TYPES OF PRIVILEGE ACCOUNTS YOU SHOULD BE AWARE OF

	USE	ATTACK VECTORS	HOW TO PROTECT
ROOT OR SUPER USER ACCOUNTS	Has highest level of access & control over a system or network. They are typically used for system maintenance, configuration, & installation of software or updates	Attackers often target these accounts through vulnerabilities in operating systems or through social engineering to obtain or exploit root access	Implement strong authentication, regularly update the OS, use intrusion detection systems (IDS/IPS), restrict access to trusted administrators.
ADMIN ACCOUNTS	Administrator accounts are prevalent in Windows environments and have extensive access privileges to manage user accounts, install software, and configure system settings.	Attackers may exploit vulnerabilities, use brute force attacks, or engage in privilege escalation to compromise administrator accounts.	Enforce strong password policies, implement two-factor authentication (2FA), restrict administrative access to necessary personnel, regularly patch Windows systems.
DATABASE ADMIN ACCOUNTS	DBAs manage and maintain database systems, controlling access to databases, running backups, and optimizing performance.	Attackers may exploit weak database configurations, SQL injection vulnerabilities, or gain access through phishing attacks on DBAs.	Use strong database access controls, regularly update the database software, apply least privilege principles, monitor database activity.
SERVICE ACCOUNTS	used by applications or services to access databases, servers, and other resources. They are often configured with elevated privileges.	Attackers can compromise these accounts through vulnerabilities in the applications they serve, weak or leaked credentials, or privilege escalation.	Protect the applications, limit service account privileges to what's necessary, secure and regularly rotate service account passwords, monitor service account activity.
APPLICATION ACCOUNTS	These accounts are used to run specific applications or services with predefined permissions to carry out specific tasks.	Attackers may target application vulnerabilities, exploit weakly configured permissions, or use stolen or leaked credentials to gain unauthorized access.	Secure the applications, apply principle of least privilege to application accounts, enforce strong authentication, regularly monitor and audit application account activity.
VENDOR OR THIRD PARTY ACCOUNTS	Third-party vendors may require privileged access to provide support or services to organizations.	Attackers can compromise these accounts through supply chain attacks, social engineering, or exploiting weaknesses in the vendor's security practices.	Vet and audit third-party vendors, restrict external access, require strong authentication and access controls for third-party accounts, monitor third-party activity.
PRIVILEGED USER ACCOUNTS	Privileged user accounts are used by employees or administrators who need elevated access for specific tasks, such as network configuration, server management, or security monitoring.	Insider threats, social engineering, or phishing attacks may be used to compromise privileged user accounts.	Educate employees on security best practices, enforce strong password policies, regularly monitor and audit privileged user account activity, implement user behavior analytics.
EMERGENCY BREAK-GLASS ACCOUNTS	These accounts are typically reserved for emergency access to systems or data when standard access is unavailable.	Attackers may target these accounts through weak password management, unauthorized access, or exploiting the emergency access procedures.	Encrypt and protect emergency account credentials, restrict access to break-glass accounts to a few trusted individuals, implement strong multi-factor authentication for emergency access.
SHARED ACCOUNTS	These accounts are typically used by multiple users for specific tasks. It would used as a shared access for designated purposes	Password sharing, weak access controls, unauthorized access and lack of individual accountability	Implement strong access controls, enforce individual accountability for shared account usage, regularly change shared account passwords, and audit shared account activity.