Lepide

Datasheet

Sarbanes-Oxley Act

SOX Compliance

To meet IT standards of SOX, organizations must regularly audit their entire IT infrastructure and keep a record of all changes made. Auditing Windows Server, Active Directory, File Server, and other server components natively is a very complex and time-consuming process. For instance, an IT Administrator could waste a full working day tracking just user logon and logoff activities due to the volume of data they will need to sift through. With over 270 pre-defined reports, Lepide gives IT teams the power to easily adhere to the requirements of SOX compliance.

Secure SOX Data

Ensure users aren't accessing data related to SOX unless they require that access to perform their job role.

Monitor Access to SOX Data

Monitor and alert on all user behavior relating to data that falls under SOX compliance regulations.

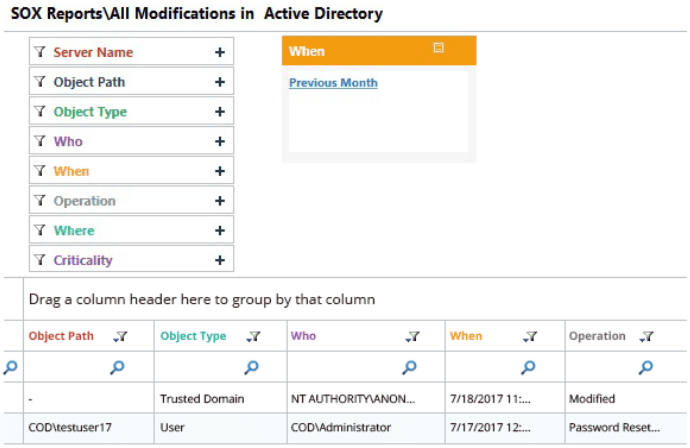
Pre-Set SOX Reports

Numerous pre-defined reports tailored to meet some of the more stringent auditing aspects of SOX compliance.

How Lepide Helps

Monitor All Changes in IT Environment

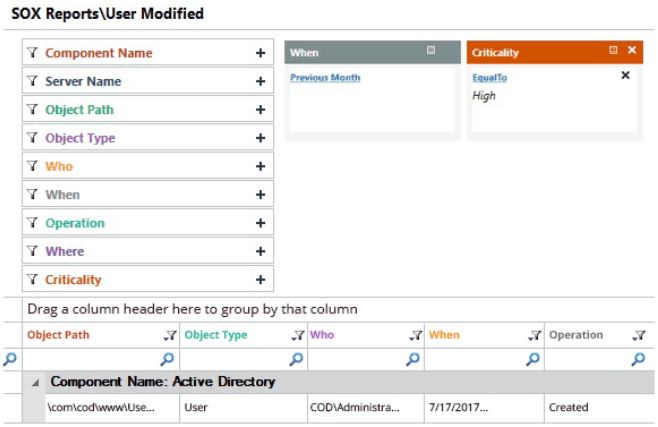
Organizations are required to audit all aspects of their IT environment; including Active Directory, Group Policy Objects, Exchange Server, SharePoint, SQL Server and File Server, NetApp Filer, Office 365 and Dropbox. Native auditing suffers from numerous drawbacks that can be difficult to overcome, such as creation of multiple event logs for a single change, the absence of pre-defined reports and more storage consumption. Lepide helps you overcome these limitations and provides continuous auditing of these server components from a single dedicated platform. It can also be configured to notify you of critical changes in real-time through email or push-notifications to the Android/Apple App.



Audit Changes in Users of Financial Data

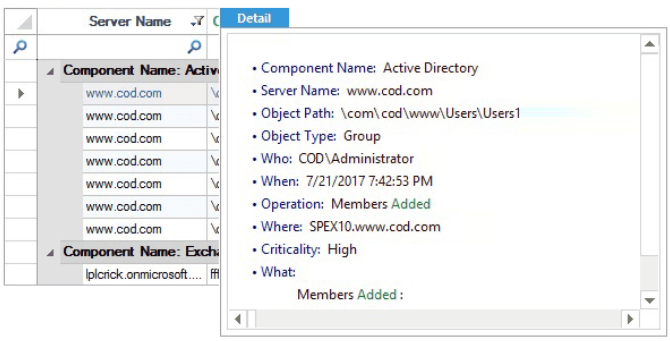
Changes in the accounts of users that process Financial Data should be properly audited. Any critical change in their configuration should be immediately brought to the attention of IT administrators.

Our solution monitors every change made in the configuration of Active Directory users, Exchange user mailboxes, SharePoint users and SQL users. It also tracks all changes made in user permissions for all vital server components.



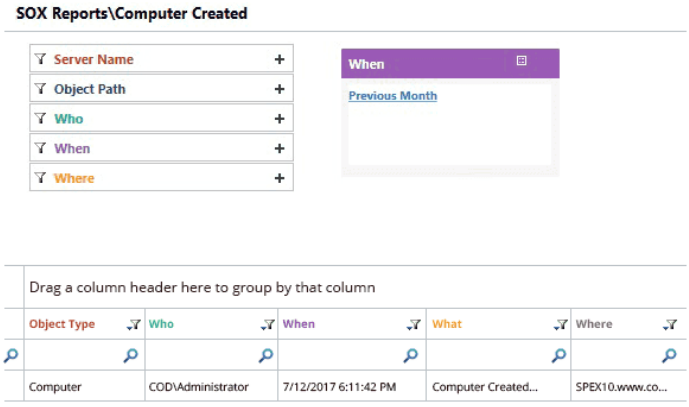
Audit Changes in Groups of Users

User Permissions are generally delegated by group memberships. Therefore, a sudden new membership could lead to full administrative privileges being given unexpectedly to a regular user account. To prevent this obvious threat to security, it is required to track changes in groups and their memberships. Predictably, native methods can be very complex when it comes to tracking these changes. Lepide, however, tracks and alerts on all changes made in groups and group memberships automatically.



Audit Changes in Computer Objects

Computers are configured as objects in Active Directory so that they can be a part of organization's network. An unwanted change made in the configuration of computer object can disconnect that computer from the network; blocking it from accessing the network resources, server programs and data. Lepide audits all changes made in the configuration of computer objects and sends real-time alerts to selected recipients via email and push-notifications to the Lepide Mobile App.



Audit Changes in Windows Server

If the configuration is wrong, the Windows Server operating system can malfunction. If the Operating System is experiencing problems, then all services, data and user authentication hosted through the concerned primary domain controller may be unavailable. This downtime can be damaging to the organization. To avoid such issues, it is recommended to audit all changes made in the configuration of Windows Server; such as changes in the NTDS folder, Sites, subnets, Schema, DNS Zone, or other AD Configuration changes. Lepide does this all with its pre-defined audit reports.

It also takes regular backup snapshots of the state of Active Directory objects and Group Policies, which can then be used to restore unwanted changes and deleted objects.