Practical Assessment: IAM

Oscorp's new medication has finally hit the market and it's been a great success. However, the formula of the medication remains a secret. The formula is considered Oscorp's most sensitive asset.

There is a lot of documentation related to this secret formula and it's all stored in a Microsoft SQL Database server 2022.

Problem:

You conducted an assessment on the application, and you found that any employee who is a member of the research lab has read access to the formula. You also found that Harry Osborne has full admin access to the database. Employees can login to the database using a username and a password.

What will your recommendation be to secure Oscorp's most sensitive asset, from an identity and access management point of view?

Your answer

Will recommend Oscorp to use principle of least privilege and separation of duties and then to have a Privilege access management tool in place.

The following IAM recommendations will uplift the security of the data:

Multi-Factor Authentication

- An enterprise wide two-factor authentication system to be rolled out for all employees to access Oscorp's environment.

- An additional multi-factor authentication to be required to access the database. This could be a biometric solution such as fingerprints.

- An approval process should be in place whenever someone wants to access the system.

Principle of Least Privilege

- Restrict access to the formula only to those who absolutely need it for their job function. Not all members of the research lab should have read access.

- Implement Role-Based Access Control (RBAC). Access to the formula should be assigned to a 'role'. Individuals who need access to the formula should be assigned the role temporarily for the duration of their need. Access should be revoked after the task is complete.

Separation of Duties

- Harry Osborn shouldn't have this much power. Instead, separate the full access by two accounts. One for Harry's daily usage (read only), and only an admin account for write access. Require formal approval from two executives to get temporarily access to the admin account.

User Access Reviews

- Recommend regular access reviews for this critical application.

Recommendations:

GRC Mastery by Abed Hamdan