SEC402: **Cybersecurity Writing: Hack the Reader**

2 Day Course	12 CPEs	Laptop Not Needed

You Will Be Able To

- Uncover the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing
- Make these elements part of your arsenal through hands-on exercises that draw upon common security scenarios
- Learn the key topics you need to address in security reports and other written communications
- Understand how to pick the best words, structure, look, and tone
- Begin improving your skills at once by spotting and fixing weaknesses in security samples
- Receive practical checklists to ensure you'll write clearly and effectively right away

Who Should Attend

If your cybersecurity job involves writing emails, reports, proposals, or other content, you'll find this course indispensable, whether you are:

- A manager or an individual team member
- A consultant or an internally-focused employee
- An expert or a beginner
- A defender or an attacker
- An earthling or an alien

You get the idea—the course is for all cybersecurity professionals who want to improve their written communications and boost their careers.

NICE Framework Work Roles

- Authorizing Official/Designating Representative (OPM 611)
- Systems Requirements Planner (OPM 641)
- System Testing and Evaluation Specialist (OPM 671)
- Knowledge Manager (OPM 431)
- Cyber Legal Advisor (OPM 731)
- Cyber Instructor (OPM 712)
- Security Awareness & Communications Manager (OPM 712)
- IT Program Auditor (OPM 805)

Want to write better? Learn to hack the reader! Discover how to find an opening, break down your readers' defenses, and capture their attention to deliver your message--even if they're too busy or indifferent to others' writing. This unique course, built exclusively for cybersecurity professionals, will strengthen your writing skills and boost your security career.

You will:

- Uncover the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing.
- Make these elements part of your arsenal through hands-on exercises that draw upon common security scenarios.
- Learn the key topics you need to address in security reports and other written communications.
- Understand how to pick the best words, structure, look, and tone.
- Begin improving your skills at once by spotting and fixing weaknesses in security samples.
- Receive practical checklists to ensure you'll write clearly and effectively right away.

This isn't your normal writing course:

- The course builds upon the author's two decades of cybersecurity experience. You'll learn from examples relevant to security professionals, whether they're experts or beginners, managers or individual team members.
- The course focuses on common writing problems you'll learn to avoid, instead of presenting tedious grammar rules or theoretical explanations. You'll advance your writing by reviewing and improving real-world cybersecurity samples.

Master the writing secrets that'll make you stand out in the eyes of your peers, colleagues, managers, and clients. Learn to communicate your insights, requests, and recommendations persuasively and professionally. Make your cybersecurity writing remarkable.

Author Statement

How can you stand out from other cybersecurity professionals with similar technical skills? How can you get your managers, clients, and colleagues to notice your contribution, accept your advice, and appreciate your input? Write better!

Here's an uncommon opportunity to improve your writing skills without sitting through tedious lectures or writing irrelevant essays. You'll make your writing remarkable by learning how to avoid common mistakes, working on real-world exercises to spot and correct cybersecurity writing problems. You'll write clearly and effectively right away with the help of practical checklists.

This course captures my experience of writing in cybersecurity for over two decades and incorporates insights from other members of the community. It's a course I wish I could have attended when I needed to improve my own writing skills. It's a course I know will help you propel your own cybersecurity career.

—Lenny Zeltser

"Outstanding course. It provides a writing framework/rubric to evaluate and guide future writing."

—Jordan Whitley, **New York Life**

Section Descriptions

DAY 1 – SECTION 1:

How to Strengthen Your Writing Skills—A Reader-Centered Approach

You'll learn how a reader-centered approach to writing allows you to prepare cybersecurity materials that connect with your audience. You'll discover how the five "golden elements" of writing work together to assist you with these tasks. These elements, which we discuss throughout the course, are:

- The right structure
- The right look
- The right words
- The right tone
- The right information

You'll understand how to use the hands-on exercises in this course to avoid problems common to the security reports, emails, and other content you regularly create.

DAY 1 – SECTION 2:

The Right Structure

We all have way too much to read. You'll learn how to structure your writing so readers don't want to put it down. You'll discover how to:

- Open with the idea your readers cares about most
- Organize the supporting ideas to make them easy to find, read, skip, and skim
- Design the structure to meet the needs of all your readers

You'll understand how to use the right structure by spotting and fixing structural issues with many cybersecurity examples.

DAY 1 – SECTION 3:

The Right Look

You have just seconds to grab your reader. You'll learn how to give your writing the right look to hook your readers at a first glance. You'll be able to:

- Create an appealing layout with lists and headings
- Design readable paragraphs
- Capitalize words correctly
- Use just the right amount of formatting
- Pick the best graphic for your objectives
- Handle screenshots and tables effectively

You'll master the right look by examining security writing samples that have an amazingly misguided look. (Expect much fun.)

DAY 2 – SECTION 4:

The Right Words

The word is mightier than the sword. You'll learn how to pick the right words to inform and persuade your readers. You'll find out how to make sure your words are:

- Clear: Use words your readers understand.
- Concise: Cut words you don't need.
- Consistent: Use parallel structure and uniform style.
- Correct: Use proper terms and spelling.

The key to using the right words is deliberate practice. You'll have many opportunities to improve poorly worded cybersecurity text.

DAY 2 – SECTION 5:

The Right Tone

Tone is the key to creating a bond with your reader. You'll learn how to make your tone:

- Professional and appropriate for the reader
- Responsive to difficult situations
- Constructive, helping the reader solve problems
- Persuasive, motivating the reader to take action or make a decision

Real-world examples will help you learn to spot tone problems, so you can turn them into writing that says just what your reader will understand and appreciate.

DAY 2 – SECTION 6:

The Right Information – Cybersecurity Incident Reports

What do readers of your cybersecurity incident report want to know? You'll learn to include the right information in such writing, so you can:

- Inform your readers about the incident
- Instill confidence that the proper steps have been taken
- Address concerns about relevant business risks
- Highlight the need for improvements, if any

The best way to learn how to write a good incident report is to look for problems in bad ones. You'll have many opportunities to do this.

DAY 2 – SECTION 7:

The Right Information – Pen Testing and Other Security Assessment Reports

Learn how to craft a security assessment report so the readers truly benefit from your insights. Master the skill of including just the right information to:

- Describe assessment methodology and scope
- Provide meaningful analysis, rather than raw findings
- Offer guidance that readers appreciate
- Include figures to support your conclusions

You'll review many problematic penetration testing and other security assessment reports, so you'll understand how to avoid their pitfalls.

DAY 2 – SECTION 8:

The Right Information – Malware and Other Threat Reports

Writing about cybersecurity threats, such as phishing messages, malware infections, and attack groups, can be challenging because of the multiple audiences that might read the reports. Learn how to include the right information in such writing, so your readers:

- Understand why the threat is relevant
- Know what to do after reviewing your report
- Trust the basis for your analysis
- Appreciate your research and advice

Guess what? You'll learn to include the right information in threat reports with the help of hands-on exercises, during which you'll spot and fix information-related weaknesses.

"Cybersecurity writing skills are critical for professional development."

—R. Wajda, **Secure Cloud LLC**

"I attended a training at my company right before coming here related to improving written communication. I notice similarities here but the cybersecurity focus here is invaluable!"

—Andrew Walker, **Novant Health**