

Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

IDS III - On-site Log Analysis, Event Correlation and Response (Custom) Certification Class



Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

Q/CND® Qualified/ Cyber Network Defense Certificate of Mastery CoM (Q/MC, Linux, IDS I, II, III, Q/CND, Security+, CASP or CISSP) A practical provides adequate evidence to support the claim of knowing something
IDS I Catching the Hackers Intro to Intrusion Detection Certification Class & Exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert & Exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class & Exam
Q/MC® Qualified/ Mission Critical Certification Class & Exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
SU CISSP® Certified Information Security Systems Professional Class & Exam
Linux/UNIX® Security Certification Class & Exam
SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class & Exam
Cloud Computing Security Knowledge Certification (CCSK) Class & Exam
Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam
IDS III: On-site Log Analysis, Event Correlation and Response Practicum

This 72 hour class investigates how to strengthened network- and host-based intrusion detection systems (IDS). You will explore the leading IDS products on the market today, including Cisco, ISS real secure, SNORT, Tripwire Enterprise (and shareware) and more. You will compare managed services to make informed decisions about which is best suited to your organization. You will explore the pros and cons of perimeter defenses and deep internal defenses. Hacker attack labs will enrich your skills of port scanning, exploit buffer overruns, and other network assaults in action. When you leave this cutting-edge seminar, you will know where to position sensors and consoles; the types of responses you will receive; and how to react to alerts using industry-standard IDS countermeasures. Bonus: You will receive a Network Intrusion Defense Kit drive.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Advanced
Contact Hours: 37 hr Lecture 35 hr labs
Prerequisites: Basic competency with TCP/IP & Linux.
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD
Method of Evaluation: 95 % attendance 2. 100 % completion of Lab
Grading: Pass = Attendance+ labs & quizzes Fail > 95% Attendance

Sample Job Titles
Information Assurance (IA) Architect
Information Security Architect
Information Systems Security Engineer
Network Security Analyst
Research & Development Engineer
Security Architect/ Security Engineer
Security Solutions Architect
Systems Engineer/ Systems Security Analyst

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

KU Outcomes

- * Students will be able to write a system incidence response policy.
- * Students will be able to describe and write various risk analysis methodologies.
- * Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
- * Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
- * Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Who Should Attend:

CIO's; Information Security Officers; Information Technology Managers, administrators, and Auditors; Telecommunications and Network Administrators; Consultants; Systems and Data Security Analysts; Project Managers; and Technology Planners

Class Lesson Plan 37 hrs lecture/ 35 hrs labs:

2hrs Lecture 0 hr Labs

1. Introduction to IDS

- defining the role of intrusion detection in your overall network security program
- firewalls Vs IDS's
- strengths and weaknesses of host-based and network-based IDS

- integrating IDS and firewalls

2 hrs Lecture 0 hr Labs

5. IDS and threat management: staff roles --clearly define responsibilities

- law enforcement contact
- overall coordinator
- documentation
- logging

2 hrs Lecture 2 hr Labs

7. the role of IDS in threat management --forensic gathering tool

- early-warning system
- escalation procedures
- document security policy and procedures
- defining the scope of incidents to be managed
- IDS alarm severity level definitions
- incident response sources
- integrating IDS and firewalls
- IDS case studies: insourcing vs. outsourcing
- developing an effective incident response capability

1hrs Lecture 0 hr Labs

3. Managed /Insourcing vs. Outsourcing Options

2 hrs Lecture 3 hr Labs

4. Implementing IDS

- choosing an intrusion detection system
- host-based and network-based IDS
- key attributes of IDS
- placement determination
- who administers the IDS

2 hrs Lecture 4 hr Labs

8. Reacting to Threats

- monitoring traffic
- sending an alert: console, audible, pager, E-mail
- taking action based on policy
- forcing the session to disconnect
- blocking all network access from the attacking source
- blocking all network access
- incident response resources

4 hrs Lecture 4 hr Labs

9. Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information
- security mechanisms

- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

10. Essential Tools and Resources

11. What You Can Expect in the Future

Cyber threat evasion and threat mitigation 4 hr Labs

Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information
- security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Cyber Threat Vector on live cyber range 4 hr Labs

Validating the Threats: Hacker Attack Methods

- cyber range threats
- reconnaissance
- mapping networks
- access points
- relationships between systems
- system configuration
- services offered
- user information
- security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

