CA204: Cyber Security Reporting

7 Instructional Hours 10 CPEs 3 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER

This course provides a comprehensive foundation in academic writing, technical documentation, and cybersecurity reporting. It guides learners through essential research practices, literature analysis, structured writing techniques, and proper formatting and referencing standards. Additionally, it introduces AsciiDoc as a modern tool for technical documentation and explores its practical use in creating structured, publishable content. The course concludes with applied cybersecurity reporting concepts, including vulnerability assessments and standardized frameworks such as CVE, CWE, and CVSS. Overall, it equips learners with the skills needed to produce clear, professional, and evidence-based reports in both academic and cybersecurity contexts.

You Will Be Able To

- Apply appropriate research methods (qualitative, quantitative, and mixed) to gather and analyze data
- Conduct structured literature reviews to identify trends, gaps, and insights in existing research
- Produce well-organized academic and technical documents with clear structure, tone, and style
- Use proper formatting and referencing techniques (APA, MLA, Chicago) to maintain academic integrity
- Create professional technical documentation using AsciiDoc and compile it into multiple formats
- Develop cybersecurity reports, including vulnerability assessments and risk scoring using CVSS

Who Should Attend

This course is designed for students, researchers, and professionals who need to develop strong writing and reporting skills, particularly in technical or cybersecurity domains. It is suitable for individuals involved in academic research, technical documentation, or security assessments who want to improve clarity, structure, and professionalism in their written communication. No advanced writing background is required, but a basic understanding of research or IT concepts will be beneficial.

Relevant Combat Roles

- Cybersecurity Analyst
- Penetration Tester / Ethical Hacker
- Threat Intelligence Analyst
- Technical Writer (Cybersecurity / IT)
- Security Operations Center (SOC) Analyst
- Research Analyst

Topics Covered

Academic Writing & Research
Basics of academic writing, clarity, and key research methods (qualitative & quantitative).

Literature Review
Finding, analyzing, and evaluating existing research for relevance and credibility.

Structure, Style & Referencing
Proper document organization, formal tone, and citation styles (APA, MLA, Chicago).

Plagiarism & Ethics
Avoiding plagiarism through correct citation, paraphrasing, and integrity practices.

Technical Documentation & AsciiDoc
Clear technical writing, AsciiDoc syntax, theming, and documentation tools.

Cybersecurity Reporting & Quality
Reporting principles, CVE/CWE/CVSS frameworks, and best practices for quality assurance.

Labs

Academic Research & Professional Reporting
(research methods, academic report writing, and structured technical documentation)

AsciiDoc Technical Documentation & Publishing
(AsciiDoc formatting, tables, code snippets, and PDF/HTML document compilation)

Cybersecurity Assessment & Professional Reporting
(vulnerability assessments, executive summaries, technical findings, and remediation reporting)

CVSS Risk Assessment & Vulnerability Scoring
(CVSS scoring, vulnerability severity analysis, and risk rating justification)