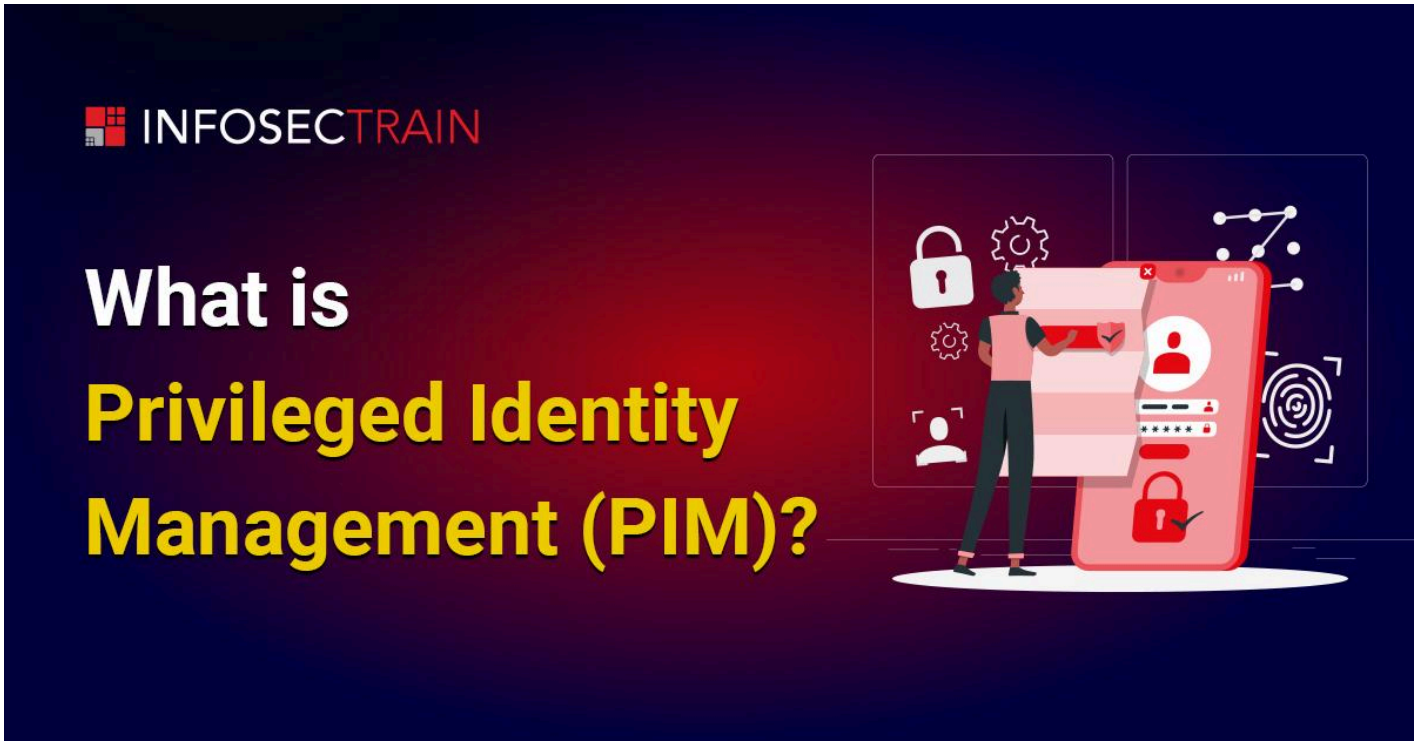
Downloaded from: justpaste.it/cp6m5

What is Privileged Identity Management (PIM)?



Understanding Privileged Identity Management (PIM)

Privileged Identity Management is a service within Azure Active Directory (Azure AD) that enables users to manage, monitor, and govern privileged access to resources in Azure AD and other Microsoft Online Services like Microsoft 365 or Microsoft Intune. PIM focuses on protecting access to sensitive roles and reducing the risk of excessive, unnecessary, or misused access permissions.

Key Features of Privileged Identity Management (PIM)

- **Just-In-Time (JIT) Access:** PIM ensures that users only have elevated privileges when they need them and for a limited duration. This reduces the time that an account has privileged access and minimizes exposure to potential security breaches.

- **Role Activation and Deactivation:** Users can request to activate their roles when necessary, after which the access is automatically deactivated once the specified time expires.
- **Approval Workflow:** Administrators can configure PIM to require approval before privileged roles are activated, adding an extra layer of security and oversight.
- **Access Reviews:** PIM supports periodic access reviews to confirm that users with privileged roles still need that access. This helps organizations maintain proper access hygiene.
- **Audit History and Alerts:** PIM provides comprehensive audit logs and alert capabilities. Administrators can track who activated what role and when ensuring any anomalies or suspicious activities are flagged for investigation.

Use Cases for Privileged Identity Management (PIM)

- **Administrator Role Management**: Ensuring only specific administrators have access to manage services and only during designated times.
- **Azure Resource Management**: Controlling who can access or modify resources in an Azure subscription to avoid unauthorized changes.
- **Office 365 Global Admin Role**: Assigning global admin roles only temporarily to mitigate risks related to having too many permanent global administrators.

Benefits of Privileged Identity Management (PIM)

Here is how PIM helps to improve security:

- **Minimizing Attack Surface**: By limiting privileged access to only when necessary, PIM minimizes the risk of accounts being compromised by cyber-attacks targeting privileged roles.
- **Reducing Insider Threats**: With JIT access and approval workflows, organizations can limit the potential for internal misuse of elevated privileges.
- **Enhanced Compliance**: PIM supports compliance by providing visibility and control over who has access to sensitive roles and for how long. Organizations can use PIM to meet regulatory and industry standards that require strict access management protocols.

AZ (104 + 500) Combo Training with InfosecTrain

InfosecTrain's Azure Administrator & Security Online Training (AZ-104 + AZ-500) Combo equips learners with foundational Azure administration and advanced security skills, including Privileged Identity Management (PIM). This training enhances understanding of securing, managing, and controlling privileged access within Azure environments.