

Quest InTrust Anomaly Analyzer Knowledge Pack

Benefits

- Saves time and improves efficiency by automatically discovering user trends and activity
- Ensures tighter information security by proactively discovering user trends, internal to the network, which might be against company policy
- Enables organizations to proactively look for user trends without prior knowledge of user activity

Understanding user activity at every level and in every application is imperative to the security of all organizations. Whether supporting an internal security requirement or external regulatory compliance initiative, collecting, storing and reporting on this data must be a priority for any IT organization.

Although most organizations have enabled auditing at all levels, they oftentimes find it difficult to trend user activity against such things as file access, successful logons and Web access by user. By automatically setting a baseline of user activity, organizations can discover an anomaly to their normal routines and therefore be pro-active in stopping a violation to corporate policy.

In order to better secure the network and its assets, companies must pre-determine user trends on activity such as:

- Successful logons (times and location of logons)
- Web server access
- File access

To successfully trend users' actions, logs must be kept for an extended period of time. In order to meet these requirements and recognize a return on investment, companies must implement a scalable solution with cost effective long term storage.

The Quest InTrust® Anomaly Analyzer Knowledge Pack can help. It automates the process of collecting, storing, reporting and trending user activity.

Having this information available, even without prior knowledge of a user's activity, makes this a very powerful tool for security administrators. For example, users accessing the network during non-business hours might trigger an investigation into their activity. This investigation could then turn up misuse of privileges by the user in question and save the company valuable time and money.

Reports can be generated on a daily, weekly or quarterly basis depending on a company's needs. The figure below represents a view into an anomalous event showing that this user doesn't normally logon this particular day of the week.

Anomalous event details

Date/Time	5/31/2005 3:00:45 PM
Day of the week	Tuesday
User	OSQA\spike2
Workstation	ABOO
Server	ABOO
Event	528 - Success
Logon type	Service
Rate of commonness	0.077316

Uncommonness of each parameter:

User	0.06
Server	0.03
Workstation	0.04
Event	0.13
Logon type	0.14
Date	0.27
Day of week	0.27
Hour	0.05

Figure 1: Anomaly Analyzer Knowledge Pack Report Sample

Having this functionality means that companies can proactively monitor their users' trends and potential misuse of privileges, which might lead to a violation of corporate policy.

For more information on how InTrust can help your organization address internal security mandates and external compliance requirements, regardless of your environment, visit <http://wm.quest.com/products/intrust/>.