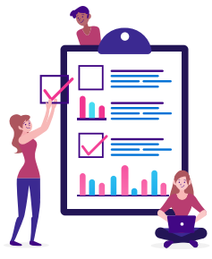
Planning Documents for PAM
Implementation Use Cases

Just-in-Time (JIT) Privileged Access & Password Vaulting

Objective:

- Implement JIT access to minimize standing privileges.
- Utilize password vaulting with automated rotation.



Key Components:

- Privileged access requests approval process.
- Time-bound access enforcement.
- Secure vault storage for shared credentials.
- Automated password rotation and retrieval policies.

Implementation Steps:

- Identify privileged accounts requiring JIT access.
- Define approval workflows and expiration policies.
- Deploy and configure a privileged access vault.
- Test JIT access request and password retrieval mechanisms.
- Monitor and review access logs regularly.

Expected Outcome:

- Reduced risk of credential exposure.
- Minimized attack surface.
- Enhanced accountability for privileged actions.

Session Monitoring & Multi-Factor Authentication (MFA) for Privileged Access

Objective:

- Enable real-time session monitoring and recording.
- Enforce MFA for privileged access authentication.

Key Components:

- Session recording and playback capabilities.
- Behavioral anomaly detection mechanisms.
- MFA integration with privileged accounts.

Implementation Steps:

- Deploy session monitoring tools for privileged accounts.
- Configure real-time alerting on suspicious activities.
- Integrate MFA solutions (e.g., OTP, biometrics).
- Enforce MFA for all privileged account logins.
- Conduct regular security audits on monitored sessions.

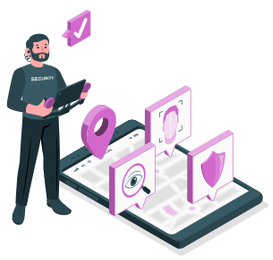
Expected Outcome:

- Stronger authentication barriers.
- Improved security visibility.
- Reduced risk of insider threats.

Least Privilege for Application-to-Application (A2A) & Privileged Access Review

Objective:

- Enforce least privilege principles for A2A communications.
- Conduct regular privileged access reviews and certifications.



Key Components:

- Role-based access control (RBAC) enforcement.
- Periodic access reviews by business owners.
- Automated deprovisioning of unnecessary privileges.

Implementation Steps:

- Identify applications requiring A2A communication.
- Define and implement the principle of least privilege.
- Establish periodic access review policies.
- Automate privilege revocation for unused accounts.
- Audit compliance with security policies regularly.

Expected Outcome:

- Reduced lateral movement risks.
- Improved governance over privileged access.
- Stronger enforcement of least privilege principles.

For more content like and follow me:

@bertblevins

Zero Trust-Based Privileged Access Control

Objective:

- Implement Zero Trust-based privileged access policies.
- Grant access dynamically based on risk factors.

Key Components:

- Risk-based authentication mechanisms.
- Endpoint health verification.
- Dynamic access provisioning.

Implementation Steps:

- Define risk-based policies for privileged access.
- Integrate real-time user behavior analysis.
- Enforce endpoint security checks before access approval.
- Implement continuous access validation.
- Regularly refine policies based on security assessments.

Expected Outcome:

- Enhanced access control with risk-based validation.
- Minimized exposure to credential-based attacks.
- Continuous security improvements based on user behavior analytics.

Additional Planning Documents for PAM Implementation Use Cases

Automated Privileged Access Deprovisioning

Objective:

- Ensure automatic deprovisioning of privileged accounts when no longer needed.
- Reduce security risks associated with orphaned accounts.

Key Components:

- Automated lifecycle management.
- Integration with HR and IT systems.
- Access review and expiration policies.

Implementation Steps:

- Identify and classify privileged accounts.
- Implement an automated deprovisioning system.
- Define role-based expiration policies.
- Integrate with HR and IT management systems.
- Continuously monitor and audit deprovisioning processes.

Expected Outcome:

- Minimized risk of privilege escalation.
- Enhanced compliance and governance.
- Reduced attack surface.

Privileged Access Risk Scoring & Anomaly Detection

Objective:

- Implement risk-based scoring to assess privileged access threats.
- Detect and respond to anomalous privileged activities.

Key Components:

- AI-driven risk analysis.
- Real-time behavioral monitoring.
- Automated incident response.

Implementation Steps:

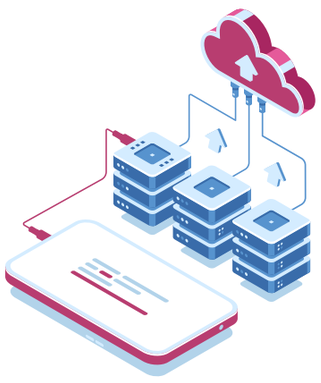
- Define risk factors for privileged access.
- Deploy machine learning-based threat detection.
- Establish real-time alerting mechanisms.
- Automate response workflows for high-risk events.
- Conduct periodic model tuning and policy refinement.

Expected Outcome:

- Proactive threat mitigation.
- Improved privileged access oversight.
- Automated security response to potential breaches.

For more content like and follow me:  **@bertblevins**

Cloud Privileged Access Management

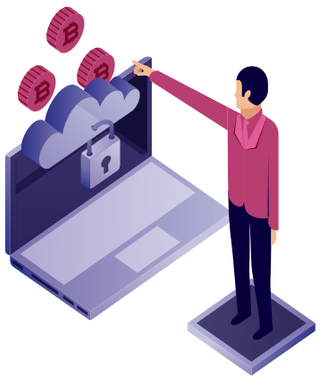


Objective:

- Secure privileged access in multi-cloud environments.
- Implement centralized control over cloud-based privileged accounts.

Key Components:

- Cloud-native access controls.
- Least privilege enforcement.
- Secure identity federation.



Implementation Steps:

- Identify cloud-based privileged accounts and services.
- Implement role-based access control (RBAC) for cloud services.
- Enforce conditional access policies.
- Monitor and audit cloud privilege escalations.
- Regularly review and optimize access policies.

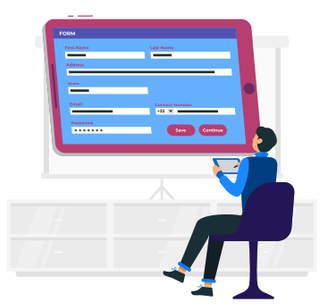
Expected Outcome:

- Consistent privileged access security across cloud platforms.
- Reduced risk of unauthorized cloud access.
- Stronger compliance with cloud security frameworks.

Endpoint Privileged Access Management (EPAM)

Objective:

- Secure privileged access on endpoints (workstations, servers, etc.).
- Prevent unauthorized elevation of privileges.



Key Components:

- Local administrator rights management.
- Endpoint privilege escalation monitoring.
- Just-in-Time elevation for endpoint tasks.

Implementation Steps:

- Identify endpoints requiring privilege management.
- Deploy endpoint privilege management tools.
- Configure policies for Just-in-Time elevation.
- Implement real-time alerting on suspicious privilege escalations.
- Conduct regular policy reviews and updates.

Expected Outcome:

- Reduced risk of endpoint privilege abuse.
- Improved security posture on workstations and servers.
- Minimized need for standing administrator rights.

For more content like and follow me:  **@bertblevins**