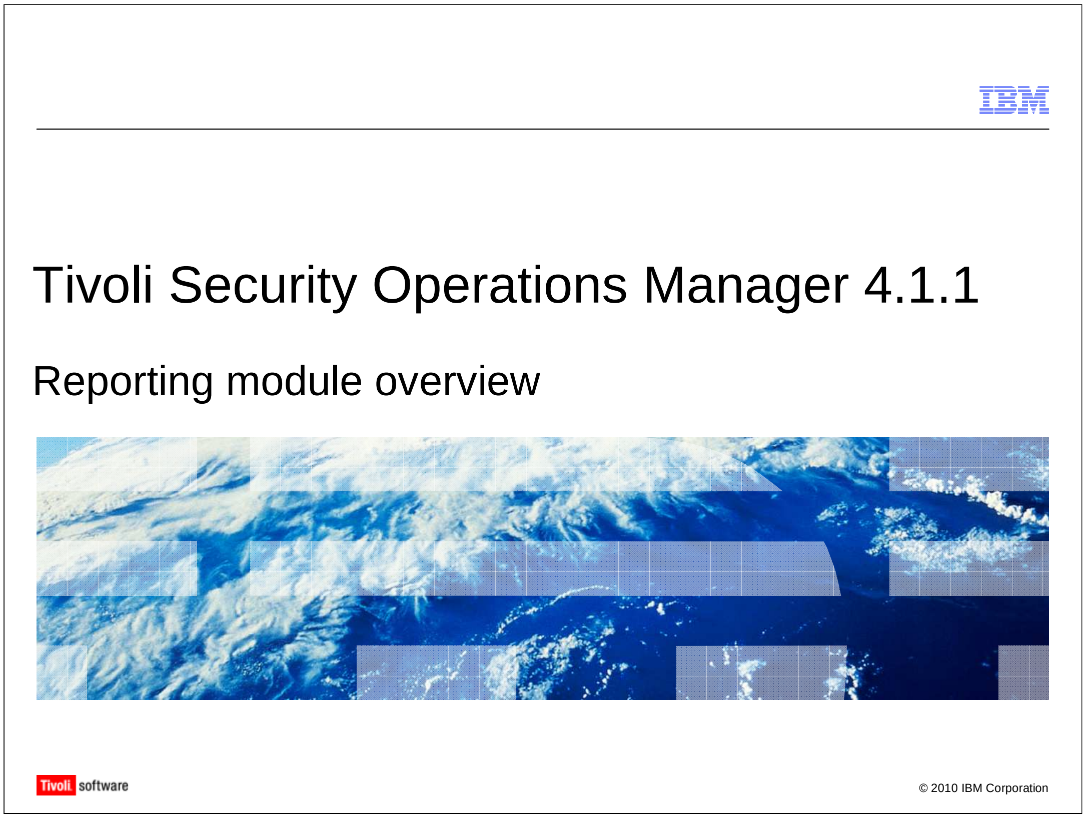
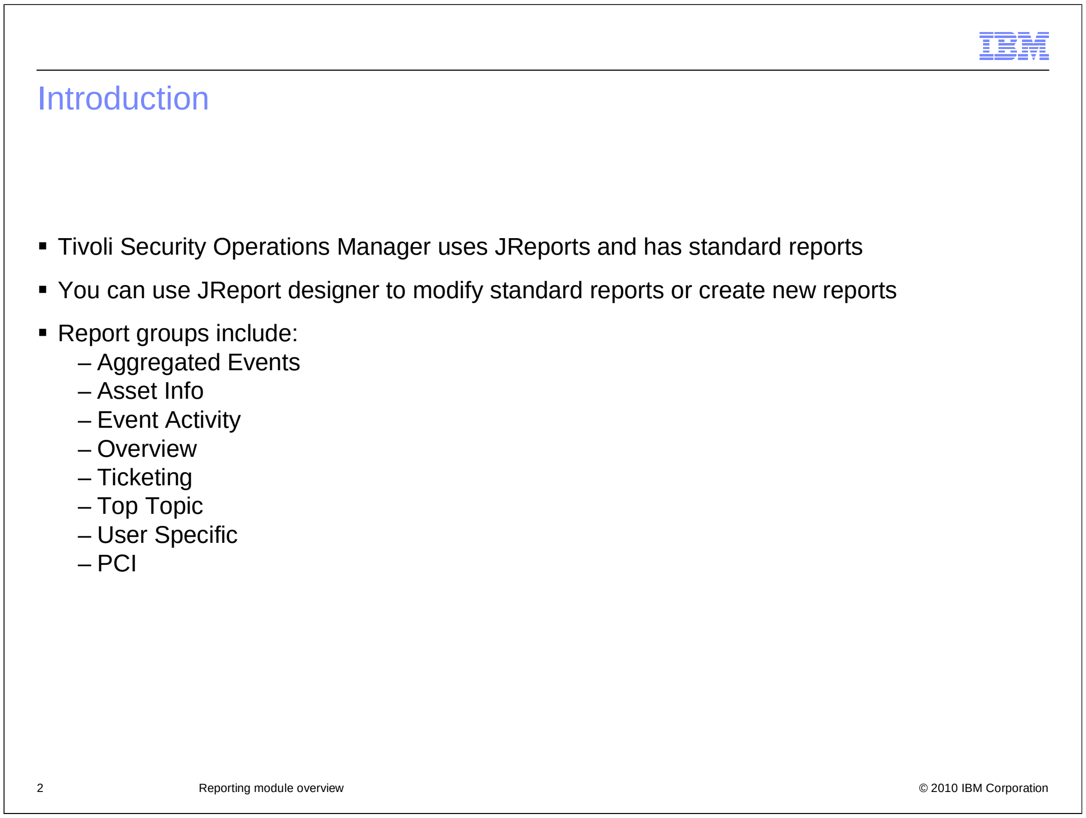


Tivoli Security Operations Manager 4.1.1

Reporting module overview

This training module provides an overview of the Tivoli® Security Operations Manager 4.1.1 Reporting module. By the end of this module, you should be familiar with the various reports offered by Tivoli Security Operations Manager.

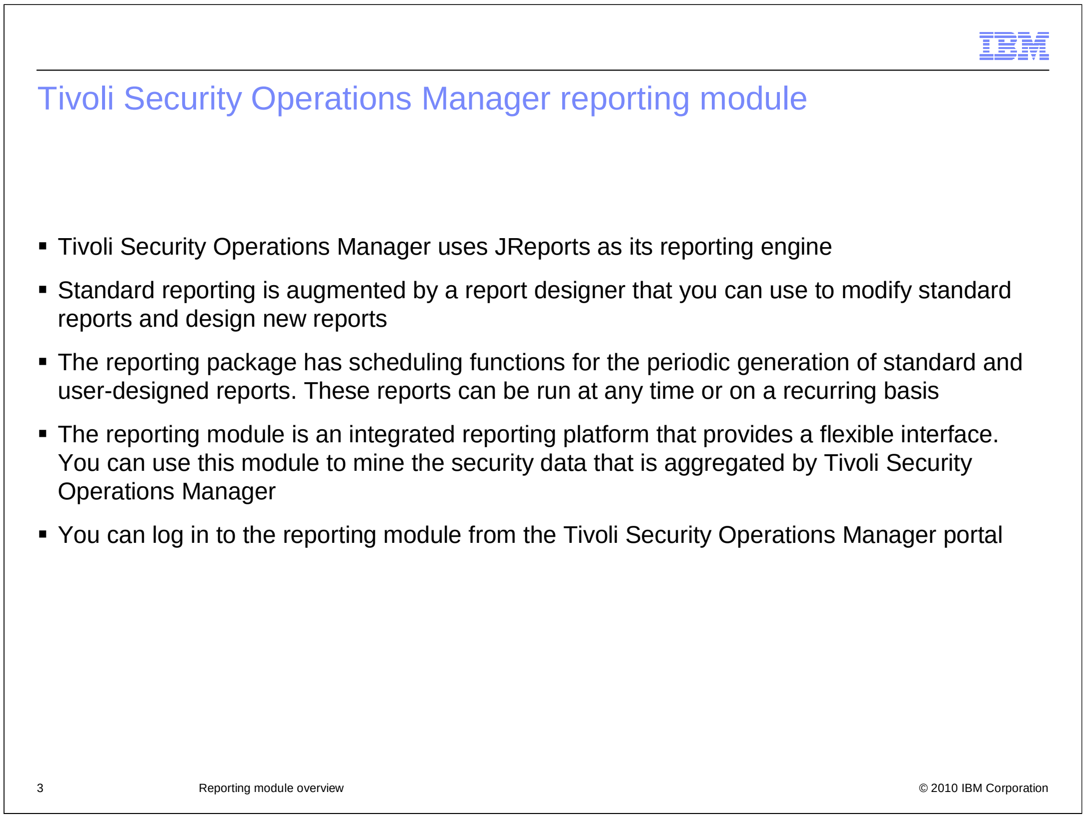


Introduction

- Tivoli Security Operations Manager uses JReports and has standard reports
- You can use JReport designer to modify standard reports or create new reports
- Report groups include:
  - Aggregated Events
  - Asset Info
  - Event Activity
  - Overview
  - Ticketing
  - Top Topic
  - User Specific
  - PCI

In this module, you learn that Tivoli Security Operations Manager uses JReports and also has standard reports. You will also learn that you can use JReport designer to modify standard reports or create new ones.

