

11.2. Role-Based Permissions

In the Spectra360 Security Operations Center (SOC) platform, implementing role-based permissions is essential for managing access to sensitive information and system functionalities. This approach ensures that users have the appropriate level of access required to perform their duties, thereby enhancing security and operational efficiency.

Role-Based Access Control (RBAC):

RBAC is a method of managing access to computer systems or networks based on the roles of individual users within an organization. Instead of granting permissions directly to users, RBAC assigns permissions to roles, and users are then assigned to specific roles. This approach simplifies access management by allowing administrators to assign and revoke access based on job responsibilities, reducing the complexity of managing individual user permissions.

Key Components of RBAC:

1. **Roles:** Defined based on job functions within the organization, such as SOC Analyst, Incident Responder, or SOC Manager.
2. **Permissions:** Specific access rights assigned to roles, determining what actions users in those roles can perform within the SOC platform.
3. **Users:** Individuals assigned to roles, inheriting the permissions associated with those roles.

Implementation Steps:

1. **Define Roles:** Identify and create roles that reflect the various job functions within the SOC.
2. **Assign Permissions:** Allocate appropriate permissions to each role, ensuring alignment with job responsibilities.
3. **Assign Users to Roles:** Map users to roles based on their job functions, granting them the corresponding permissions.

Benefits of Role-Based Permissions:

- **Enhanced Security:** Limits access to sensitive information and critical system functions to authorized personnel only.
- **Simplified Management:** Streamlines the process of assigning and revoking access rights as users change roles within the organization.

- **Regulatory Compliance:** Helps meet compliance requirements by enforcing strict access controls and maintaining detailed access records.
-

Revision #3

Created 9 February 2025 21:06:29 by Admin

Updated 10 February 2025 10:52:14 by Admin