Lepide

Datasheet

FISMA

FISMA

Even if NIST framework is in place, it can still be quite difficult for an organization to ensure that their IT security standards comply with FISMA regulations. The best way to do this is through a stringent IT auditing strategy.

Native Auditing through the Event Viewer suffers from numerous drawbacks; and using it can often take an inordinate amount of time to track a single user action.

Our solution tracks user behavior and access to data across on-premise, cloud and hybrid environments and provides you with reports directly relevant to the specific standards required by FISMA.

Secure FISMA Data

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

Monitor Access to FISMA Data

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

Pre-Set FISMA Reports

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

How Lepide Helps

Audit Changes in Password Policies

Passwords are crucial to maintaining IT security in the environment. Organizations define password policies through domain-wide Group Policy Objects. Any unexpected changes in these policies can weaken IT security and allow users an opportunity to violate security standards. Lepide audits every change in Group Policy Objects, including password policies, and sends real-time alerts through email, or push notifications to the Lepide Mobile App, when any such critical changes are detected.

Audit Changes in Logon/Logoff Policies

Logon/logoff policies define the rules of user logons and logoffs. These policies are crucial to maintaining the security of IT infrastructure. Any sudden change to these policies can potentially be damaging, so FISMA requires you to keep track of them. Lepide monitors all changes in the logon/logoff policies and records them in pre-defined reports. You can configure settings to receive real-time alerts through email or notifications to the Lepide Mobile App. You can restore the entire Group Policy Object to its original state with a few clicks.

Changes in Group Memberships

Mostly the permissions to users are assigned through groups in Active Directory, Exchange Server, SQL Sever and SharePoint. Any change in group memberships will modify the permissions held by a particular user – and this can result in inappropriate or unauthorized levels of privilege. Lepide monitors every change in the group memberships and highlights them in pre-defined reports.

Changes in Account Lockout Policies

If a user has made multiple failed attempts to logon at a computer, as per security standards, that user account should be locked out immediately as there could be foul play. The provision to lock a user account is applied through the Group Policy Object, and any change in that policy may give privileges to an intruder to use multiple password combinations to login from a trusted account. Lepide continuously monitors the changes made in user account policies and alerts on them in real-time. Once notified, you can use Lepide itself to restore the state of Group Policy to its original one.