Access Control Assignment

Ryan Coon

CYB-515

Dr. Edward Marchewka

September 18, 2024

**Explain what enterprise credential management and privileged access management are, and provide at least one example of each.**

Enterprise Credential Management (ECM) refers to the systematic management of digital credentials, including passwords, keys, and tokens, that are used to access various enterprise resources. The primary goal of ECM is to ensure that credentials are securely stored, managed, and distributed to authorized users while minimizing the risk of unauthorized access. This process often involves the use of tools that automate credential rotation, enforce password policies, and provide reporting capabilities to track access and usage.

Example: A company using a password manager like LastPass or Dashlane to securely store and manage employee passwords across various applications. The password manager can automatically generate strong passwords, facilitate password sharing securely among team members, and alert users when passwords need to be updated.

Privileged Access Management (PAM) focuses specifically on managing and controlling access to critical systems and sensitive data by users with elevated privileges. PAM solutions help organizations enforce the principle of least privilege, ensuring that users only have access to the resources necessary for their job functions. This reduces the risk of data breaches and insider threats.

Example: A financial institution implementing CyberArk to manage and monitor access to its financial systems. CyberArk can secure privileged accounts, enforce access controls, and generate audit logs to ensure compliance with regulations while detecting any suspicious activities related to privileged access.

Discuss why they are important to a company's cybersecurity defense posture and describe how the two are connected.

ECM ensures that digital credentials, such as passwords and tokens, are securely stored and managed. By automating credential rotation and enforcing strong password policies, ECM reduces the risk of credential theft and unauthorized access, which can lead to data breaches.

PAM, on the other hand, specifically focuses on controlling access for users with elevated privileges. Privileged accounts often have access to critical systems and sensitive data, making them prime targets for cyberattacks. PAM solutions enforce the principle of least privilege, ensuring that users only have access to the resources necessary for their job roles.

The connection between ECM and PAM lies in their complementary roles in managing access. Effective ECM lays the groundwork for PAM by ensuring that all credentials, including those for privileged accounts, are securely managed. When combined, they create a robust framework that enhances overall security, minimizes attack surfaces, and helps organizations maintain compliance with regulations, ultimately strengthening their cybersecurity defense posture.

Develop a specific plan for the implementation of access controls in your company.

Step 1: Assessment and Planning

Identify Resources

Define Roles and Responsibilities

Conduct Risk Assessment

Step 2: Policy Development

Access Control Policy: Create a formal policy outlining:

User access levels

Authentication methods

Compliance requirements

Step 3: Technology Selection

Choose Access Control Solutions:

Identity and Access Management (IAM) systems

Role-Based Access Control (RBAC) tools

Privileged Access Management (PAM) solutions

Step 4: Implementation

Configure Access Controls

Integrate with Existing Systems

Step 5: Training and Awareness

User Training

Awareness Campaigns

Step 6: Monitoring and Review

Regular Audits

Continuous Monitoring

Feedback Loop

Step 7: Documentation

Maintain Records