TeamQuest -The Compliance Games Training

Duration: **1 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Team Quest – The Compliance Games is a highly engaging, **team-based, gamified workshop** that combines generative AI prompting with real-world cybersecurity operations.

Set inside a **retro-futuristic command center**, learners face "**The Fog**"—a metaphor for ineffective AI collaboration caused by poor prompts and lack of context.
Through six immersive missions, participants learn how to communicate effectively with AI systems like **Microsoft Security Copilot**, building clarity, control, and confidence in AI-assisted security operations.

Prerequisites

Recommended knowledge:

- Security operations and incident response,
- Microsoft Defender for XDR,
- Microsoft Purview,
- Microsoft Entra,
- Microsoft Intune.

Who Should Attend

Ideal for:

- SOC analysts and **incident responders**,
- **Security engineers** using Microsoft Defender, Purview, Entra, and Intune,
- **Cybersecurity managers**, architects, and operations teams,
- Professionals integrating **generative AI** into security workflows.

TeamQuest -The Compliance Games Training

Duration: **1 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, participants will be able to:

- Explain the **role of generative AI** in modern security,
- Describe **large language models (LLMs)** and how they support copilots,
- Understand **Azure OpenAI** as a secure AI foundation,
- Apply **prompting techniques** for Microsoft Security Copilot,
- Evaluate and mitigate **AI risks and biases**,
- Design and deploy **responsible AI solutions** in security operations,
- Integrate Copilot across **Defender XDR, Purview, Entra, and Intune**,
- Lead teams through AI-assisted threat detection and incident response.

Outline

Understanding The Fog and human–AI misalignment

- Introduction to The Fog as a behavioural and organisational pattern.
- How vague requests and weak context reduce AI effectiveness.
- The role of human judgement in guiding machine intelligence.

Foundations of generative AI for security teams

- Overview of generative AI and its evolution within artificial intelligence.
- Understanding large language models and how they generate responses.
- Strengths and limitations of generative AI in security scenarios.

Responsible AI and risk management

- Principles of responsible generative AI development.
- Identifying potential harms in AI-assisted security workflows.
- Measuring bias, inaccuracies, and unintended outcomes.
- Mitigation strategies to improve reliability and trust.

Introduction to Microsoft Copilot for Security

- What Microsoft Copilot for Security is and how it supports analysts.
- Core terminology and concepts used within the platform.
- How Copilot processes prompts, context, and security signals.

Prompting strategies that cut through The Fog

- Elements of an effective prompt for security investigations.
- Providing context, constraints, and clarity in prompts.
- Common prompting mistakes and how to avoid them.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Adapting prompts for different security use cases.

Copilot integration across the Microsoft security stack

- Using Microsoft Copilot with Microsoft Defender XDR for threat investigation.
- Applying Copilot insights within Microsoft Purview for compliance and governance.
- Supporting identity and access decisions with Microsoft Entra and Copilot.
- Enhancing endpoint and device management with Microsoft Intune and Copilot.

TeamQuest missions and applied collaboration

- Team-based missions simulating real security operations scenarios.
- Cross-functional collaboration to solve complex security challenges.
- Applying improved prompting and analysis under time pressure.
- Translating lessons learned back into day-to-day security workflows.

Exams and assessments

There are no formal exams included in this course. Learning is reinforced through team-based challenges, scenario-driven missions, and instructor-led discussions that assess understanding through application rather than written testing.

Hands-on learning

This course includes:

- Gamified, team-based missions aligned to real security operations scenarios.
- Guided exercises using Microsoft Copilot for Security across multiple tools.
- Instructor-led facilitation and feedback throughout each mission.