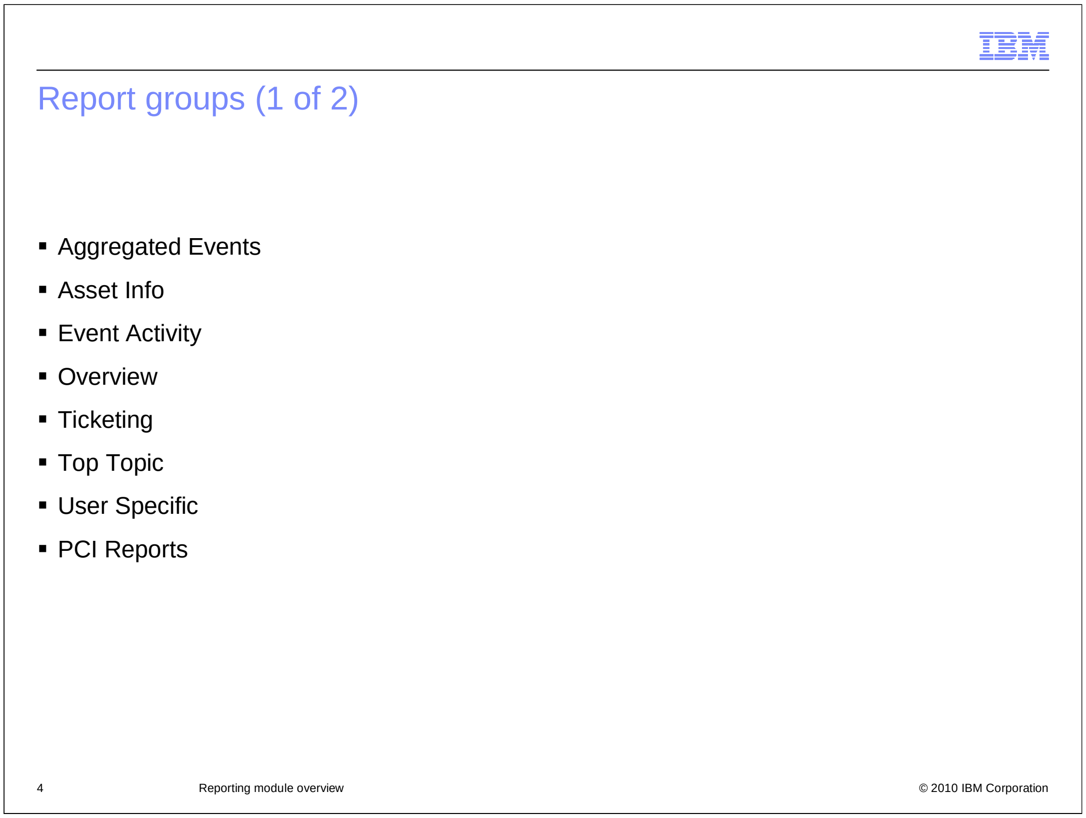
The list of report groups is shown on the slide.



Tivoli Security Operations Manager reporting module

- Tivoli Security Operations Manager uses JReports as its reporting engine
- Standard reporting is augmented by a report designer that you can use to modify standard reports and design new reports
- The reporting package has scheduling functions for the periodic generation of standard and user-designed reports. These reports can be run at any time or on a recurring basis
- The reporting module is an integrated reporting platform that provides a flexible interface. You can use this module to mine the security data that is aggregated by Tivoli Security Operations Manager
- You can log in to the reporting module from the Tivoli Security Operations Manager portal

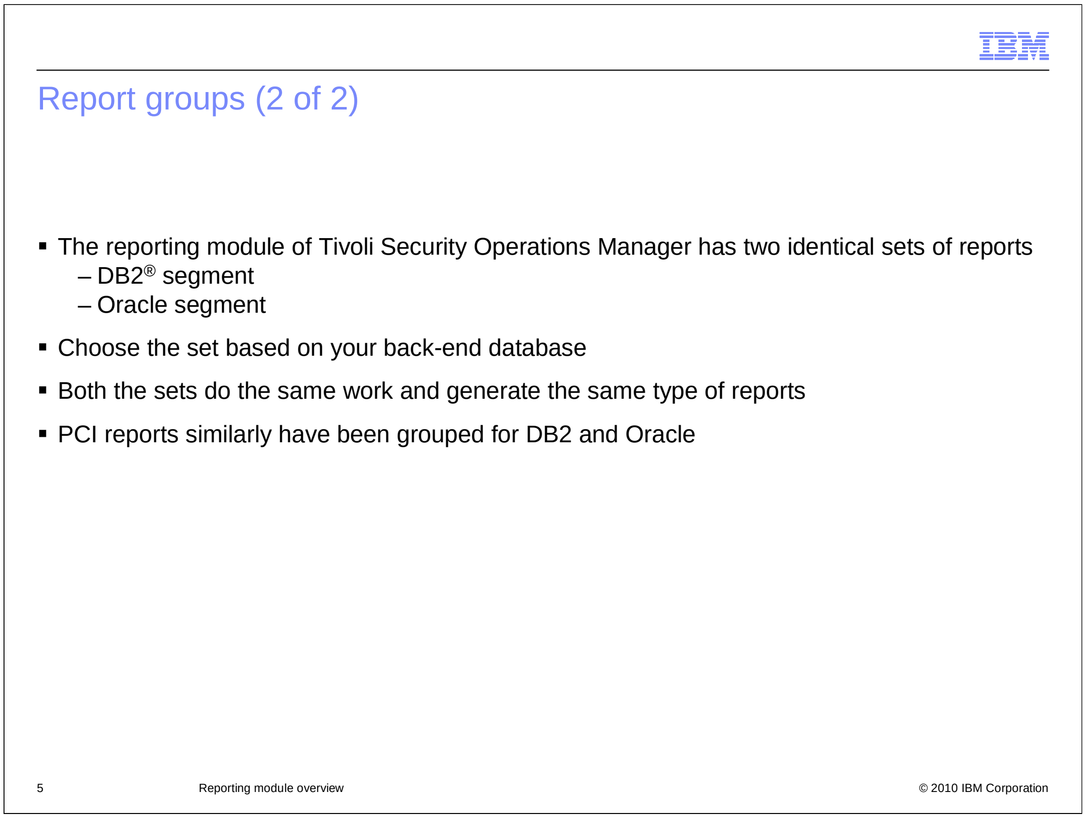
Tivoli Security Operations Manager uses JReports as its reporting engine. Analysts can modify standard reports and create new ones through a report designer that augments standard reporting. This JReport designer and a set of standard reports are included with Tivoli Security Operations Manager. If you want to change any of the standard reports or create new reports, you can use the JReport designer. These reports can be started at any time, or can be scheduled to run on a recurring basis. The reporting module is an integrated reporting platform that provides a flexible interface. Individuals who are responsible for security operations can mine the security data that is aggregated by Tivoli Security Operations Manager. Users can log in to the reporting module from the Tivoli Security Operations Manager portal.



