|  |  |
| --- | --- |
| **Course Code & Number: Name:** | |
| **Course Developer/Author:  Email:** | **eLearning Instructional Designer: Nickolas Gallegos** |

**Module Number and Title:** Directly from the *Course Design Plan: Modules* section. You will create a module design plan for each module on that document.

|  |
| --- |
| **SCADA Cyber Attacks History** |

Module Overview: Directly from the *Module Overview* column from the *Course Design Plan: Modules* section*.*

|  |
| --- |
| **In this module, students will learn about several Cyber Attack events and get an idea of what vulnerabilities SCADA systems have or have had in the past. Students will also learn how these attacks are neutralized and prevented today. 4-6 Case Studies will be discussed** |

Module Objectives:In the space below, provide the module objectives. There are typically 1 – 5 module objectives that describe what the students will be able to do after completing this module.Identify the course objective(s) that align with each module objective and, if necessary, describe the relationship. Objectives should encourage higher level thinking. *For assistance with writing effective course objectives, please refer to these resources:* [Bloom’s Taxonomy](http://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/) *and* [OPA Resource](http://www.depts.ttu.edu/opa/resources/docs/Program_Assessment_Handbook_4_13_2015.pdf) (page 7)*.*

**For K-12 courses,** **leave the Module Objectives blank in the beginning**—you will align modules to TEKS first, and then, at the end of development, you will write succinct module objectives that integrate TEKS with the actual tasks of the module.

| **Module Objectives**  By the completion of this module, students will be able to: | **Bloom’s Taxonomy Level** | **Assessment Strategy** | **Course Objectives Alignment (#)** |
| --- | --- | --- | --- |
| 1. Define major Cyber Attacks on SCADA systems | Remember |  |  |
| 1. Define key terms regarding SCADA and the protocols and systems that are utilized by SCADA systems | Remember |  |  |
| 1. Identify key vulnerabilities that lead to attacks becoming successful | Understand |  |  |
| 1. Consider what vulnerabilities could exist still today and how they could affect a SCADA system | Analyze |  |  |

Task Outline:In the table below, provide a title for each task students will need to complete in order to learn the topic/content. Describe the task and the reasoning for including in this module. Finally, note the module objective(s) that each task aligns with. **For K-12 courses,** list the detailed TEKS item that the task aligns with or supports (TEKS 1A, 1B, etc.). A K-12 example has been provided to illustrate how this document works. [Gagne’s Nine Events of Instruction](http://citt.ufl.edu/tools/gagnes-9-events-of-instruction/)

|  |  |  |  |
| --- | --- | --- | --- |
| **Step # of** [Gagne’s Nine Events…](http://citt.ufl.edu/tools/gagnes-9-events-of-instruction/) | **Task Title** | **Task Description/Rationale**   1. Write in first or second person, addressing students directly. 2. Include rationale or purpose for the task. Relate to Module Objectives where appropriate. 3. Explicit instructions for completing the task. | **Module Objective Alignment (#) or TEKS** |
| *1* | *Opening Activity* | *Below is a new clip about a controversial issue in the last presidential election. As you learn more about the presidency in this lesson, you’ll be able to look back on what you see here and decide if your understanding of this event has changed at all. Watch the video, take a few notes, and then take the Lesson Opener quiz to make sure you understood the most important parts.[link to video]* | 8B, 10B, 11C |
| 1 | Introduction | Explain how this discussion will be organized. This topic will be discussed using case studies of past cyber events. Students will learn about what a cyber-attack is, reasons they are performed, and the different vectors utilized to perform them. |  |
| 2 | Case Study 1 | Explain the attack of Case Study 1: how it happened, what effects it had, why it was done, what vulnerabilities were utilized, and how the vulnerabilities were fixed or if they still exist today. |  |
| 3 | Case Study 2 | Explain the attack of Case Study 2: how it happened, what effects it had, why it was done, what vulnerabilities were utilized, and how the vulnerabilities were fixed or if they still exist today. |  |
| … | … | … |  |
| *N*+1 | Case Study *n* | Explain the attack of Case Study *n*: how it happened, what effects it had, why it was done, what vulnerabilities were utilized, and how the vulnerabilities were fixed or if they still exist today. |  |
| *N*+2 | Review | Review the case studies discussed. Review the vulnerabilities used and how they affect security today. What protections and policies exist or may exist because of these past events? Pose questions about how a system might be exploitable today. |  |

Proposed Case Studies

|  |
| --- |
| * Stuxnet * Shamoon * Dam in New York * German Steel Mill * BlackEnergy3 * Ukraine Power Grid * Kemuri * Target Stores |