pathlock

An Insider Threat Checklist for Your Business - Critical Applications

The ten things you should do to ensure business application users don't commit fraud or jeopardize sensitive data.

Ensure User Credentials Have Expiration Date

When you create a temporary or privileged user in your application, you must have procedures in place to ensure the User ID has a defined expiration date.

Automate the Deactivation of IDs

ID expiration dates should be used to automatically deactivate the credentials of temporary or privileged users to ensure access is only available when needed.

Don't Waste Time and Resources Reviewing Logs

Analyze user sessions, events, activities and master data changes for access or rule violations automaticaly and only spend time reviewing violations.

Automatically Detect Anomalous Behavio

Utilize a solution that alerts you to actions that deviate from the norm. For example, a user who rarely accesses customer information exports a batch of customer records.

Know When Your Application Is Accessed & What Users Are Doing

Receive alerts automatically when privileged users access your application or are doing something they shouldn't be.

Keep Up-to-Date on Ever-Changing Roles & Responsibilities

Review user access periodically to ensure users only have access to data and functions they need to do their job.

Keep an Audit Log to Show What Data Has Changed

You can't understand and protect against the inside threat without a record that clearly identifies WHAT data was changed and HOW it was changed.

Fully Document Reasons for Exceptional Access

In order for businesses to function, you may need to grant exceptional access. Keep a system of record to detail who, what, when, where, how and why access was granted.

Prohibit the Use of Shared System and Database Admin Passwords

If you don’t have a system in place to prevent it, you know all too well that users will share IDs and passwords, making it easier for the insider to access critical data.

Prevent Audit Trail Manipulation with an Independent System

By implementing an independent system, you ensure that a user is unable to cover their tracks by altering audit logs.