DORT

The Role of Identity in Existing Security Frameworks

Mapping Identity and Access Controls to CIS CSC and NIST CSF

The Role of Identity in Existing Security Frameworks

Identity already plays an important role in many security frameworks and is critical to any zero trust strategy. They fall into six areas: identity inventory, MFA, Access Control, IAM Hygiene, Log Collection, and Session Management.

We've mapped the CIS Critical Security Controls (CIS Controls) and the NIST Cybersecurity Framework to these six areas.

	CIS CSC	NIST CSF
Identity Inventory	**CIS CSC 5.5** Establish and Maintain an Inventory of Service Accounts **CIS CSC 5.6** Centralize Account Management **CIS CSC 6.6** Establish and Maintain an Inventory of Authentication and Authorization Systems	**NIST CSF PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Multi-Factor Authentication	**CIS CSC 6.3** Require MFA for Externally-Exposed Applications **CIS CSC 6.4** Require MFA for Remote Network Access **CIS CSC 6.5** Require MFA for Administrative Access	**NIST CSF PR.AC-7** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Inactive Accounts and Hygiene Issues	**CIS CSC 5.3** Disable Dormant Accounts	
	CIS CSC 4.7 Manage Default Accounts on Enterprise Assets and Software	

	CIS CSC	NIST CSF
Access Control	**CIS CSC 6.1** Establish an Access Granting Process	**NIST CSF PR.AC-3** Remote access is managed
	CIS CSC 6.2 Establish an Access Revoking Process	**NIST CSF PR.AC-4** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
	CIS CSC 6.7 Centralize Access Control	**NIST CSF PR.IP-11** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
	CIS CSC 6.8 Define and Maintain Role-Based Access Control	
Collecting Logs	**CIS CSC 8.12** Collect Service Provider Logs	**NIST CSF DE.AE-3** Event data are collected and correlated from multiple sources and sensors
	CIS CSC 8.2 Collect Audit Logs	**NIST CSF DE.DP-4** Event detection information is communicated
Session Management	**CIS CSC 4.3** Configure Automatic Session Locking on Enterprise Assets	