Report groups (1 of 2)

- Aggregated Events
- Asset Info
- Event Activity
- Overview
- Ticketing
- Top Topic
- User Specific
- PCI Reports

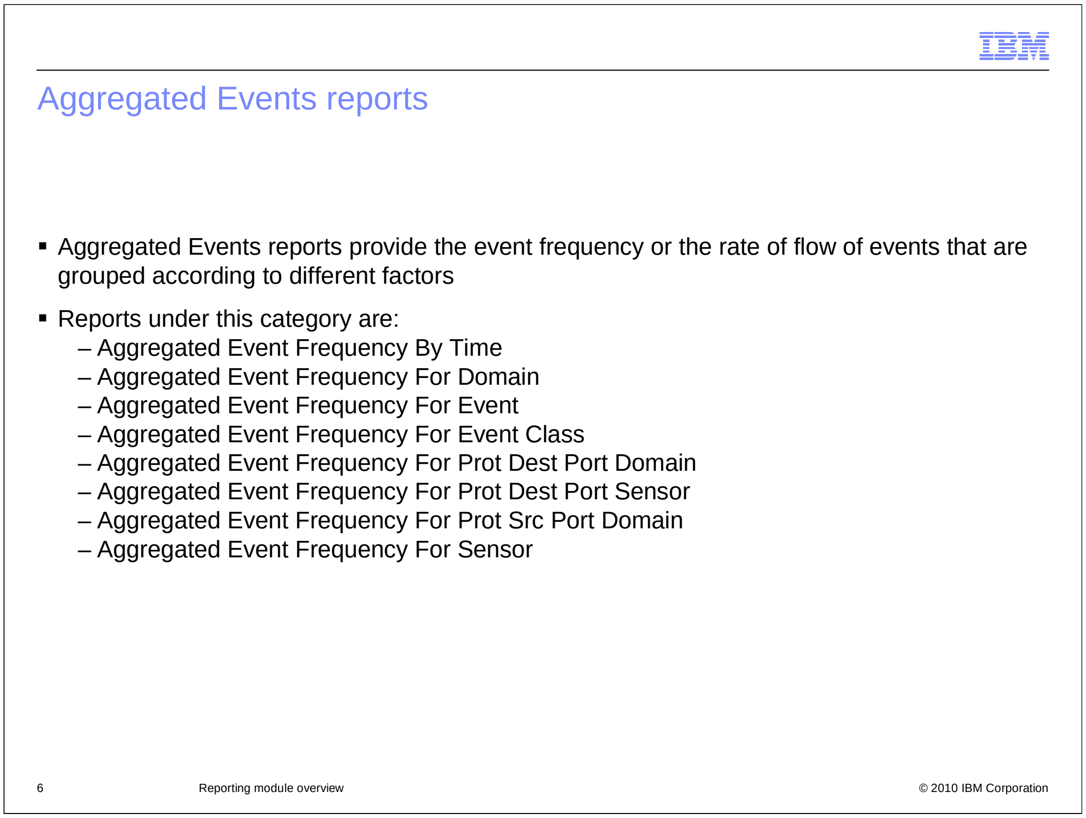
The reports in Tivoli Security Operations Manager have been divided into the following groups: Aggregated Events, Asset Info, Event Activity, Overview, Ticketing, Top Topic, User Specific, and PCI Reports.



Report groups (2 of 2)

- The reporting module of Tivoli Security Operations Manager has two identical sets of reports
  - – DB2® segment
  - – Oracle segment
- Choose the set based on your back-end database
- Both the sets do the same work and generate the same type of reports
- PCI reports similarly have been grouped for DB2 and Oracle

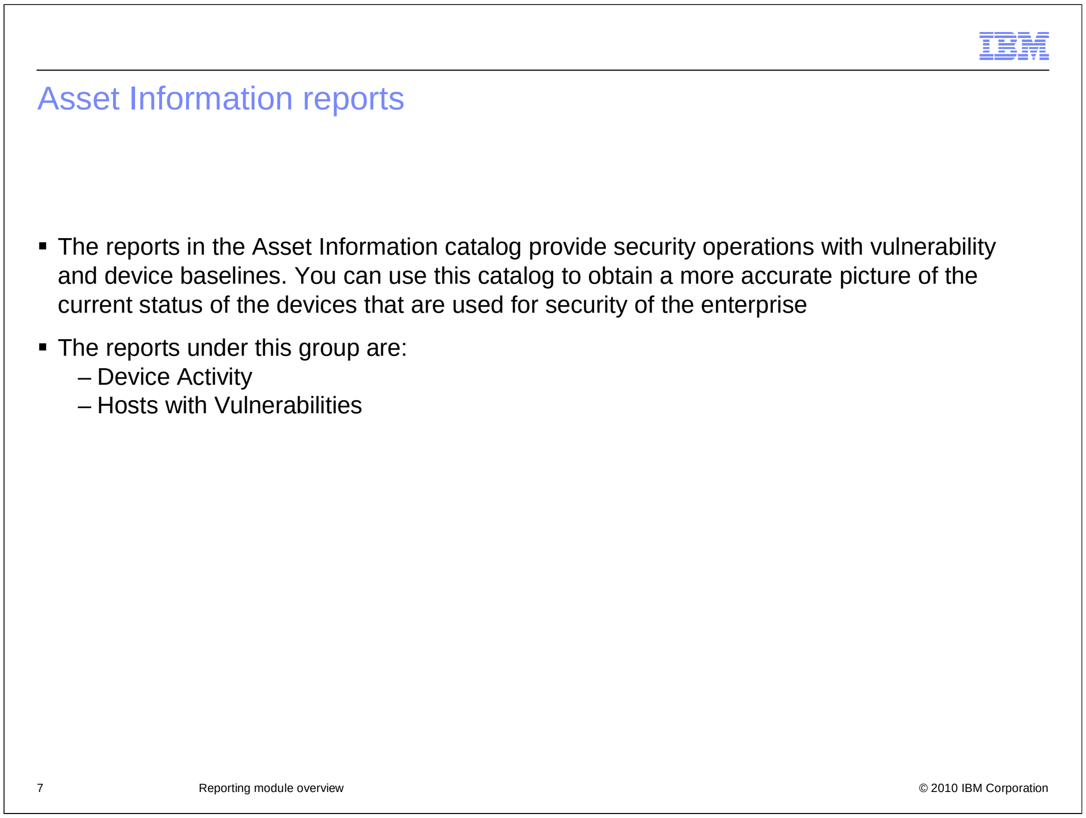
In the reporting module, you find the same set of reports under the DB2 segment and the Oracle segment. The set of reports that you choose depends on the back-end database that you are using for Tivoli Security Operations Manager. These sets have the same reports and produce the same research. The only difference between them is the back-end database that Tivoli Security Operations Manager is using in your environment. While executing a report, the JReports server runs queries on the back-end database. There is a slight difference in the queries that are executed, based on the database that you are using. A new feature for Tivoli Security Operations Manager is the PCI report generation. As with other sets of reports, PCI reports are grouped for DB2 and Oracle.



Aggregated Events reports

- Aggregated Events reports provide the event frequency or the rate of flow of events that are grouped according to different factors
- Reports under this category are:
  - Aggregated Event Frequency By Time
  - Aggregated Event Frequency For Domain
  - Aggregated Event Frequency For Event
  - Aggregated Event Frequency For Event Class
  - Aggregated Event Frequency For Prot Dest Port Domain
  - Aggregated Event Frequency For Prot Dest Port Sensor
  - Aggregated Event Frequency For Prot Src Port Domain
  - Aggregated Event Frequency For Sensor

