IBM Software Demos
Tivoli Security User Compliance Management

User Compliance Management Demo

Introduction

Today, most organizations have built a robust security perimeter around their businesses to keep outsiders from accessing confidential data. However, sensitive data, whether intellectual property or customer information, is often exploited by company insiders. In fact, insider threat accounts for almost 80% of data breaches. And protecting data from insiders requires a much different approach to security management.

It requires careful user lifecycle management, where users in your infrastructure are automatically provisioned onto the network, assigned specific privileges and their activity monitored for compliance to your security policies. It also requires that de-provisioning of users be handled in an automated fashion so that once a user's privileges have ended, they no longer have access to your critical data.

It is a challenging proposition to manage all of your users effectively. And it's even more challenging to protect sensitive data from your privileged users. Privileged users are individuals, such as IT Systems Administrators, who require super-user, or root access to be able to do their jobs in configuring systems and diagnosing and solving user problems. These super-users can gain access to and misuse sensitive data, such as personnel records and company proprietary data, either intentionally, or inadvertently. Tivoli's user compliance management solution provides a way to track IT privileged users' logins and audit the databases and information they access.

In this demonstration, you will see how Tivoli's security management products work together to provide an audit trail of unauthorized access when an IT administrator logs in to a human resource database containing sensitive information.

Demonstration

A hypothetical person named Betty Pascal is hired as an IT Specialist. Her new company uses a proprietary personnel management tool called "My People" to add her to an HR application.

- The HR application interfaces with IBM Tivoli Identity Manager, which is used for centralized identification management.
- All data is automatically transferred to Tivoli Identity Manager. Based on the user's attributes, Tivoli Identity Manager automatically provisions the level of access needed to administrate the appropriate resources

The administrator logs into Tivoli Identity Manager to verify that Betty has been added to the system.

Here you can see which resources have been provisioned for Betty: an SAP System and an account for an operating system.

IBM Tivoli Access Manager for Enterprise Single Sign-On provides strong authentication, access automation, and compliance reporting for applications across enterprise end-points. Single sign-on simplifies the end-user experience by: eliminating the need to remember and manage multiple user names and passwords, and by automating sign-on and access levels to various resources.

Betty logs onto her account, sets up automatic login to Lotus Notes and Tivoli Identity Manager.

As time goes by, Betty becomes curious about the salary and benefits of one of her peers, Anne Albert.

Betty logs into SAP. She does not know Anne's personnel number so she uses wildcards to get to her name, and retrieves the number. Then she navigates to Anne's salary page and finds the information she desires.

Since Betty is an IT Specialist and has been given privileged user status, it's easy for her to access the HR database and look up personal data. What Betty doesn't know is that her company has a solution in place which monitors the database access behavior of their employees, even those with privileged user access. Betty is then terminated because her supervisor could see that she inappropriately accessed confidential data.

IBM Tivoli Security Information and Event Manager provided critical monitoring information about Betty's User Activity to the company, and it can do so in real time via alerting policies or historical reports.

To demonstrate, let's sign on using the product's main console and use the iView reporting tool.

Here on the dashboard, a bubble chart summarizes all events, telling us who accessed what, and how that access compares to our security policies.

The blue bubbles indicate permissible activities and the red bubbles signify policy violations.

You can see at a glance that a privileged user has accessed sensitive HR resources.

We drill down to have a deeper look into the events by clicking on the red bubble.

Here we see that Betty (TIM_BPASCAL) has accessed HR data. This is a policy violation because only employees from the HR department should be looking at that data.

To dig a little deeper, we can look at other events related to what Betty was doing around that time. We choose a timeframe of one hour and look at her activities sorted by Severity, which means that the critical items are shown first.

We see that Betty not only looked at HR data, but she also created a new account in the HR database. This is not allowed because only HR employees are allowed to do that.

Additionally, Tivoli Security Information and Event Manager has management modules specific to Sarbanes Oxley, BASEL II, HIPAA, PCI, ISO27001 international regulations and other standards. Each compliance management module includes reports that demonstrate compliance to particular objectives within each regulation.

Let’s take a look at a report regarding access of confidential data that is relevant for the Sarbanes Oxley Act and other regulations supporting financial integrity.

With a click on the policy exceptions you can view all relevant exceptions to the regulations requirements in the event list.

And you can see the event showing that Betty accessed the company’s confidential employee data.

Since Betty has now been fired, she has been automatically de-provisioned. Her record is set to “Terminated” in the HR tool.

The administrator again logs in to Tivoli Identity Manager, and ensures that Betty is listed as “inactive”.

Conclusion

In this demonstration, you have seen how Tivoli Identity Manager, Tivoli Access Manager for Enterprise Single-Sign-On, and Tivoli Security Information and Event Manager work together to address security and policy compliance challenges, including unauthorized access by privileged users.

IBM provides a robust and complete solution to address the user management lifecycle including the critical task of privileged user activity monitoring. This holistic approach to managing user access can improve your risk management strategy and your operational efficiency.