Recommendation to Secure Oscorp’s Sensitive Formula

Scenario-
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?

(Identity & Access Management Focus)

To protect Oscorp’s most sensitive asset, the proprietary medication formula is stored in a Microsoft SQL Server 2022 database.

I recommend strengthening identity and access management controls using a **least-privilege, zero-trust approach**.

1. Implement Privileged Access Management (PAM)

Oscorp should deploy a Privileged Access Management solution such as **CyberArk** to secure administrative and high-risk access to the database. PAM would allow privileged credentials to be vaulted, rotated automatically, and accessed only for a limited, approved time window. This reduces the risk of credential theft and prevents attackers from maintaining persistent access if an account is compromised.

Time-bound access ensures that even if an authorized user’s credentials are exposed, the attack surface remains minimal and short-lived.

2. Enforce Role-Based Access Control (RBAC) and Least Privilege

Access to the formula should be strictly limited based on job role and business necessity.

- Remove blanket read access from all research lab employees immediately
- Grant access **only** to individuals actively working on the formula

- Ensure each role has the **minimum permissions required** to perform its duties

For example:

- Researchers may only view specific portions of the documentation
- Senior scientists may access broader sections
- Database administrators manage infrastructure but do not automatically access sensitive data

This prevents unnecessary exposure while maintaining operational efficiency.

3. Reduce and Secure Administrative Access

Currently, Harry Osborn has full administrative access to the database, which represents a **single point of failure**.

Recommendations:

- Limit the number of database administrators
- Separate administrative duties from data access
- Require PAM approval and session monitoring for all admin-level actions

Administrative access should be auditable, monitored, and granted only when required.

4. Enforce Strong Authentication Controls

To further harden access:

- Implement **Multi-Factor Authentication (MFA)** for all database logins
- Require strong password policies with regular rotation
- Eliminate shared credentials entirely

This significantly reduces the risk of credential-based attacks.

5. Apply Data Segmentation and Tiered Access

The formula documentation should be segmented into multiple sensitivity levels.

- Users only see the portions required for their role
- Higher sensitivity levels require additional approval and stronger controls
- Full access is restricted to tightly monitored, privileged sessions

This layered approach limits the impact of insider threats and compromised accounts.

Conclusion

By implementing Privileged Access Management, enforcing RBAC and least privilege, securing administrative access, enabling MFA, and segmenting sensitive data, Oscorp can significantly strengthen the protection of its most valuable intellectual property. These controls reduce both insider risk and external attack exposure while maintaining controlled, auditable access to critical assets.