kod szkolenia: SC-5008 / ENG DL 1d

Configure and govern entitlement with Microsoft Entra ID

Training on the implementation and oversight of identity and access management mechanisms within Microsoft Entra ID, with a particular focus on Identity Governance. Participants will learn how to plan and implement Entitlement Management (resource catalogs, access packages, related organizations, and the lifecycle of external users), how to conduct Access Reviews to maintain the principle of least privilege, how to design privileged access using Privileged Identity Management (PIM) and Privileged Access Groups, and how to monitor and analyze access events through log files, audit logs, and integration with SIEM tools (e.g., Microsoft Sentinel). The goal is to build a consistent approach to access control that aligns with Zero Trust principles and meets audit and regulatory requirements.

Training recipients

- Identity & Access Administrators working with Microsoft Entra ID and Azure.
- Security and compliance professionals who want to implement access controls and access review processes.
- Application administrators and resource owners (applications, groups, Azure subscriptions) responsible for granting and reviewing access.
- Individuals designing onboarding/offboarding processes and collaboration with external users (B2B) who want to automate access granting through access packages.

Benefits

1. Planning and implementation of Entitlement Management – creating catalogs, access packages, and assignment and approval rules.
2. External user access management (B2B) – affiliated organizations, collaboration policies, and access lifecycle control.
3. Designing and launching Access Reviews – configuring reviews for groups and applications, recurring schedules, automation, and enforcement of results.
4. Monitoring and maintaining Microsoft Entra ID – analyzing login and audit logs, reporting (workbooks), Identity Secure Score, and integration with SIEM solutions.
5. Implementation of privileged access – privileged access strategy, PIM configuration (Entra roles and Azure resources), Privileged Access Groups, and break-glass accounts.

Training program

Module 1: Planning and Implementing Entitlement Management in Microsoft Entra ID

- Defining resource catalogs and access packages.
- Configuring entitlement management: approval workflows, assignment policies, access conditions.
- Connected organizations and B2B collaboration scenarios.
- Reviewing per-user entitlements and auditing assignments.

Module 2: Planning, Implementing, and Managing Access Reviews

- Planning access reviews: what and who to recertify (groups, applications, roles).
- Creating reviews for groups and applications, and access review programs.
- Monitoring review results and enforcing decisions.
- Task automation and configuration of recurring Access Reviews.

Module 3: Monitoring and maintaining Microsoft Entra ID

- Analysis and diagnostics of sign-in logs in the context of access issues.
- Review and monitoring of audit logs.
- Exporting logs to SIEM tools and utilizing workbooks and reporting.
- Monitoring security posture (Identity Secure Score) and key governance metrics.

Module 4: Planning and Implementing Privileged Access

- Privileged access strategy for administrative users (roles, scopes, JIT).
- Configuring Privileged Identity Management (PIM) for Microsoft Entra roles and Azure resource roles.
- Planning and configuration of Privileged Access Groups.
- Analysis of audit history and PIM reports, and emergency access (break-glass).

Module 5: Overview of Microsoft Entra Permissions Management capabilities

- Discussion of use cases and benefits: visibility of permissions in cloud environments, risk analysis.
- Dashboard and reports: identifying excessive permissions and prioritizing actions.
- Continuous monitoring and remediation – an operational approach to maintaining the least privilege.

Expected preparation of the participant

- Basic knowledge of Azure administration and working with Microsoft Entra ID (e.g., users, groups, roles, application registrations—at a general level).
- Understanding of the basics of access management (RBAC, least privilege) and the Zero Trust concept.
- Basic familiarity with logs and monitoring (sign-in logs / audit logs) would be helpful.
- Preferred: general knowledge of onboarding/offboarding processes and collaboration with external users (B2B).

Training Includes

- manual in electronic form available on the platform: https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Czas trwania

1 dni / 7 godzin

Language

- Training: English
- Materials: English