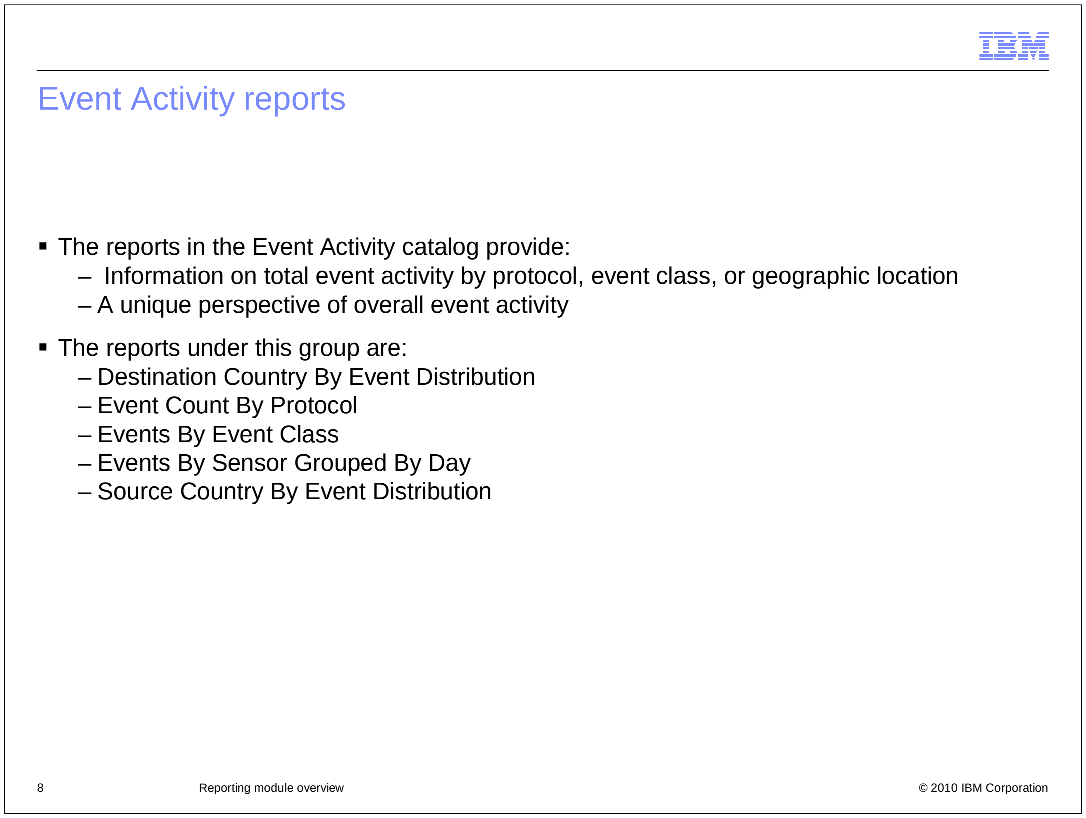
The Aggregated Events group provides the event frequency or the rate of flow of events, grouped according to different factors. Every report displays data on aggregated event frequency or the rate of flow of events, depending on a factor, such as time, domain, event, event class, or another factor.



Asset Information reports

- The reports in the Asset Information catalog provide security operations with vulnerability and device baselines. You can use this catalog to obtain a more accurate picture of the current status of the devices that are used for security of the enterprise
- The reports under this group are:
  - Device Activity
  - Hosts with Vulnerabilities

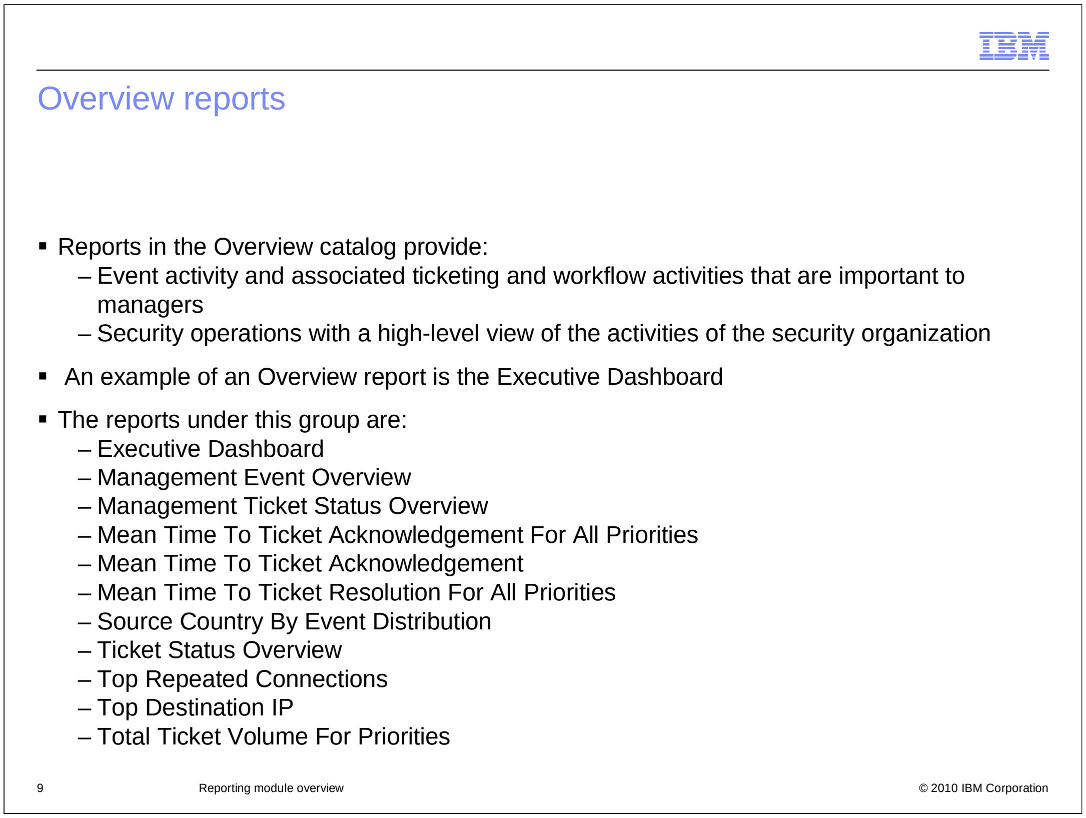
The Asset Information catalog provides security operations with vulnerability and device baselines. These baselines provide a more accurate picture of the current status of the devices that are used for the security of the enterprise. Reports in this group are Device Activity and Hosts with Vulnerabilities. Tivoli Security Operations Manager supports many vulnerability scanners. Information from these vulnerability scanners can be imported into the tool. The result is considered when data is correlated in Tivoli Security Operations Manager.



Event Activity reports

- The reports in the Event Activity catalog provide:
  - Information on total event activity by protocol, event class, or geographic location
  - A unique perspective of overall event activity
- The reports under this group are:
  - Destination Country By Event Distribution
  - Event Count By Protocol
  - Events By Event Class
  - Events By Sensor Grouped By Day
  - Source Country By Event Distribution

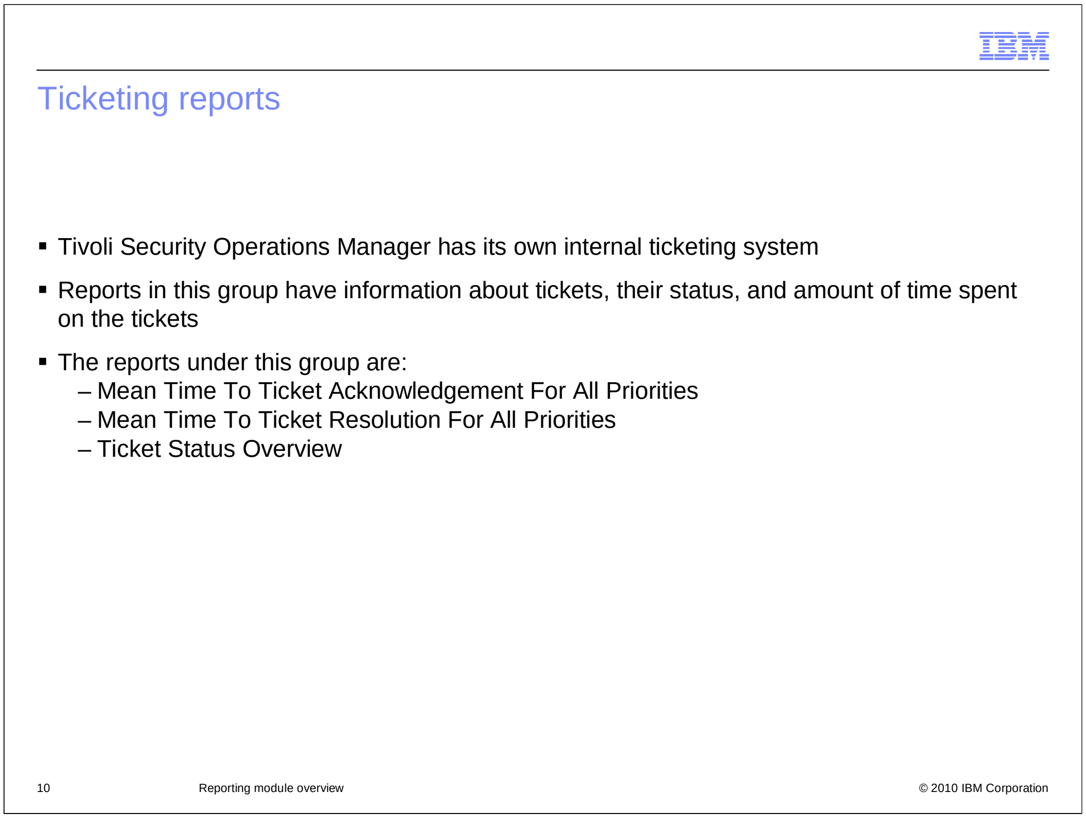
Reports in the Event Activity catalog provide information on total event activity. This activity is based on protocol, event class, or geographic location. The Event Activity reports provide a unique perspective to security analysts about overall event activity. There are multiple reports under this category. Two important reports are Destination Country and Source Country. Tivoli Security Operations Manager supports a geo-lookup server hosted by IBM. If the Central Management Server (CMS) is connected to the internet, Tivoli Security Operations Manager can retrieve the latitudinal and longitudinal information of a particular host, depending on the IP address. This information can be projected onto a world map.



