**Adam Coleman - Post Sabbatical Report**

Contents

[Value of the project to the College/unit/department 2](#_Toc16759997)

[Quality of the project 3](#_Toc16759998)

[CompTIA CertMaster Practice 3](#_Toc16759999)

[CompTIA Certmaster Learn 4](#_Toc16760000)

[TestOut 4](#_Toc16760001)

[Practice Labs 4](#_Toc16760002)

[Wiley Efficient Learning 5](#_Toc16760003)

[Any potential RIF application 5](#_Toc16760004)

[Feasibility of achieving the goals of the project 5](#_Toc16760005)

[Length of service to the College 6](#_Toc16760006)

# Value of the project to the College/unit/department

The Computer Technology (CTEC) department is currently offering CTEC 133 **– Security Fundamentals** and/or NTEC 125 – **Information Security Fundamentals** for the AAS degree. These classes are used as a foundational introduction to Information Technology (IT) security. As we are moving toward an AAT degree with our guided pathways, we are updating to an advanced security curriculum. We have chosen to use both the CompTIA Security+ and CompTIA Cybersecurity+ Analysis (CySA+) objectives for several reasons.

1. These classes will prepare the students to take CompTIA exams which are vendor-neutral, industrial recognized performance-based IT certification exams.
2. We already offer CompTIA curriculum beginning with **CompTIA IT Fundamentals+** which establishes basic computing concepts.
3. This is followed by **CompTIA A+** which focuses on IT hardware, software, and networking. This class requires the test taker to demonstrate foundational IT skills across a variety of devices and operating systems.
4. **CompTIA Security+** will expand students’ skills by focusing on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection.
5. Finally, **CompTIA Cybersecurity Analyst (CySA+)** focuses on performing data analysis and interpreting the results to identify vulnerabilities, threats and risks to an organization, configure and use threat-detection tools and secure and protect applications and systems within an organization.
6. The addition of Security+ and CYSA+ will allow the CTEC department to teach advanced security concepts.
7. The AAT program will be in alignment with the proposed Bachelors degree in Cybersecurity
8. These stackable/hierarchical certifications will work for all levels of experience from beginners up to IT professionals thus enhancing the scope of the students we will be able to serve.



Figure 1- CompTIA stackable pathway

# Quality of the project

I investigated multiple products that can be used to teach the Security+ and Cybersecurity+ class. These include:

## CompTIA CertMaster Practice

CompTIA CertMaster Practice contains only practice exams. It is designed for people that already have some knowledge of the given topic. There are no lessons, tasks, videos or lab exercises. Each test has from 10 to 40 questions.

All questions have five possible answers. The tests are very well written. You are given three choice for each question; 1) I’m sure 2) I’m not sure and 3) I don’t know. Should you select “I’m sure” or “I don’t know” you can only select one answer. If you select “I’m not sure”, you select two answers. After completing five or six questions you see if you were correct or not. Each question can be expanded to see explanations of each answer if you wish to review further. You are then asked either some of the remaining question you missed or questions you answered, “I don’t know”. This pattern continues until you answer all the questions correctly.

The instant feedback is very helpful. Test can range from 7 minutes to well over an hour. The interface is easy to follow. A full course report is generated to see the Course Average, the Course Progress and the Overall Time Spent on the questions. A full report of each question is generated for review. At the end of the training I receive a 10-hour continuing education certificate. Additionally, each question can be expanded if you wish to review further. See examples below