How to Conduct Network Vulnerability Analysis class



This course will teach you how to find vulnerabilities in systems and software by teaching the process that a hacker uses when they target an organization. One of the critical things for anyone who wants to learn either how to defend or even attack a network, is the ability to find and analyze system or network vulnerabilities. In this course, How to Conduct a Network Vulnerability Analysis, you will learn to how to follow a systematic methodology to identify potential vulnerabilities. Using passive and active vulnerability scanning methods you evaluate what threats vectors are on your network, and learn how to take the results of this data and analyze it to determine the vulnerabilities that can be used to attack, or identify the risk that needs to be mitigated. This science teaches you best practices and how to deploy three of the most popular vulnerability scanners and conduct comparisons of them. When you complete this course you'll have the knowledge and skills needed to identify vulnerabilities and act appropriately to mitigate cyber risk.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 hours lab and lecture
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs& Quizzes Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Class Materials – SU class textbook, Labs and resources CD

KU Outcomes - this course will teach you how to find vulnerabilities

Students will be able to evaluate and categorize risk using 3 scanning tools

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts -Machines a Dual Core 486M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Did you hear about North Korea hacking Sony Pictures? Or about Stuxnet, one of the most sophisticated APT affecting nuclear plants in Iran? This exciting certification will require clearing CMSD first to be able to start learning how to dissect nation-state-sponsored attacks! You will learn techniques to dynamically instrument binaries during execution with PinTool, or how to create Immunity Debugger plugins to hook malicious APIs. You will have the chance to understand and practice how to dissect the most sophisticated APT in our era, The Equation Group and see how they are able to hide their presence within hard drives by reprogramming the firmware!

Learning Objectives -

You will learn techniques to dynamically instrument Student projects include performing vulnerability assessments. You cannot talk about vulnerability assessments without also mentioning penetration testing. Although both processes serve to protect a networked environment, they are not the same thing. The two terms are sometimes incorrectly used interchangeably. In a vulnerability assessment, an exploitable flaw is identified and alleviated. The process is mostly automated to cover a wide variety of unpatched vulnerabilities. Penetration testing, is focused on real-life cyberattacks to see how a hacker can breach defenses. This testing involves both automated tools and a human to mimic an attacker. Penetration testing can help identify even the most minute security problem, such as unencrypted passwords and inadequate security settings. And because penetration testing is also a vulnerability test, it should be conducted regularly to ensure consistent IT and network security management.

The different types of vulnerability assessments

Vulnerability assessments can help you find potential exploits before hackers start snooping, ensure your systems remain up to date and patched, create a proactive focus on information security, and ultimately help your organization maintain its reputation.

There are various types of vulnerability assessments. They include: Network-based assessment As the name suggests, this scan helps pinpoint possible flaws on wired and wireless networks. Database assessment -This assessment involves locating security loopholes in a database to prevent malicious attacks, such as distributed denial-of-service (DDoS), SQL injection, brute force attacks, and other network

vulnerabilities. Web application assessment - This scan involves a careful evaluation of web applications and their source code to find any security holes. The process can be done manually or automated. -Host-based assessment This type of assessment examines any possible weaknesses or threats in server workstations and other network hosts. It also involves a meticulous examination of ports and services. Wireless network assessment -This scan validates whether an organization's wireless infrastructure is securely configured to prevent unauthorized access.

Lesson 1- 11 hr lab and 4 lecture

Class covers the physical layers of the file system (from the physical platters to the file name layer that contains file names and a directory)
Course Lessons -

Lesson 2 Intro and lab set up - 10 hours labs and lecture

- Introduction
- Course Virtual Machines
- Downloading and Installing Nmap
- Demo: Downloading and Installing Nmap

Lesson 3 Performing the Scanning Methodology – 12 hours labs and lecture

- Introduction
- Demo: Non-intrusive Target Search
- Defining Intrusive Target Search
- Demo: Finding Live Systems
- Identifying Ports and Services
- Demo: Scanning Ports and Services
- Enumerating and Identifying Vulnerabilities
- Demo: Enumerating System Information
- Module Summary

Lesson 4 Leveraging the Internet to Find Vulnerabilities -12 hr labs and lecture

- Overview
- Demo: Exploring Search Engine Capability
- Examining Common Vulnerability Sites
- Demo: Leveraging Vulnerability Sites
- Module Summary
- Module Summary 2