Overview reports

- Reports in the Overview catalog provide:
  - Event activity and associated ticketing and workflow activities that are important to managers
  - Security operations with a high-level view of the activities of the security organization
- An example of an Overview report is the Executive Dashboard
- The reports under this group are:
  - Executive Dashboard
  - Management Event Overview
  - Management Ticket Status Overview
  - Mean Time To Ticket Acknowledgement For All Priorities
  - Mean Time To Ticket Acknowledgement
  - Mean Time To Ticket Resolution For All Priorities
  - Source Country By Event Distribution
  - Ticket Status Overview
  - Top Repeated Connections
  - Top Destination IP
  - Total Ticket Volume For Priorities

Reports in the Overview catalog provide a perspective for managers. This perspective includes event activity and associated ticketing and workflow activities. These reports provide a high-level view of the activities of the security organization. This report set contains some important reports, such as Executive Dashboard. The dashboard provides graphs, showing the security posture and level of your environment. Other reports in this group are listed on the slide.

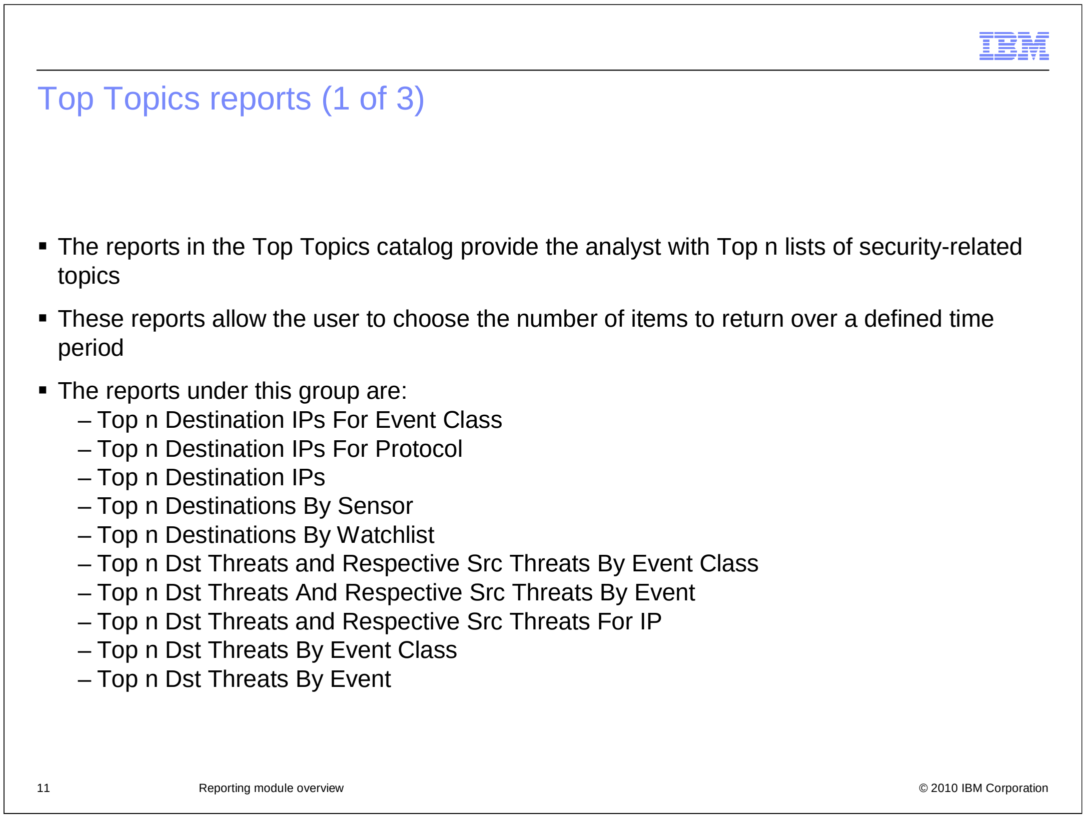


Ticketing reports

- Tivoli Security Operations Manager has its own internal ticketing system
- Reports in this group have information about tickets, their status, and amount of time spent on the tickets
- The reports under this group are:
  - Mean Time To Ticket Acknowledgement For All Priorities
  - Mean Time To Ticket Resolution For All Priorities
  - Ticket Status Overview

10 Reporting module overview © 2010 IBM Corporation

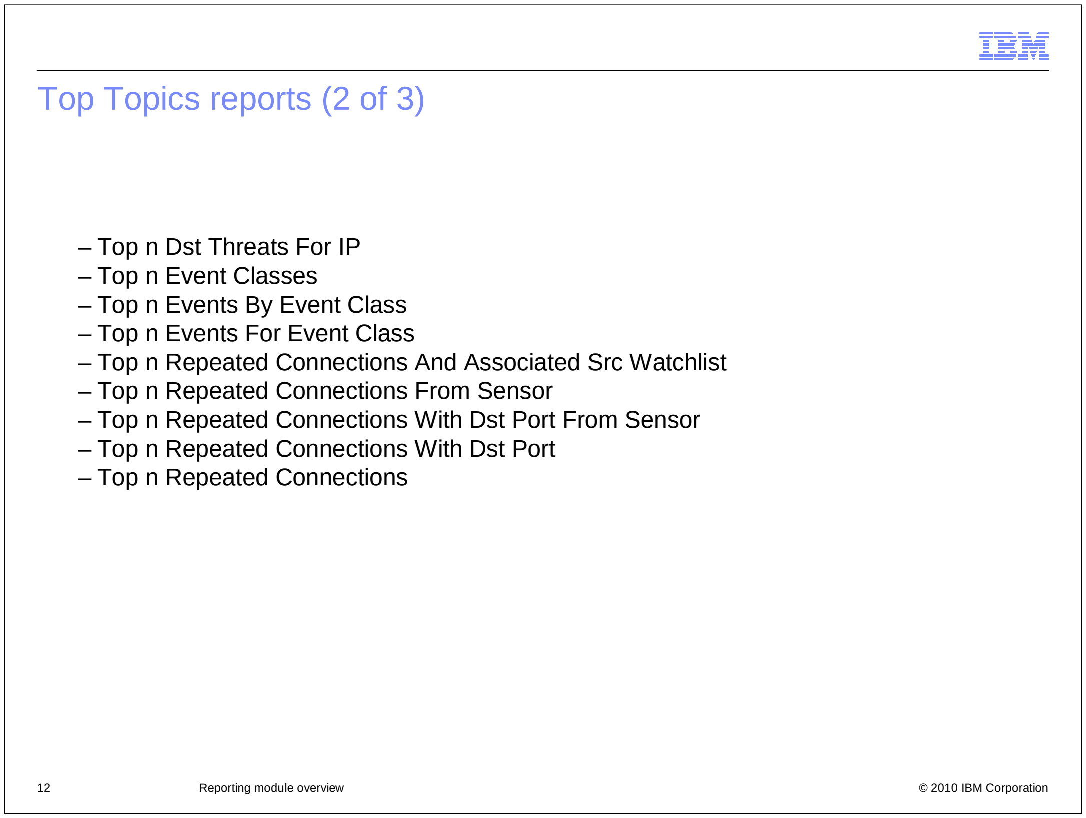
Tivoli Security Operations Manager contains its own internal ticketing system. The reports in this group provide information about tickets, their status, and the amount of time spent on the tickets. The three reports in this group are Mean Time to Ticket Acknowledgement for All Priorities, Mean Time to Ticket Resolution for All Priorities, and Ticket Status Overview.



