Overview

The **Microsoft SecOps Educational Workshop** is designed to help participants understand how modern security operations teams can effectively detect, investigate, and respond to cyber threats in today's highly dynamic threat landscape. The workshop blends foundational concepts, live demonstrations, real-world attack scenarios, and architectural discussions to build a strong understanding of Microsoft's unified security operations platform.

This workshop provides a complete view of end-to-end security operations across identities, endpoints, email, applications, cloud workloads, and infrastructure. Through guided walkthroughs and scenario-based learning, participants gain clarity on how threats are identified, correlated, investigated, and remediated using Microsoft's integrated detection and response capabilities.

Rather than focusing solely on alerts and tools, the workshop emphasizes **how modern attacks unfold**, why traditional SOC approaches struggle with alert fatigue and silos, and how Microsoft's SecOps approach brings together visibility, automation, and intelligence. The objective is to build confidence and strategic thinking around operating a resilient, efficient, and intelligence-driven Security Operations Center (SOC).

Workshop Topics :

Through this workshop, our data security engineers will equip your team with deep insights and knowledge across the following areas:

1. Understanding the Modern Threat Landscape
    - How today's attacks span identities, endpoints, email, cloud, and applications, common attacker techniques, and why an integrated SecOps approach is essential.
2. Microsoft's SecOps Architecture
    - How **Microsoft Sentinel** and **Microsoft Defender XDR** work together to deliver unified visibility, advanced detection, investigation, and response across the digital estate.
3. Threat Detection and Signal Correlation
    - Practical insights into how security signals from multiple sources are correlated into high-fidelity incidents, reducing noise and improving analyst efficiency.
4. Investigation and Incident Response
    - Real-world scenarios demonstrating how SOC teams can investigate incidents, trace attack paths, understand attacker behavior, and take coordinated response actions across identities, endpoints, and cloud resources.
5. Best Practices for Building a Modern SOC
    - Actionable guidance aligned to Zero Trust principles, MITRE ATT&CK, threat-informed defense, and continuous improvement of detection and response capabilities.