Lesson 5 Understanding the Types of Vulnerability Scanning 13 hr labs and lecture

- Overview and Passive Analysis
- Demo: Conducting Passive Analysis
- Actively Scanning for Flaws
- Demo: Conducting Active Scanning
- Reviewing Vulnerability Scanning Tools
- Module Summary

Lesson 6 Executing Vulnerability Scanning 14 hrs labs and lecture

- Overview
- Demo: Nessus
- Introducing Nexpose
- Demo: Nexpose
- Introducing OpenVAS
- Demo: OpenVAS
- Vulnerability Scanner Comparison
- Module Summary

Lesson 7 Conclusion 12 hrs labs and lecture

- Course Conclusion and Next Steps

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Python Class and Exam



Nowadays it is common practice amongst ethical hackers to write nifty scripts and automate any structured process, ranging from small network scans to wide area network packet sniffing. In recent years, Python has become the language of choice for such tasks, and there are good reasons for this. In this class you will learn ethical hacking using Python, we will discuss the reasons that make these two such a brilliant couple. Below is the list of topics we shall be going over: What is ethical hacking? What is Python? Why use Python for ethical hacking? Simple dictionary attack using Python What is Ethical Hacking? The term hacking goes a long way back. To be exact, it all started at the Railroad Club of MIT, where both the term 'hacking' and 'hacker' were first coined. It's been almost 50 years now, and hacking has evolved into a discipline in the current day and age. With the increase in awareness regarding data protection and data privacy, hacking has been deemed as an illegal activity today. If caught, there's a good chance that you will be prosecuted for quite some time depending on the degree of harm caused. None the less, to protect themselves from hackers of all sorts, employment of Ethical Hackers has become a common practice amongst organizations. Ethical hackers are given the responsibility of finding and fixing security flaws for a certain organization before black hat hackers find them.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 hr Lecture and labs
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Labs& Quizzes Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Class Materials – SU class textbook, Labs and resources CD

KU Outcomes

Students will be able to hack using python.
Students will be able to describe how to use python to write break code
Students will be able to evaluate and categorize risk using Pthon coding

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts -Machines a Dual Core 486M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Below is the list of topics we shall be going over: What is ethical hacking? What is Python? Why use Python for ethical hacking? Simple dictionary attack using Python What is Ethical Hacking? The term hacking goes a long way back. To be exact, it all started at the Railroad Club of MIT, where both the term 'hacking' and 'hacker' were first coined. It's been almost 50 years now, and hacking has evolved into a discipline in the current day and age. With the increase in awareness regarding data protection and data privacy, hacking has been deemed as an illegal activity today. If caught, there's a good chance that you will be prosecuted for quite some time depending on the degree of harm caused. None the less, to protect themselves from hackers of all sorts, employment of Ethical Hackers has become a common practice amongst organizations. Ethical hackers are given the responsibility of finding and fixing security flaws for a certain organization before black hat hackers find them

Learning Objectives -

You will learn a general-purpose scripting language that has gained immense popularity amongst professionals and beginners for its simplicity and powerful libraries. Python is insanely versatile and can be used for almost any kind of programming. From building small scale scripts that are meant to do banal tasks, to large scale system applications – Python can be used anywhere and everywhere. In fact, NASA actually uses Python for programming their equipment and space machinery. Python can also be used to process text, display numbers or images, solve scientific equations, and save data. In short, Python is used behind the scenes to process a lot of elements you might need or encounter on your devices.

Lesson 1 -10 hours Labs and lecture
Why use Python for Ethical Hacking?
Python for super users skills
Python for use libraries.
Building python libraries
AI artificial intelligence has Pytorch and Tensorflow
Data Science has Pandas, Numpy, Matplotlib.

NAPALM, NetworkX etc make developing network tools a breeze
Ethical hackers generally develop small scripts
Python scripting language for juice performance - small programs - big programs
Python as a community tool
Learning Python for career opportunities

Lesson 2 -10 hours Labs and Lectures
Similarly, Python is brilliant for ethical hacking for the following;
Cyber Security Training
Nifty python libraries like Pulsar,

Lesson 3 -6 Labs and Lecture
Dictionary Attack using Python
Let us create a small Python program that can be used to crack a password using the dictionary attack

Lesson 3- 10 hr labs and lecture
Python is a very simple language yet powerful scripting language, it's open-source and object-oriented and it has great libraries that can be used for both for hacking and for writing very useful normal programs other than hacking programs. In the future and present era python is very popular and it's easy to learn, learning to hack with python will be fun and you will learn python programming in the best way. What you will learn Code your own reverse shell (TCP and HTTP).