Top Topics reports (1 of 3)

- The reports in the Top Topics catalog provide the analyst with Top n lists of security-related topics
- These reports allow the user to choose the number of items to return over a defined time period
- The reports under this group are:
  - Top n Destination IPs For Event Class
  - Top n Destination IPs For Protocol
  - Top n Destination IPs
  - Top n Destinations By Sensor
  - Top n Destinations By Watchlist
  - Top n Dst Threats and Respective Src Threats By Event Class
  - Top n Dst Threats And Respective Src Threats By Event
  - Top n Dst Threats and Respective Src Threats For IP
  - Top n Dst Threats By Event Class
  - Top n Dst Threats By Event

Reports in the Top Topics catalog provide analysts with Top *n* lists of security-related topics. A user can choose the number of items to return over a defined period of time. All reports in this group start with Top *n* Destination or Top *n* Destination Threats. The value of *n* is taken from the user when Tivoli Security Operations Manager is running the report. The topmost *n* factors can be represented by the reports that are present under the Top Topic. The Top Topic contains many reports, most of which are self-explanatory.

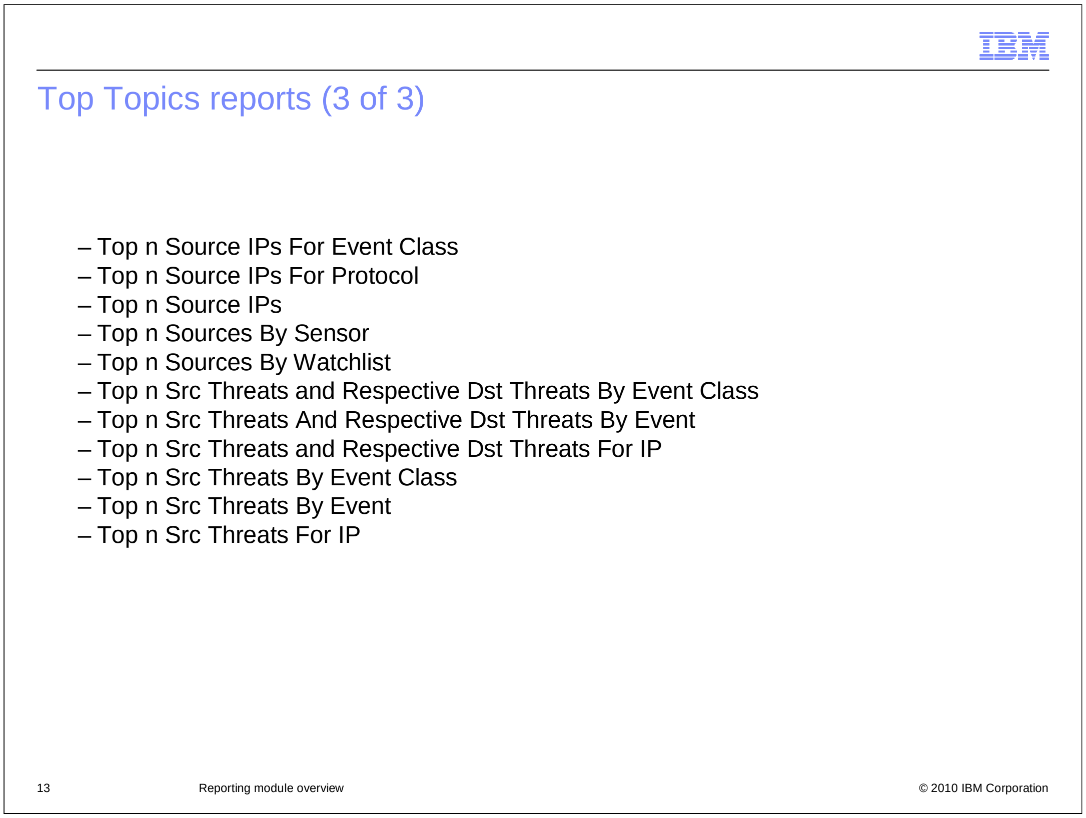


Top Topics reports (2 of 3)

- – Top n Dst Threats For IP
- – Top n Event Classes
- – Top n Events By Event Class
- – Top n Events For Event Class
- – Top n Repeated Connections And Associated Src Watchlist
- – Top n Repeated Connections From Sensor
- – Top n Repeated Connections With Dst Port From Sensor
- – Top n Repeated Connections With Dst Port
- – Top n Repeated Connections

12 Reporting module overview © 2010 IBM Corporation

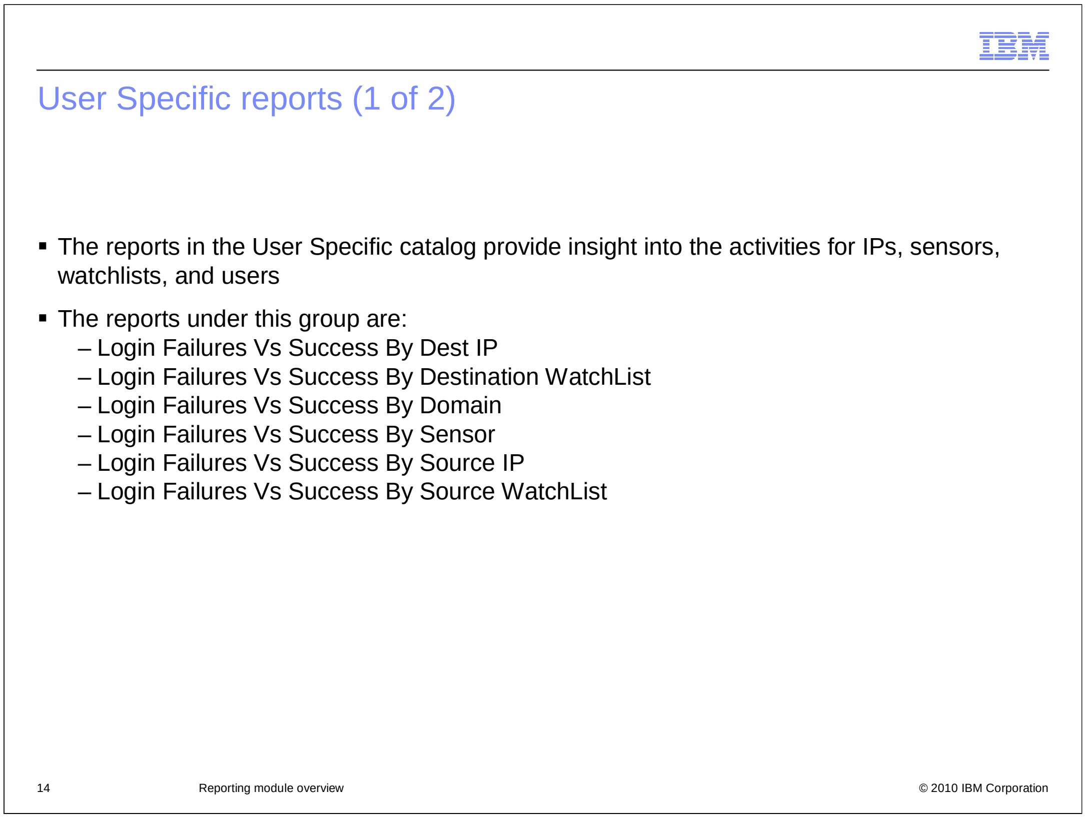
This list is a continuation of the Top Topics reports list.