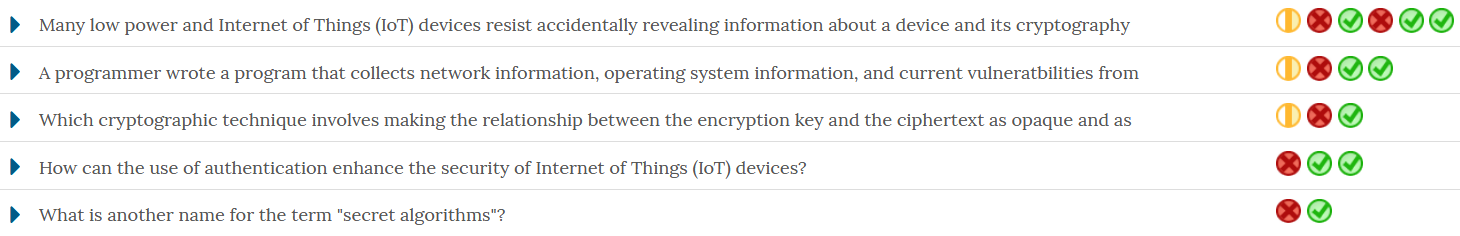


Figure 2 - Full report for each question

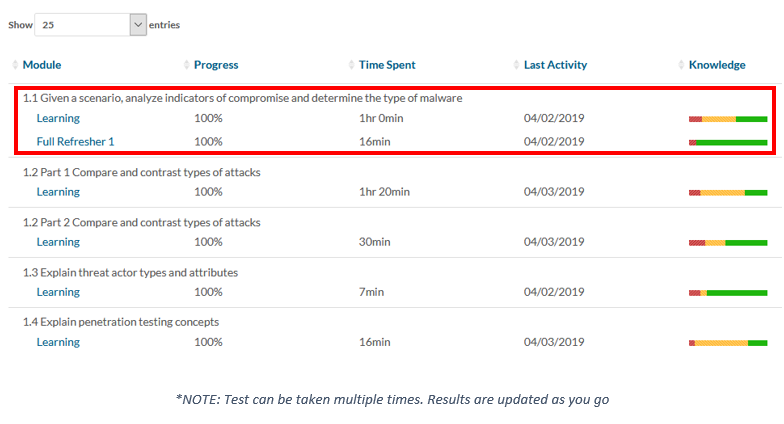


Figure 3 - Review for each test

## CompTIA CertMaster Learn

CertMaster Learn for Security+ includes 24 self-paced lessons, each featuring instructional content, matching videos and flashcards to review terms, definitions and acronyms. Along the way students can test their knowledge of key concepts by answering more than 400 multiple choice questions, with extensive feedback included in each answer.

Each of the lessons is also accompanied by an interactive performance-based question, requiring the learner to apply the knowledge they’ve gained in a scenario based on the real-world cybersecurity environment.

There are analytical reports that shows the user their strengths and weaknesses based on percentile ranking, average scores on the practice exams and average score on the assessments. There are tools on how to improve your score, learning important concepts and memorization with flash cards. It even has a game center with such games as Card Picker, Card Hunter and Card Sweeper.

## TestOut

TestOut is designed to give students a full range of hands-on experience in a simulated environment. This web-based software used multiple methods to give students a full range of learning experiences. These include:

* Video lessons that discuss the given topic.
* Video demonstrations of the topic(s)
* Interactive simulated labs that reinforces the learning objective.
* Detailed fact sheets with further explanations.
* Exams with practice questions at the end of each module.
* TestOut practice certification questions.
* A “CompTIA Study Questions Section” that covers exam objectives by course section.

Practice Labs

With Practice Labs students get access to real hardware and software they need to develop their practical skills. This is not a simulation, but rather an emulation. This mean you login and access the actual equipment you would expect to find in any work place and get hands-on experience using the hardware and software. The benefit of using this type of system is you get full functionality.

Practice labs lists the exam objectives, explains the task that is to be completed, gives a lab diagram of the equipment being used then gives step-by-step instructions on how to complete the lab. When each individual item is completed, there is an explanation as to the importance of the task with respect to the overall objective. This product offers Learning Management System (LMS) integration, student tracking and reporting, and customizable courseware.

**NOTE:** In computing, there are more than one way to complete tasks. Because of this, with simulators such as Practice Labs or TestOut, there will be limited performance. With emulators, students can have full access to the equipment and software but there may be time considerations with connecting through the internet.

Wiley Efficient Learning

This on-line product is another test bank complete with flash cards. You take an assessment exam based on the subject matter by chapter. You can select the number of questions to the test and use study or exam mode. With test mode, you take the test then see how you did. In study mode, the minute you select an answer, you are told the result and an explanation of the correct answer.

# Any potential RIF application

NOT SURE HOW TO ANSWER THIS

# Feasibility of achieving the goals of the project

I was able to find a conference that covers a good portion of the material needed for this project. I attended the CompTIA Partner Summit from August 6, thru Aug 8, 2019. I attended the following workshops:

1. **Analyzing This and That with CySA+** - In this workshop we discussed such topic as Industry Standards, Certification and renewal pathways, and Job Growth in the security industry. We then discussed key tools such as NMAP, Wireshark, Zenmap, and Social Engineering Toolkit (SET), Metasploit, Splunk, and many others that are vital in the industry.
2. **Making Security+ stick with Virtual Labs** – In this workshop, we discussed the pros and cons of Simulators and Emulators, Discussed using different cloud platforms such as Amazon Web Services (AWS), Microsoft Azure and IBM Watson
3. **Best Practices for Implementing Virtual Labs** - How to administer virtual labs in a LMS. How to use virtual machines to demonstrate security issues in class, reporting capabilities, and the advantages of using virtual machines.
4. **De-Mystifying Cybersecurity Education: How can Cybersecurity Trainings be Affordable and Effective at the Same Time?** – IN this workshop we discussed how technology and data are growing at an exponential rate. How do we keep our data safe from inside and outside of our companies? Cybersecurity must be current. Analysist are in high demand and need to be trained in technical and soft skills.
5. Besides the workshops I attended, I was able to network and meet some incredible instructors. I was able to ask them about their teaching practices, what did and didn’t work, how they presented the material, what students liked and how they measured their outcomes.

The Security+ Canvas shell has been created and is approximately 40% completed. I am going to incorporate some of the material I picked up at the conference above into the shell. I have no doubt that it will be completed and ready for the fall 2019 quarter. After that I plan on taking the CySA+ by February 2020.

I’m was overly optimistic with my initial timeline. I didn’t realize the amount of work there was. Initially, I hoped to take the Cloud+ and Security+ test at the end of Spring break but the conference above wasn’t in my projected time frame and there was much more material to go over to create the Canvas shell for it to be ready by fall quarter. I have purchased my voucher and plan on taking the Security+ exam by the end of September 2019.

# Length of service to the College

I have worked at Clark College full time for 8 or 9 years.