Lesson 4 – 10 hr labs and lecture
Learn various concepts such as cryptography, computer networks & security, application security, idAM (identity & access management), vulnerability analysis, malware threats, sniffing, SQL injection, DoS, session hijacking, and various security practices for businesses from scratch with hands-on demonstrations. Enroll in this Cyber Security certification training program to learn from experienced industry professionals, work on real-time projects and become a certified expert..

Lesson 5 – 10 hrs labs and lecture
Root - since Python is basically part of every single Linux install, you could do a shitton retrieving system and user information by just using the normal packages. You won't even need to install nmap or similar; using plain Python packages, you could check which services are running and such.).

Lesson 6 10 hr labs and lecture
Gives information on useful tools every penetration tester/hacker should have in their arsena
snippet of codes to fix and learn
everything from writing network sniffers,
stealing email credentials,
bruteforcing directories
crafting mutation fuzzers
investigating virtual machines,
creating stealthy trojans.

Lesson 7 - 16 Lecture & Labs
Python 3.x bit shifting
code hygiene
offensive forensics with the Volatility Framework
expanded explanations of the Python libraries ctypes, struct, lxml, and BeautifulSoup,
offensive hacking strategies like splitting bytes, leveraging computer vision libraries, and scraping websites.

- Create a trojan command-and-control server using GitHub
- Detect sandboxing and automate common malware tasks like keylogging and screenshotting
- Extend the Burp Suite web-hacking tool
- Escalate Windows privileges with creative process control
- Use offensive memory forensics tricks to retrieve password hashes and find vulnerabilities on a virtual machine
- Abuse Windows COM automation
- Exfiltrate data from a network undetected

When it comes to offensive security, you need to be able to create powerful tools on the fly. You will not find a lab this extensive anywhere else! Overall: All in all this course is so relevant and so practical that there is no reason not to put this one on your wishlist

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Python Powershell Incident Response Class



Nowadays most of the windows-based attacks are happening around PowerShell. As an Incident Responders, you should know your way around PowerShell especially on how the attackers can leverage PowerShell in various ways within the attack lifecycle. The aim of this article is to give a glimpse of different techniques in the PowerShell arsenal which can aid responders in hunting activities. This course focus is on battling the much maligned Advanced Persistent Threat (APT). This course is up to date with the latest forensics techniques. Incident management is an often-debated, frequently misunderstood topic that can quickly befuddle even the most advanced security teams. So to clear things up, we took "lessons learned" from successes and failures over the years. And while it may not answer every question you may have about modern incident response, we hope that it sets the wheels in motion for something better than what you have today.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	41 hr Lecture 31 hr labs
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs& Quizzes Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Class Materials – SU class textbook, Labs and resources CD

KU Outcomes

Students will be able to write a script in powershell.

Students will be able to describe how to use powershell to write various risk incident and analysis methodologies.

Students will be able to evaluate and categorize risk using powershell incident response

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts -Machines a Dual Core 486M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Did you hear about North Korea hacking Sony Pictures? Or about Stuxnet, one of the most sophisticated APT affecting nuclear plants in Iran? This exciting certification will require clearing CMSD first to be able to start learning how to dissect nation-state-sponsored attacks! You will learn techniques to dynamically instrument binaries during execution with PinTool, or how to create Immunity Debugger plugins to hook malicious APIs. You will have the chance to understand and practice how to dissect the most sophisticated APT in our era, The Equation Group and see how they are able to hide their presence within hard drives by reprogramming the firmware!

Learning Objectives -

You will learn techniques to dynamically instrument binaries during execution with PinTool, or how to create Immunity Debugger plugins to hook malicious APIs. You will have the chance to understand and practice how to dissect the most sophisticated APT in our era, The Equation Group and see how they are able to hide their presence within hard drives by reprogramming the firmware! This course is a enrichment style lab immersion concept:

This class has recently been retooled to focus on battling the much maligned Advanced Persistent Threat (APT). The class motto is "APT is in your network, start hunting". The APT focus makes it 100% relevant to not just forensic investigators, but to anyone wanting to learn to defend their network. The Material - this course is a smorgasbord of valuable skills and information for incident responders, system administrators, and forensicators alike.