Top Topics reports (3 of 3)

- – Top n Source IPs For Event Class
- – Top n Source IPs For Protocol
- – Top n Source IPs
- – Top n Sources By Sensor
- – Top n Sources By Watchlist
- – Top n Src Threats and Respective Dst Threats By Event Class
- – Top n Src Threats And Respective Dst Threats By Event
- – Top n Src Threats and Respective Dst Threats For IP
- – Top n Src Threats By Event Class
- – Top n Src Threats By Event
- – Top n Src Threats For IP

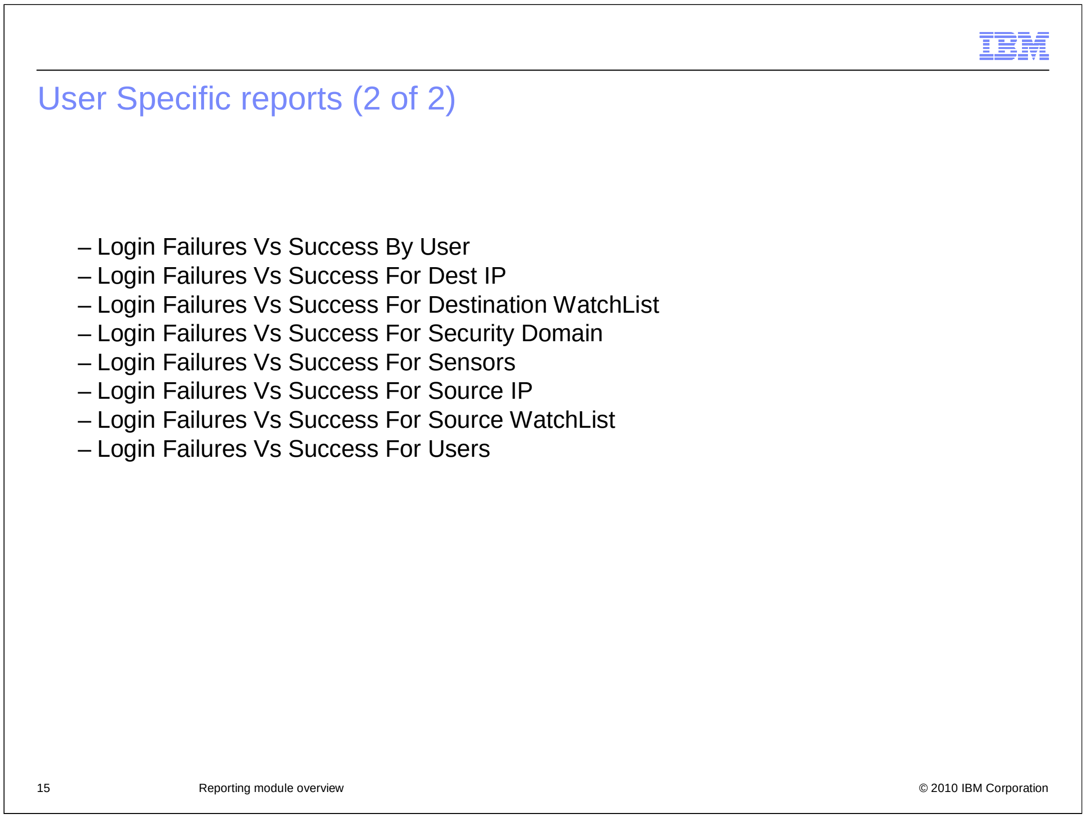
This list is the final section of the Top Topics reports list.



User Specific reports (1 of 2)

- The reports in the User Specific catalog provide insight into the activities for IPs, sensors, watchlists, and users
- The reports under this group are:
  - Login Failures Vs Success By Dest IP
  - Login Failures Vs Success By Destination WatchList
  - Login Failures Vs Success By Domain
  - Login Failures Vs Success By Sensor
  - Login Failures Vs Success By Source IP
  - Login Failures Vs Success By Source WatchList

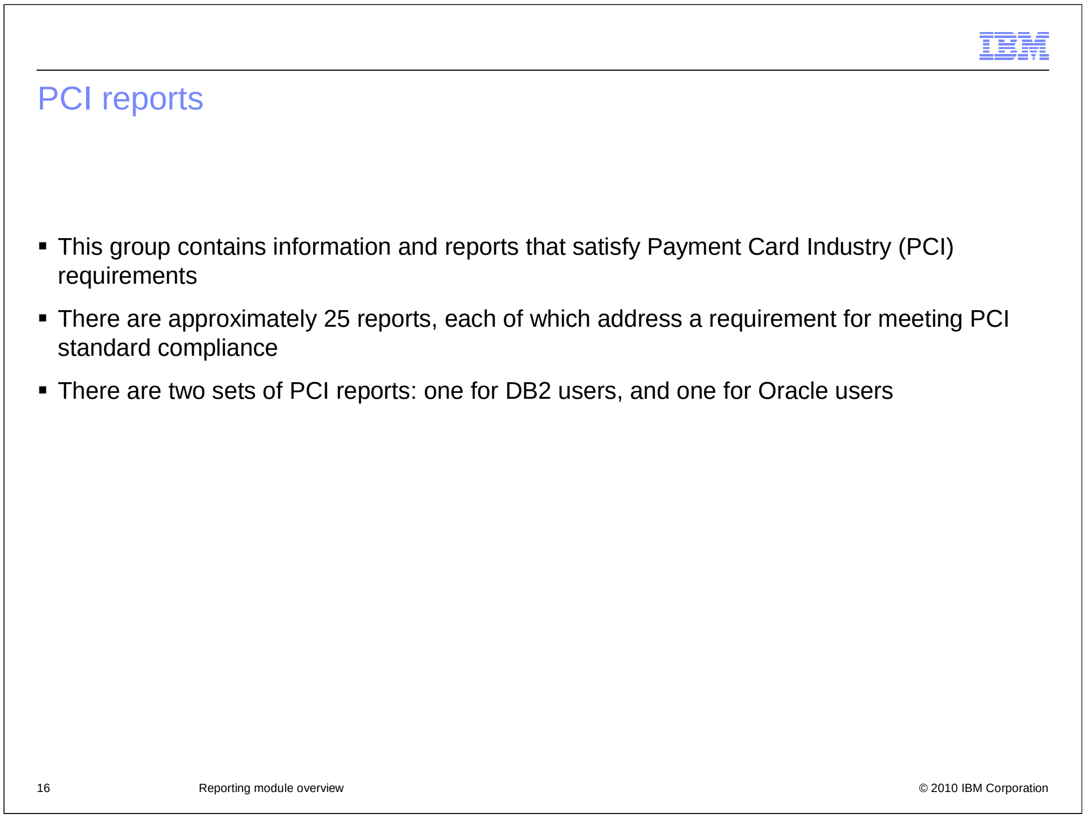
Reports in the User Specific catalog provide insight into IP, sensor, watchlist, and user activities. All the actions performed by different users are in the User Specific group. These actions include logging into a particular computer or network and all the reports that pertain to this information.



User Specific reports (2 of 2)

- – Login Failures Vs Success By User
- – Login Failures Vs Success For Dest IP
- – Login Failures Vs Success For Destination WatchList
- – Login Failures Vs Success For Security Domain
- – Login Failures Vs Success For Sensors
- – Login Failures Vs Success For Source IP
- – Login Failures Vs Success For Source WatchList
- – Login Failures Vs Success For Users

This list is a continuation of the User Specific reports list.

