

IBM Software Demos

Tivoli Compliance Insight Manager

Securing the Enterprise and Ensuring Compliance

Introduction

1. (00:00:11.00)

In today's world of increasing regulations and audits, companies must comply with a myriad of rules, such as Sarbanes-Oxley, the Gramm-Leach-Bliley Act, HIPAA, Basel II, and more. Compounding this complexity, recent studies report that privileged users are often the most likely source of risk. Through inadvertent mistakes or malicious activities, this inside risk can cost a company millions.

2. (00:00:22.30)

To know if insiders are following acceptable policies or change management procedures, hundreds of companies today use Consul security solutions from IBM. These organizations rely on the policy-based approach of Consul InSight to simplify insider security auditing, compliance monitoring and enforcement for heterogeneous environments, ranging from mainframes to the desktop.

Demonstration Scenario

3. (00:00:44.40)

The Consul InSight Suite provides the unique ability to capture comprehensive security data, interpret it, and communicate results through a dashboard, for full audit and compliance reporting. To see how this is achieved, let's take a look at Consul InSight Security Manager.

Launch the Compliance Dashboard and maximize its window

4. (00:01:00.00)

The Compliance Dashboard shows you an organization's current state of compliance when measured against an existing policy. The node grid on the left gives you an at-a-glance view of where any issues may exist. The red bubbles on the grid indicate that there are events to explore, and the size of the bubbles give an indication of the total number of events of a specific type. So let's investigate user activities on financial data by viewing the summary of the Finance database.

In the Database Overview section at the bottom of the page, click the Finance icon

5. (00:01:29.00)

Here again we see a warning at the intersection of Sales and Financial Highly Sensitive Data. By clicking on the bubble, we get a list of events.

In the Event information grid, click the large red bubble at the point where "Finance high" and "Sales" intersect

6. (00:01:38.00)

InSight provides the ability to view events in many different ways. Let's sort this list by

IBM Software Demos

Tivoli Compliance Insight Manager

severity and investigate the severe alerts.

In the Event list, click the down-arrow located on the right side of the Severity heading

7. (00:01:45.00)

Here we see that Michael, one of the junior sales account managers, has looked at Salary data. By clicking on the event we drill down into the details.

In the first row of the table, click the date in the When column

8. (00:01:55.00)

Notice that, with a couple of mouse-clicks, we have gone from a graphical overview of the status of Financial data to a detailed view of a specific event. In these details we can clearly see that Michael is part of the Sales group, and that he viewed Financial Highly Sensitive Data over the weekend. Michael should not be able to look at this data, and that's why it's flagged as a policy exception.

9. (00:02:17.00)

A distinctive feature of InSight is that all the events are evaluated against a set of policy rules defining allowed activities. In addition, InSight makes it easy to determine your organization's existing security policy rules by offering a Policy Generator. Let's see why this event is classified as a policy exception.

In the Severity row of the table, click the text **This is a policy exception**

10. (00:02:36.00)

Policy exceptions occur when an event is compared to applicable policy rules and it is determined that the event is not allowed. By looking at the explanation, you can see exactly why this event was exceptional. The rules state that all Financial Highly Sensitive data should be available to members of Financial Management, to the Finance Staff, and to Administrators. However, nowhere do we see a rule allowing members of the Sales group access to this information.

11. (00:03:02.00)

These policy rules are closely related to regulatory requirements, such as those in Sarbanes Oxley. Let's take a look at the add-on compliance modules available for InSight.

At the top of the page, click the Regulations icon

12. (00:03:12.00)

Consul offers a number of regulation-specific compliance modules. All modules contain a set of predefined group and policy rules specific to the regulation, as well as documentation and an extensive list of relevant reports. Let's go to the SOX module and take a look at the set of predefined reports.

Click the red arrow located to the left of Sarbanes Oxley

Click the Reports icon located below Sarbanes Oxley

IBM Software Demos Tivoli Compliance Insight Manager

13. (00:03:31.00)

We were investigating Michael's viewing of a specific, restricted-access file. Now let's take a look at the big picture to determine what other things have happened on the finance data. A useful report for this purpose is the Data Access report.

Scroll down and click **Sarbanes Oxley (12.1.4) Data access**

14. (00:03:49.00)

This report gives a summary of all the events that have happened on SOX-relevant data. This is HR Data, Sensitive Data and Financial Data. Let's filter on Financial Data.

Click the filter icon in the "On What group" column heading

Enter ***Financial*** in the On What Group text field, then click **Apply**

15. (00:04:02.00)

The list gets shorter and here we see that Sales is responsible for 21 events. Let's find out how it is possible that Michael in Sales could access this data in the first place by looking at a standard report.

At the top of the page, click the Reports icon

16. (00:04:14.00)

InSight comes with a long list of predefined standard reports, such as configuration, verification, and investigative reports. In addition, InSight provides a powerful, custom report writer.

Click the red arrow to the left of Daily verification to collapse that section

Click the red arrow to the left of Configuration tools to expand that section

17. (00:04:28.00)

Under the Configuration tools section, we find the Events by Type report. This report provides a summary of all the different events that have occurred.

Click **Events by type**

In the #Events column on the first row of the table, click **12**

18. (00:04:41.00)

In the earlier reports we saw that Michael had looked at financial data and generated some policy exceptions by doing so. We saw that the policy rules don't provide approval for people in the Sales group to access this data.

19. (00:04:53.00)

But Michael was able to access this data, which indicates that someone granted him access privileges. InSight makes it easy to determine who gave Michael these rights. Let's drill down and see what happened.

IBM Software Demos Tivoli Compliance Insight Manager

In the first row of the table, click the date in the When column

20. (00:00:05.06)

As we can see, Eric, an administrator, added Michael to the group Finance02. A little investigation tells us that people in that group have access rights to salary data. Now we know what Michael did and who gave him access. But why did Eric give him these rights? For this question we will take a look at the User History report.

At the top of the page, click the Reports icon

Expand the Detailed investigation section and select **User History**

21. (00:00:05.30)

This report gives a summary of the number of events people triggered during a particular period of time.

On the User History page, under Time period setup, change the Start time to **November 26**, then click the **Execute** button

22. (00:00:05.42)

Here we see that Michael had 21 events on the Finance Server.

In the #Events column, click **21** (third row from the bottom)

23. (00:00:05.46)

Drilling into Michael's events, we see that he first looked at Sales Contracts of U.S. customers. That's probably the reason he was granted rights to this data in the first place.

24. (00:00:05.56)

But after that he also took a look at the Salary data. Michael initially accessed this data five times, which created policy exceptions with a low severity. But as you can see, the three additional accesses have a higher severity.

25. (00:00:06.08)

This information helps security personnel quickly identify suspect behavior, and it enables them to accurately determine how violations of company policy are enabled. With the advanced monitoring and reporting features of the Consul InSight Suite from IBM, you have continuous, non-intrusive assurance, and documentary evidence, that your data and systems are being managed in line with company and regulatory policies.