Business Requirement document	
The current Business problem	1. Ineffective Onboarding process for privileged accounts 1.1 Operational inefficiency The onboarding is done manually and take in average 3 days per account. That results in a 20% error rate in privilege assignments, delaying IT operations and disrupting workflows. For example, in 2024, configuration errors delayed critical application deployments by 48 hours. 2. Generic & unmanaged accounts Most privileged business and IT users rely on a single account for all operations. An audit in 2024 identified 150 shared "admin" accounts and forgotten system accounts, leading to untraceable actions and increased security risks. 2.1 A rising of credential theft Over the past two years, phishing and credential stuffing attacks caused a 30% increase in compromised administrator credentials, enabling attackers to bypass security controls. 3. Lack of authorisation or Access Control Processes 3.1 An increase in sensitive data leaks The absence of granular access controls has led to a 25% increase in sensitive data leaks over the past three years. For instance, in 2023, a contractor with excessive privileges exposed 10,000 customer records, both inadvertently and maliciously. 3.2 Frequent critical system outages Misconfigured privileges caused 10 major outages in critical Windows and Unix servers in 2024, resulting in an average downtime of 6 hours per incident and significant operational disruptions. 4. Inefficient monitoring of privileged accounts 4.1 Financial fraud In 2024, a compromised administrator account led to €500,000 in financial fraud due to unmonitored privileged access, used to divert funds. 4.2 Malware propagation into critical servers Unmonitored accounts facilitated ransomware attacks, with 30% of critical servers infected in 2024, causing operational disruptions. 4.3 Compliance violations In 2025, the organization incurred a €250,000 fine for non-compliance with GDPR, NIS2, and ISO27001 due to inadequate oversight and audit trails for privileged accounts.

Root cause analysis	This initial analysis, derived from historical incident reports, preliminary stakeholder interviews, and internal audits, identifies potential root causes. A detailed investigation will follow BRD approval during dedicated workshops. 1. Ineffective Onboarding Process o Lack of standardized policies for account creation, leading to manual errors (observed in 20% of audited cases in 2024). o Insufficient integration between HR systems and IT directories, causing delays and unverified privileges. o Limited training for IT administrators on secure practices, exacerbating rushed processes. 2. Lack of Authorization and Access Control Processes o Absence of least privilege enforcement in access policies, allowing over-provisioning. o No regular access review mechanisms, resulting in accumulated unused privileges. 3. Inefficient Monitoring of Privileged Accounts o Missing real-time monitoring tools, preventing anomaly detection. o Inadequate audit logging standards, failing regulatory requirements like GDPR.
Proposed solutions	1. Implementing a semi-automated onboarding after a verification via Discovery scan: Ensure account separation, manual errors and mitigating credential theft. 2. Implementing a just-in-time approval workflows for privileged accounts: JIT access allows continuous verification, prevents leaks and ensures GDPR/NIS2 compliance. 3. Implementing a session recording for privileged accounts: Ensure real-time monitoring with AI anomaly detection, mitigates fraud and supports ISO27001 audits with 1-year retention.
Impacted Systems	1. Active Directory: Hosts accounts, supports Zero Trust discovery 2. Multi-Cloud (AWS/Azure/GCP): Hosts IAM accounts, scanned for privileged access 3. Databases & IoT Devices: Host DBA/IoT accounts; integrated for management 4. CyberArk (Vault, PVWA, CPM, Conjur): Enables onboarding, JIT, secrets, AI detection 5. IDP: Manages SSO with 0Auth/SAML/SCIM 6. SIEM: Real-time monitoring for NIS2 compliance 7. Integration: The system shall integrate seamlessly with Workday (Source of Truth), SailPoint (IGA), Active Directory, Azure AD (IDP), and Splunk (SIEM) using SCIM, LDAP, OAuth/SAML, and API protocols to ensure real-time data synchronization, self-service access via PVWA, incident alerting, and compliance with ISO27001, NIS2, RGPD, and DORA.
Assumptions & dependencies	1. AD/IDP: configured for scans and SCIM integration. 2. CyberArk: supports multi-cloud/IoT with JIT and AI detection. 3. SIEM and storage enable real-time monitoring and RGPD retention.
Business Requirements	**BR-01**: Semi-automated onboarding for all accounts (executives, IoT), with separation. **BR-02**: JIT approval with continuous verification and password rotation. **BR-03**: Session recording with AI detection, retained 1 year for RGPD/NIS2.