

11.1. Access Control Mechanisms

Access control mechanisms are essential components of the Spectra360 Security Operations Center (SOC) platform, ensuring that only authorized individuals can access specific resources within the system. These mechanisms help protect sensitive data and maintain the integrity of the organization's information systems.

Key Access Control Models:

1. **Discretionary Access Control (DAC):**

- In DAC, the data owner determines who can access specific resources. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions.

2. **Mandatory Access Control (MAC):**

- In MAC, users do not have much freedom to determine who has access to their files. For example, security clearance of users and classification of data (as confidential, secret, or top secret) are used as security labels to define the level of trust.

3. **Role-Based Access Control (RBAC):**

- RBAC allows access based on the job title. RBAC largely eliminates discretion when providing access to objects. For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.

4. **Attribute-Based Access Control (ABAC):**

- ABAC grants access rights to users through the use of policies which evaluate attributes (user attributes, resource attributes, and environment conditions).

Implementation in Spectra360 SOC Platform:

The Spectra360 SOC platform employs a combination of these access control models to ensure robust security:

- **User Authentication:** Verifying the identity of users through methods such as passwords, biometric scans, or security tokens.
- **Authorization:** Assigning access rights based on user roles, attributes, or predefined policies to ensure users can only access resources necessary for their duties.
- **Audit Trails:** Maintaining logs of user activities to monitor access patterns and detect unauthorized actions.

Best Practices:

- **Principle of Least Privilege:** Grant users the minimum level of access necessary to perform their job functions.
 - **Regular Access Reviews:** Periodically review and update access permissions to accommodate changes in roles or responsibilities.
 - **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security beyond just passwords.
 - **Continuous Monitoring:** Regularly monitor access logs to promptly identify and respond to unauthorized access attempts.
-

Revision #3

Created 9 February 2025 21:06:22 by Admin

Updated 10 February 2025 10:52:07 by Admin