D487 Guidance Document – How to Use the Study Aids

Purpose of the Study Aids:

The aids assist you in digging deeper into the material. They aid in building an understanding of the material presented in the Learning Resources. Researching the material via the aids is required, however, since you learn and acquire knowledge by interacting with the text and videos.

About Testing:

Some of the aids provide self-testing. Yet, the path to learning the material is not constantly taking tests. You cannot usually test your way to success. For example, taking the Pre-Assessment multiple times usually does not build knowledge and understanding. Just taking tests is a tempting way to get through the material, but it may not give you the depth of insight needed to be successful in the course. Studying the text, the videos, and the Cohort Modules is key.

Syllabus and Cohort Modules:

The Syllabus is the roadmap to the course. The links to the Cohort Modules in the Syllabus offer insight into Secure Software Design's major themes and topics.

DIKW:

DIKW stands for Data, Information, Knowledge, and Wisdom. This is a ladder of understanding the material in this course.

**Data** – You learn terms, definitions, and basic concepts at this layer. This is an essential step, but you cannot stop here. Isolated facts require context to be meaningful. Unfortunately, many students do not go beyond this layer. They wonder why the actual exam ends up being so challenging. The reason is that the actual exam requires applying concepts and facts to different situations.

**Information** – The tying together of different facts and concepts happens here. Patterns begin to emerge. You can start to answer some what-if questions.

**Knowledge** - You acquire some comfort level with the material. You can apply concepts to different situations. Answering questions becomes more in-depth; you are not just repeating what you memorized. To use the analogy of an automobile mechanic, you know the tools' names and then how to employ them to fix an automobile.

**Wisdom** – This level does not mean that you know everything about the discipline. We are all learning all the time, both students and faculty. This level means that you see the value of what you’ve learned and can apply it in the world. It becomes visible at work, for example, when you encounter a software issue. In conversing with professionals in the field, you grasp their ideas and concerns.

A Chart of Using DIKW in the Course:

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Goals** | **Tools** | **Questions** |
| Data | Understand basic terms and concepts | * Pre-Assessment * Gap Assessment * Matrix | Examples:  What is static testing?  What is dynamic testing?  How are fuzzers used?  What is the SDLC?  What is the SDL?  What are the elements of risk? |
| Information | Begin to make connections between facts | Use the templates in conjunction with your readings. Fill them in as you go through the readings   * Security Assessment * SDL Activities * SDL Best Practices | What are the elements of doing a security assessment?  Why is it important to consider security issues early in a software project?  What are the elements of a risk analysis?  Why is a product risk profile important?  What is a threat profile?  How do you do threat modeling?  What roles do Data Flow Diagrams play? |
| Knowledge | Applying Information | Use the following templates:   * SDL- Design and Development * Ship * Post-release * Roles and Responsibilities | What are the basic tools in software security testing?  How do you know if your testing is effective?  What are the criteria in deciding when it is safe and secure to ship a product?  Why is post-release such a critical phase?  Describe how you would handle a post-release incident crisis.  Describe the three major personnel in secure software development and what each person does. |
| Wisdom | Thinking like an Information Security Professional | Explore some of the concepts covered in the course on the Internet. Read some case studies about various software compromises and attacks. | How do information security professionals try to prevent software compromises?  How have software attacks affected you personally?  What are some of the software issues that you see in your workplace? |
| Self-evaluation | Being conversant with the material | You are ready to do the D487 test if you have a good comfort level. | How well do you feel about answering the questions? |