Cloud Security Workshop – Overview

The Cloud Security Workshop is designed to help participants understand modern cloud-focused cyber threats and how Microsoft security capabilities work together to protect cloud and hybrid environments. The workshop combines conceptual explanations, architectural discussions, demonstrations, and real-world attack scenarios to build a strong foundation in cloud security.

This workshop provides a holistic view of end-to-end protection across cloud identities, workloads, platforms, applications, and data. Participants gain clarity on how identity security, cloud posture management, and workload protection each play a distinct role in securing cloud environments.

Through guided walkthroughs and scenario-based discussions, participants learn how cloud attacks originate, how misconfigurations and identity weaknesses are exploited, how threats move across cloud resources, and how Microsoft security services detect, prevent, and respond to these risks.

Rather than focusing only on individual tools, the workshop emphasizes cloud security principles, shared responsibility, and attacker techniques in cloud environments. It explains why each security capability exists, how gaps in configuration and governance are abused, and how Microsoft's integrated cloud security approach helps address these challenges.

The goal of the workshop is to build clarity and confidence around cloud security concepts, enabling participants to think strategically about risk management, cloud protection, and secure cloud operations.

What Participants Will Learn

- Understanding of the cloud-focused threat landscape, including common attack paths and risk areas
- Clear view of Microsoft cloud security architecture, with emphasis on cloud security posture management and workload protection
- Practical insight into securing cloud workloads, platforms, and data through real-world scenarios
- Exposure to cloud threat detection, investigation, and response concepts
- Best practices for improving cloud security posture using secure configuration and governance principles