**Scope of Work: Account Discovery**

1. **Identification:** Identify all privileged accounts existing across the organization's digital landscape, including those hidden or unmanaged.
2. **Automated Scans:** Conduct automated scans of network systems, applications, and endpoints to uncover privileged accounts that might have escaped conventional management.
3. **Shadow Account Detection:** Detect and highlight shadow accounts – accounts that are active but not part of the standard management framework.
4. **Dormant Account Identification:** Identify dormant privileged accounts that might still have active credentials, posing a potential security risk.
5. **Visibility Enhancement:** Provide comprehensive visibility into the privileged account landscape, enabling proactive risk assessment and mitigation.
6. **Risk Evaluation:** Assess the potential security risks associated with discovered privileged accounts, categorizing them based on their potential impact.
7. **Access Path Analysis:** Analyze the access paths and permissions associated with each privileged account to determine their potential exposure.
8. **Security Gap Identification:** Identify gaps in privileged account management, such as accounts without proper monitoring or security configurations.
9. **Prioritization:** Prioritize remediation efforts based on the criticality of accounts and associated security risks.
10. **Recommendations:** Offer recommendations for securing and managing discovered privileged accounts effectively.

**Scope of Work: Account Onboarding**

1. **New Account Setup:** Establish a structured process for creating new privileged accounts based on defined roles and responsibilities.
2. **Security Policy Adherence:** Ensure that each newly created account adheres to organization-wide security policies and standards.
3. **Access Control Configuration:** Configure access controls and permissions for new accounts based on the principle of least privilege.
4. **Password Policy Enforcement:** Implement strong password policies for new privileged accounts, including regular rotation and complexity requirements.
5. **Automated Workflows:** Streamline the account onboarding process through automated workflows, minimizing manual interventions.
6. **Approval Workflow:** Integrate an approval process to ensure that new privileged accounts are provisioned only after appropriate authorization.
7. **Monitoring Integration:** Integrate new accounts into monitoring and auditing systems to track their activity and detect anomalies.
8. **Regular Review:** Conduct regular reviews of newly onboarded accounts to verify their necessity, access level, and adherence to security standards.
9. **Password Rotation:** Enforce regular password rotation for new privileged accounts to mitigate the risk of credential compromise.
10. **Deprovisioning:** Establish protocols for deprovisioning or disabling newly created accounts when they are no longer required.
11. **Documentation:** Maintain detailed records of the onboarding process, including account details, configurations, and associated policies.
12. **Training:** Provide training to relevant personnel involved in the onboarding process to ensure consistent adherence to best practices.

**Requirements for Account Discovery:**

1. **Comprehensive Scanning:** Implement a solution that can comprehensively scan an organization's network, systems, applications, and endpoints to identify privileged accounts.
2. **Automated Detection:** Enable automated account discovery to continuously monitor and identify new privileged accounts as they are created.
3. **Shadow Account Detection:** Develop capabilities to detect and highlight shadow accounts – accounts that exist outside the standard management processes.
4. **Dormant Account Identification:** Include mechanisms to identify dormant accounts that might still pose a security risk due to retained credentials.
5. **Granular Visibility:** Provide granular visibility into the attributes and permissions associated with each discovered privileged account.
6. **Risk Scoring:** Integrate risk scoring mechanisms to prioritize the remediation of discovered accounts based on their potential impact.
7. **Integration with PAM Platform:** Ensure seamless integration with the broader Privileged Access Management (PAM) platform to centralize management.
8. **Customizable Scans:** Allow organizations to customize scanning parameters and frequency to align with their specific security needs.
9. **Real-time Alerts:** Provide real-time alerts for the discovery of high-risk privileged accounts, enabling immediate action.

**Requirements for Account Onboarding:**

1. **Structured Process:** Establish a structured and standardized process for creating new privileged accounts.
2. **Access Request Workflow:** Develop an access request workflow that includes approvals to ensure proper authorization for account creation.
3. **Security Policy Adherence:** Enforce adherence to organization-wide security policies and standards during the onboarding process.
4. **Least Privilege Principle:** Implement access controls based on the principle of least privilege to assign appropriate permissions to new accounts.
5. **Password Policies:** Enforce strong password policies, including complexity requirements and regular rotation, for new privileged accounts.
6. **Automation Capabilities:** Include automation capabilities to streamline the account onboarding process and minimize manual errors.
7. **Monitoring Integration:** Integrate newly onboarded accounts into monitoring and auditing systems for activity tracking and anomaly detection.
8. **Regular Review Mechanism:** Implement a mechanism for regularly reviewing the necessity and access levels of newly created accounts.
9. **Deprovisioning Protocols:** Develop protocols for deprovisioning or disabling accounts that are no longer required or active.
10. **Documentation:** Require documentation of the onboarding process, including account details, configurations, and associated policies.
11. **Training and Education:** Provide training and educational resources to personnel involved in the account onboarding process.

**Goals of Account Onboarding:**

1. **Structured Provisioning:** Establish a structured process for creating new privileged accounts, ensuring consistency and adherence to policies.
2. **Controlled Access:** Implement access controls and permissions based on the principle of least privilege for new accounts.
3. **Policy Adherence:** Ensure that newly created accounts align with organization-wide security policies and standards.
4. **Secure Configurations:** Set up secure configurations, including strong password policies and regular password rotation, for new accounts.
5. **Reduced Attack Surface:** Minimize the attack surface by enforcing proper security practices for newly onboarded privileged accounts.
6. **Auditing and Monitoring:** Facilitate monitoring and auditing of newly created accounts to detect any unauthorized activity.
7. **Efficient Management:** Streamline the management of privileged accounts throughout their lifecycle, from creation to deprovisioning.
8. **Operational Efficiency:** Improve operational efficiency by automating account onboarding processes, reducing manual interventions.
9. **Compliance Management:** Assist in maintaining compliance by ensuring that new accounts adhere to regulatory requirements.
10. **Minimized Risk:** Mitigate the risk of unauthorized access and potential breaches by controlling the introduction of new privileged accounts.

**Goals of Account Discovery:**

1. **Complete Visibility:** Attain a comprehensive view of all privileged accounts across the organization's digital landscape, leaving no account undiscovered.
2. **Risk Mitigation:** Identify hidden, unmanaged, or shadow privileged accounts that might pose security risks and proactively mitigate these risks.
3. **Security Gap Identification:** Uncover gaps in privileged account management, providing insights to enhance security practices.
4. **Accurate Inventory:** Maintain an accurate inventory of privileged accounts to facilitate efficient management and control.
5. **Proactive Response:** Enable a proactive response to security threats by identifying potential vulnerabilities before they are exploited.
6. **Compliance Assurance:** Assist in achieving compliance with industry regulations by identifying all privileged accounts and enforcing proper management.