⭐ 2-DAY TOC – CYBERSECURITY REPORT WRITING

8 hours per day Including breaks

Audience: Cybersecurity Auditors, SOC Analysts, VAPT Testers, Compliance Teams

Focus: Practical reporting, Copilot prompting, scenario writing, template-based outputs. Use of industry-standard templates

🟦 DAY 1 — Cyber Security Report Writing Foundations

50% Practice • 50% Micro-Theory

Every module includes hands-on tasks, Copilot prompting, and trainer review of delegate outputs.

Module 1 — Essentials of Cybersecurity Reports

Main Topics Covered

• Purpose of cybersecurity reporting

• Technical vs executive writing

• Characteristics of effective reports

• Common reporting mistakes

• What “good” vs “bad” reporting looks like

Practical Activities

• Rewrite poorly written sentences

• Convert raw notes into a structured paragraph

• Copilot refinement

Trainer Reviews

• Rewritten sentences

• Copilot-refined paragraph

Templates Introduced

• Executive Summary Template

• Executive Briefing Template

Module 2 — Structuring Technical Security Reports

Main Topics Covered

• CEIR structure (Condition, Evidence, Impact, Recommendation)

• Writing clear, objective findings

• Translating technical issues into business language

• Writing actionable recommendations

• Avoiding repetition

Practical Activities

• Write a CEIR-structured finding

• Copilot rewrite

• Peer comparison

Trainer Reviews

• CEIR finding

• Copilot-refined finding

Templates Introduced

• Audit Finding Template (CEIR Model)

• Risk Assessment Template

Module 3 — Incident & SOC Reporting Techniques

Main Topics Covered

• NIST-aligned incident reporting structure

• Writing clear incident summaries

• Evidence logging

• Timeline creation

• Root cause articulation

• SOC alert documentation

Practical Activities

• Write an incident summary from raw logs

• Copilot refinement

Trainer Reviews

• Incident summary

• Copilot-refined summary

Templates Introduced

• Incident Report Template

• Gap Analysis Template

Module 4 — Visual Presentation & Security Dashboards

Main Topics Covered

• When to use visuals

• Types of visuals (tables, charts, heatmaps)

• Presenting security metrics

• Creating management-ready dashboards

• Avoiding clutter and misrepresentation

Practical Activities

• Create a table

• Create a dashboard snippet

• Create a visual summary using Copilot

Trainer Reviews

• Table

• Dashboard snippet

• Visual summary

Templates Introduced

• Security Dashboard Template

• Executive Briefing Template

Module 5 — VAPT & Risk Reporting

Main Topics Covered

• OWASP-aligned VAPT reporting

• CVSS scoring basics

• Severity justification

• Writing remediation recommendations

• Avoiding overly technical jargon

Practical Activities

• Rewrite VAPT findings

• Copilot rewrite + severity justification

Trainer Reviews

• VAPT finding

• Copilot-refined remediation

Templates Introduced

• VAPT Finding Template

• Risk Assessment Template

Module 6 — Compliance & Audit Reporting

Main Topics Covered

• ISO 27001 audit observation writing

• Gap analysis structure

• Maintaining objectivity

• Evidence-based reporting

• Writing clear compliance statements

Practical Activities

• Rewrite audit observations

• Copilot refinement

Trainer Reviews

• Audit observation

• Copilot-refined gap statement

Templates Introduced

• Audit Finding Template

• Gap Analysis Template

🟦 DAY 1 Closing Activity

Trainer Reviews

• One final CEIR finding per delegate (reviewed live)

🟩 DAY 2 — AI-Enabled Cybersecurity Reporting & Capstone

80% Practice • 20% Micro-Theory

Module 7 — AI-Assisted Cybersecurity Documentation (Extended Practical Module)

Main Topics Covered

• Why AI is essential for modern reporting

• GDPR-safe prompting

• The 5 rules of effective prompting

• Using Copilot for:

• Executive summaries

• Findings

• Visuals

• Risk statements

• Recommendations

• Validating AI output

• Avoiding hallucinations

Practical Activities

Practical 1 — Executive Summary Generation

• Write prompt → Copilot generates summary → refine

• Template: Executive Summary Template

Practical 2 — Writing a Proper Finding (CEIR)

• Rewrite poor findings using Copilot

• Template: Audit Finding Template

Practical 3 — Visual Representation

• Convert raw data into visuals using Copilot

• Template: Security Dashboard Template

Trainer Reviews

• 2 executive summaries

• 2 CEIR findings

• 1 visual summary

Module 8 — Capstone Scenario Setup

Main Topics Covered

• Understanding full report expectations

• Applying templates to real scenarios

• Structuring a complete cybersecurity report

Templates Shared

• Incident Report Template

• VAPT Finding Template

• Audit Finding Template

• Executive Summary Template

• Security Dashboard Template

Module 9 — End-to-End Cybersecurity Reporting (Capstone)

Main Topics Covered

• Integrating all report components

• Ensuring consistency and clarity

• Using Copilot to refine each section

Delegate Deliverables

• Executive Summary

• Incident Summary

• Technical Analysis

• Evidence Log

• Risk Assessment

• Recommendations

• Dashboard Snapshot

Trainer Reviews

• 3 full reports (random selection)

Module 10 — Presentation of Findings to Management

Main Topics Covered

• Presenting to non-technical leaders

• Communicating risk clearly

• Defending findings

• Handling questions

Trainer Reviews

• 3 delegate presentations

Template Used

• Executive Briefing Template

Module 11 — Quality Review & Professional Writing Techniques

Main Topics Covered

• Common reporting mistakes

• Improving clarity, tone, structure

• Peer review techniques

• Ensuring accuracy and neutrality

Trainer Reviews

• 2 peer-reviewed samples

• 1 Copilot-refined sample

Module 12 — Final Feedback & Wrap-Up

Main Topics Covered

• Best practices

• Long-term improvement roadmap

• Using prompt libraries

• Writing checklist

Resources Provided

- Prompt Library
- Reporting Checklist