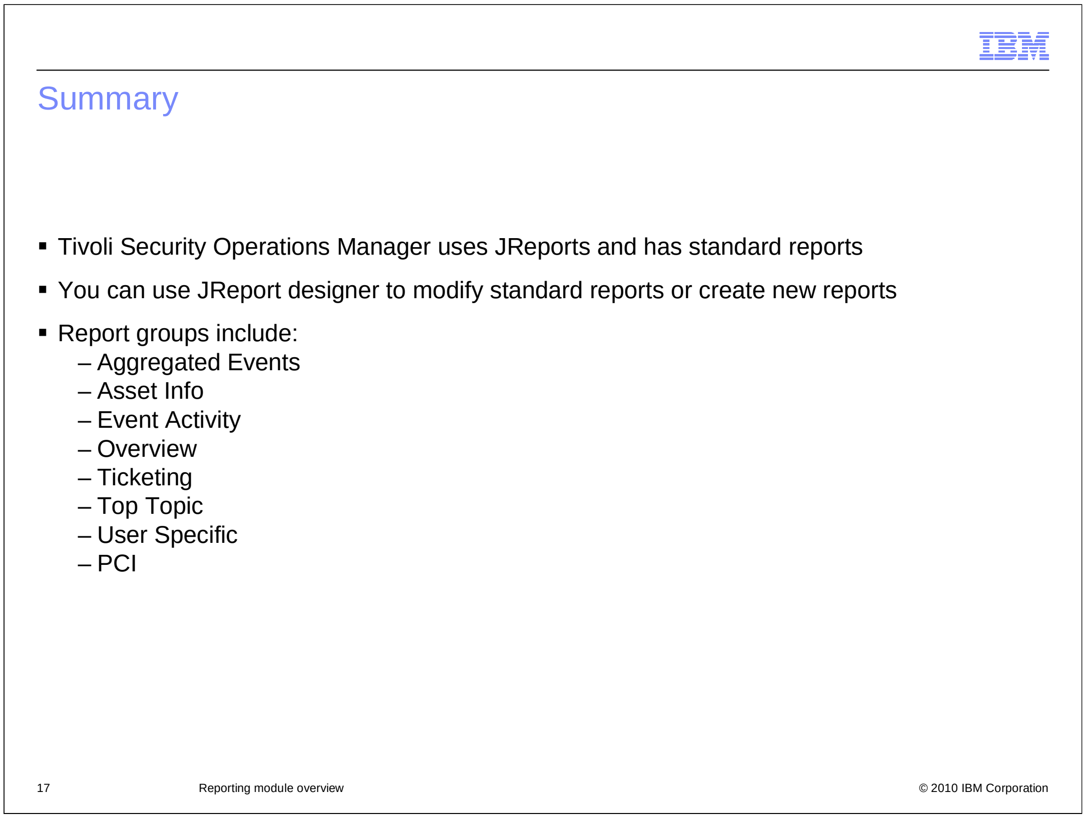


PCI reports

- This group contains information and reports that satisfy Payment Card Industry (PCI) requirements
- There are approximately 25 reports, each of which address a requirement for meeting PCI standard compliance
- There are two sets of PCI reports: one for DB2 users, and one for Oracle users

16 Reporting module overview © 2010 IBM Corporation

The final set of reports is PCI Reports, which were recently added to Tivoli Security Operations Manager. This group contains information and reports that satisfy Payment Card Industry (PCI) requirements. There are several reports cataloged under this group, and there are two sets of PCI reports: one for DB2 users and one for Oracle users.

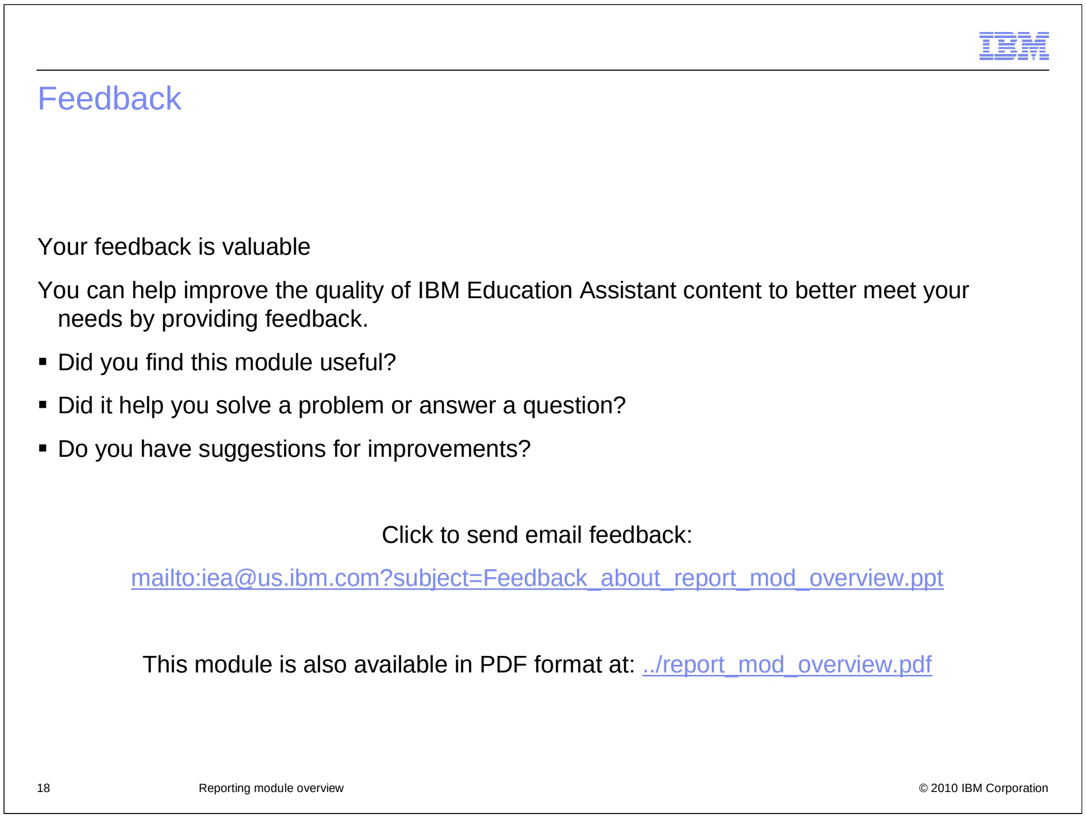


Summary

- Tivoli Security Operations Manager uses JReports and has standard reports
- You can use JReport designer to modify standard reports or create new reports
- Report groups include:
  - Aggregated Events
  - Asset Info
  - Event Activity
  - Overview
  - Ticketing
  - Top Topic
  - User Specific
  - PCI

17 Reporting module overview © 2010 IBM Corporation

In this module, you learned that Tivoli Security Operations Manager uses JReports and also has standard reports. You learned about the types of report groups, and you learned that you can use JReport designer to modify standard reports or to create new ones.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

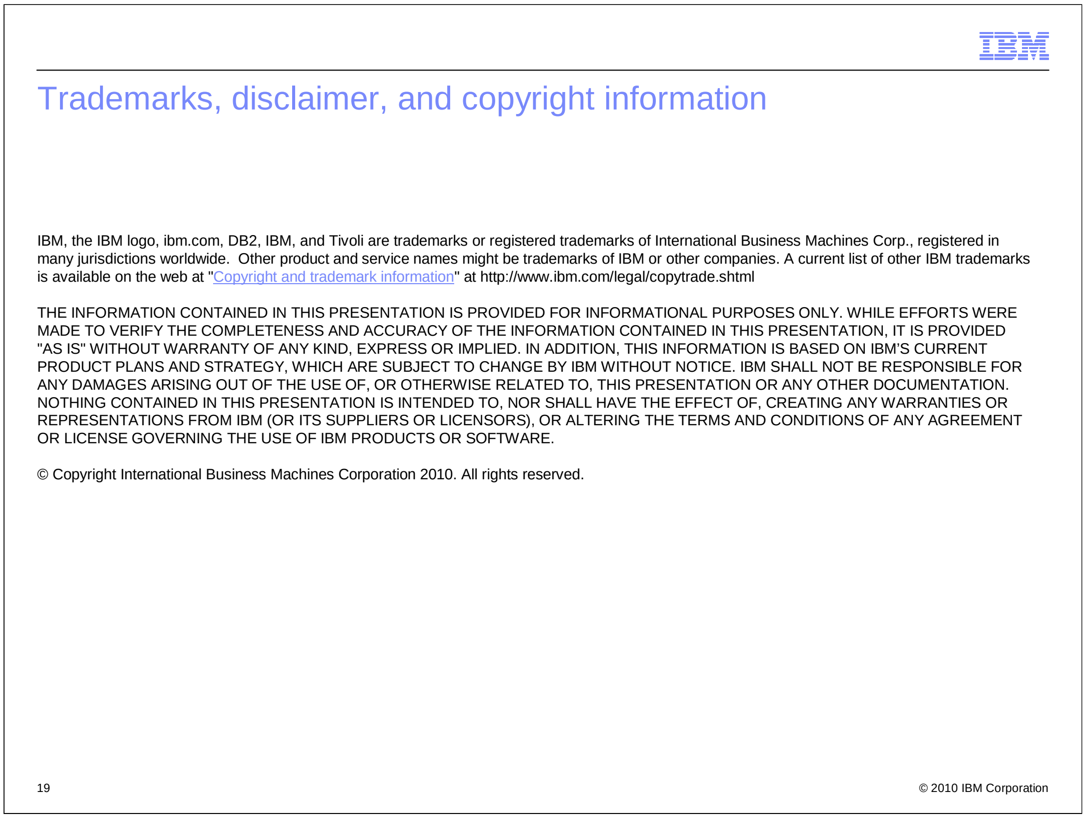
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_report_mod_overview.ppt

This module is also available in PDF format at: ../report_mod_overview.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DB2, IBM, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.