**Privilege Access Management**

**PAM**

In today’s digital landscape, securing privileged access is crucial to safeguarding our organization’s sensitive data and critical systems. Privileged Access Management (PAM) is a strategic initiative aimed at enhancing our cybersecurity posture by effectively managing and monitoring privileged accounts. Implementing PAM will significantly reduce the risk of unauthorized access, ensure compliance with regulatory requirements, and improve operational efficiency. Additionally, PAM will enhance server uptime by preventing unauthorized changes and reducing the risk of system outages caused by misuse of privileged credentials.

In order to provide Cybersecurity continuity and compliance with audits of regulators, we need to implement a Privilege Access Management (PAM) solution. It protects organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources.

All privileged accounts shall be managed in one central system, which keeps track of any changes made. It's also important for this system to be able to work with existing directory services like Active Directory. Additionally, there should be a secure vault for storing passwords, which can be accessed by administrators during emergencies. The passwords stored in this vault must be encrypted in accordance with the Encryption Standard of the Bank. The bank shall keep a list of all privileged accounts and update it regularly to discover any new or changed accounts.

A privileged access management system must be configured to utilize robust backup, recovery, and availability methodologies to ensure resiliency and availability of the credentials stored within the system as well as the timely recovery of the system in the event of a system failure

|  |  |  |
| --- | --- | --- |
| **Name** | **Q-ty** | **Description** |
| Privilege Access Management (PAM) | 17 internal User  2 External User  2 Auditor | Privilege Access Management (PAM) solutions aim to secure, control, and monitor access to critical systems and sensitive data by privileged users, reducing security risks, ensuring compliance, and enhancing operational efficiency. |

**Purpose and Technical Requirements**

The system must be installed on a Windows Server, locally.

All necessary software licenses, including operating systems, must be included in the proposed product and registered in the purchaser's name.

The system must have a built-in database that does not require additional administration.

**Secure Vault**

A Secure Vault is required to store privileged credentials and sensitive data in an encrypted and highly secure environment. The vault should offer robust encryption standards, access controls, and auditing capabilities to ensure that only authorized users can access stored information. It should also integrate with existing security frameworks to provide seamless and secure operations. The system must support at least (not less than) the FIPS 140-2 standard for enhanced security.

**DR/HA Vault**

A Disaster Recovery (DR) and High Availability (HA) Vault ensures continuous access to privileged accounts even during system failures or disasters. The solution should offer automated failover, data replication, and recovery mechanisms to maintain operational continuity. High availability configurations are essential to minimize downtime and ensure that critical systems remain accessible under all circumstances.

**Centralized Policy and Management Console**

A Centralized Policy and Management Console provides a unified interface for defining, implementing, and managing security policies across all privileged accounts. It should enable administrators to easily enforce access controls, monitor usage, and generate compliance reports. This console must be user-friendly and integrate seamlessly with other IT management tools to streamline administration and policy enforcement.

**Session Recording, Search with Keyword, Live Monitoring and Termination**

Session Recording captures and logs all activities performed during privileged sessions for auditing and compliance purposes. The solution should include advanced search capabilities with keyword filtering, enabling quick retrieval of specific session data. Live monitoring and session termination features are crucial for real-time oversight and the ability to immediately address suspicious or unauthorized activities.

The system should be able to record mouse behavior, keystrokes, and provide video archive capabilities with search functionality.

The system should have the ability to restrict opening unwanted programs in Windows by identifying window titles.

**Threat Analytics (Automatic Anomaly Detection and Prevention)**

Threat Analytics involves the automatic detection and prevention of anomalies in privileged access activities. The solution should use predefined signatures or behavioral analysis to identify unusual patterns or potential security threats. Real-time alerts and automated response mechanisms are essential for proactive threat management and mitigation. Automatic session termination or password changes based on high-risk activities must be supported. The system shall be able to receive and analyze information from SIEM solutions and return analysis results.

**Password/Key Management**

Password and Key Management functionalities automate the generation, storage, rotation, and management of passwords and cryptographic keys. The solution shall support complex password policies, automatic rotation, and secure storage to minimize the risk of credential theft or misuse. Integration with existing IT infrastructure and applications is necessary for seamless operations.

**SSO Integration (Microsoft AD and Azure AD)**

SSO Integration with Microsoft Active Directory (AD) and Azure AD allows for single sign-on capabilities, streamlining user access to multiple systems and applications. The solution shall support seamless authentication, leveraging existing AD credentials to provide a unified and secure login experience. This integration enhances user convenience while maintaining high security standards.

**3rd-Party Access Management**

3rd-Party Access Management ensures secure and controlled access for external vendors and contractors to the organization’s systems. The solution shall provide mechanisms for temporary access, detailed monitoring, and strict enforcement of least privilege principles. Secure access gateways and auditing capabilities are crucial to protect sensitive data and systems from potential external threats.

**Additional Requirements**

The system shall provide the ability to search full text in the audit journal and recover by the time of action for the session.

The solution must be able to forward logs to multiple SIEM solutions simultaneously, each in different formats.

**Services to be delivered**

The supplier company must implement the proposed product in the buyer's environment. supplier must integrate proposed system with at least existing ticketing system in the organization.

**Mandatory Requirements:**

The supplier must submit a Manufacturer's Authorization Form (MAF) for the proposed product, which must be issued after the date of tender.

Provided software licenses and product by the supplier must have registered in the purchaser's name.

The provided Privileged Access Management (PAM) solution must be ranked among the top five in the Gartner Magic Quadrant for Privileged Access Management.

The system must have at least 1 year of manufacturer's support for software and other necessary components. In case of need, the communication must be carried out directly with the manufacturer.

The bidder company must have documentation confirming the experience of delivering similar procurement objects, totaling at least 2 (two) Successfully Completed contracts. To confirm this, it is possible to use agreements and acts of acceptance and handover, or a table indicating the SPA/CMR/NAT/MEP numbers of the tender application.

Team Member of the supplier must have at least one Engineer’s certificate related to PAM product. The team member must be present at all stages of PAM implementation