Lesson 1- 11 hr lab and 4 lecture

Class covers the physical layers of the file system (from the physical platters to the file name layer that contains file names and a directory structure), and how to properly mount images for analysis (e.g. read only). Just when you think the first day couldn't cover any more

information the class jumps into the exciting world of Enterprise Analysis and Live System Incident Response (my favorite!!). This portion teaches students about domain authentication, how to secure domain administrator credentials, and many methods of accessing system information on remote of hosts (Many of my future blog posts will revolve around utilizing PowerShell for "Live System 'Enterprise' Incident Response" for lack of a better term).

Lesson 2 – 10 hr labs 4 hr lecture

The second day is spent covering memory forensics. Memory Forensics covers the details of memory (memory structures and such), and how to implement memory forensics TODAY. Students will learn how to acquire memory, as well as, how to provide in depth analysis of the memory once acquired. Memory forensics is absolutely necessary when combating APT as it is one of the best, if not only, methods to detect rootkits. The best part of lesson 2 is that it doesn't focus on one method of analyzing memory. We spend the time to teach students the pros and cons to different tools, and even different methods of using the same tool.

Lesson 3 - 10 hrs labs and 4 hr lecture

is dedicated to timeline analysis. No one should be considered a forensicator or incident responder if they do not have an intimate knowledge of timeline analysis (Specifically using log2timeline). Log2timeline came out of a GCFA Gold Paper written by Kristinn Guðjónsson, and the community has never looked back. Log2timeline is really a cultural shift in the way we perform investigations, as it aggregates almost every forensic artifact into one timeline that truly tells the story of actions taken on a machine. We will interpret a specific artifact, then you lose fidelity in your timeline (possibly the opportunity to spot malicious activity).

Lesson 4 and 5 - 21 hr labs and 6 hr lecture

begin with XP Restore Point and Volume Shadow Copy analysis which can be harnessed for some really cool stuff. We can use these snapshots to add fidelity and depth to our timeline, and we can use them to recover deleted files. Then deep dive forensics (This is where the class dives into the weeds of file system analysis). The class dives into \$MFT analysis which introduces us to a second set of timestamps (\$STDINFO), and new artifacts like the NTFS TriForce (David Cowen's baby). These artifacts are presented in this class –and we wraps up with methods and techniques of finding unknown malware. Assuming anti-virus fails to detect a threat, what are some methods we can use for detection? This class end introduces and spends half a day discussing the concept of malware funneling which is the process of reducing data through a series of automated tasks until you have a small enough data set that you can perform manual analysis. Labs (1-6): After the lesson students spend the rest of the lesson in the lab as a team exercise. The team investigates a set of hosts that were part of an intrusion, however this is not your normal everyday exercise....this is where it gets interesting!

This course is developed around an "as real as it gets" scenario. The scenario is about an R&D firm that makes a great discovery, only to be hacked by APT. Students are given four hosts to conduct forensic investigations to determine what happened. Questions like the initial infection vector, when the initial infection occurred, what data was lost, and the current state of the network can be answered. When we talk about this lab it is important to understand the level of detail used to create this virtual network. Not only did the network have 100s of hosts and 1000s of users, we ensure this network was as real looking as possible. We hired a professional Red Team and trained them up to act like APT, he hired domain architects to build the domain in a professional/secure manner, and he even loaded the systems with some of the latest security tools. You will not find a lab this extensive anywhere else!

Overall: All in all this course is so relevant and so practical that there is no reason not to put this one on your wishlist.

SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery CPoM / non degree-
Q/SA® Qualified/ Security Analyst Penetration Tester Certification Class & exam
Q/PTL® Qualified/ Penetration Tester License workshop
Q/EH® Qualified/ Ethical Hacker Certification Class & exam
Q/ND® Qualified/ Network Defender Certification Class & exam
Q/FE® Qualified/ Forensic Expert Certification Class & exam
SU CISSP® Certified Information Security Systems Professional Class & exam
SU Security+® CompTIA Certification Class & exam
SU CASP® - CompTIA Advance Security Professional Certification Class & exam
Linux/UNIX® Security Certification Class & exam
Cloud Computing Security Knowledge Certification (CCSK & Plus) Class & exam
Q/PTL® Qualified/ Penetration Tester License Practical required to graduate
Q/ND® Qualified/ Network Defender Certification Practical required to graduate
Q/FE® Qualified/ Forensic Expert Certification Class Practical required to graduate



Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery Powershell Forensics Class



Even for seasoned PowerShell users, a deep and robust understanding of the language fundamentals can be incredibly powerful for writing more efficient, readable, and usable code. Section 1 of the course focuses on building a solid foundation upon which more complex use cases can then be constructed. With a focus on Blue Team specific functions, we frame the discussion around the PowerShell basics in terms that will be immediately useful for students. For example, common data structures are discussed as a fundamental aspect of PowerShell and immediately applied as Blue Team triage and analysis tactics. This base is built from the ground up and accessible to students with no prior scripting experience, but with enough nuance to shed light on the "why does it work this way" question for more seasoned PowerShell users. For professionals already familiar with the basic concepts, PowerPlay offers an interactive, out-of-band challenge system for students to drill various concepts and techniques related to the course material.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	41 hr Lecture 21 hr labs
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Labs& Quizzes Fail > 95% Attendance

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. Machines a Dual Core 16M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

This course Effective Blue Teams work to harden infrastructure, minimize time to detection, and enable real-time response to keep pace with modern adversaries. Automation is a key component to facilitate these capabilities, and PowerShell can be the glue that holds together and enables the orchestration of this process across disparate systems and platforms to effectively act as a force multiplier for Blue Teams. This course will enable Information Security professionals to leverage PowerShell to build tooling that hardens systems, hunts for threats, and responds to attacks immediately upon discovery.

Now that we have a strong understanding of the fundamentals, this course section focuses on ways to weaponize PowerShell both from an offensive and defensive perspective. The section begins with a focus on offensive PowerShell use cases. Threat actors have long used PowerShell as an attack platform, delivering fileless malware and living off the land using built-in capabilities. The next section turns this discussion around and focuses on the Blue Team aspects of controlling PowerShell execution.

The section then dives deep into log analysis and data parsing and discovery. The goal is to maximize the utility of native features of operating systems and applications while fully understanding how to find important data. If Blue Teams can identify sensitive data in unexpected locations, those data can be handled or protected properly. The section concludes with a discussion of PowerShell as a platform to enable Blue Teams to work within DevOps development practices. As modern development teams transition practices, Blue Teams must adapt. Automation plays an important role in this process, as Blue Teams fight to scale capabilities to match modern development frameworks. PowerShell provides this automation platform and can be the catalyst to enable continuous assurance of critical business services. PowerShell is uniquely positioned for this task of enabling Blue Teams. It acts as an automation toolset that functions across platforms and it is built on top of the .NET

Students will learn:

- PowerShell scripting fundamentals from the ground up with respect to the capabilities of PowerShell as a defensive toolset
- Ways to maximize performance of code across dozens, hundreds, or thousands of systems
- Modern hardening techniques using Infrastructure-as-Code principles
- How to integrate disparate systems for multi-platform orchestration
- PowerShell-based detection techniques ranging from Event Tracing for Windows to baseline deviation to deception
- Incident Response techniques leveraging PowerShell-based automation

This course is meant to be accessible to beginners who are new to the PowerShell scripting language as well as to seasoned veterans looking to round out their skillset. Language fundamentals are covered in-depth, with hands-on labs to enable beginning students to become comfortable with the platform. For skilled PowerShell users who already know the basics, the material is meant to solidify knowledge of the underlying mechanics while providing additional challenges to further this understanding.

The PowerPlay platform built into the lab environment enables practical, hands-on drilling of concepts to ensure understanding, promote creativity, and provide a challenging environment for anyone to build on their existing skillset. PowerPlay consists of challenges and questions mapping back to and extending the course material. Between the course material and the PowerPlay bonus environment, students will leave the course well equipped with the skills to automate everyday cyber defense tasks. You will return to work ready to implement a new set of skills to harden your systems and accelerate your capabilities to more immediately detect and respond to threats.

Exercises - Hands-on PowerShell: Get comfortable with PowerShell cmdlets, objects, and the pipeline to start making meaningful tools.

Triage the VM: Quickly understand the state of a system, from networking details to process execution and removable devices

Scripting in PowerShell: Leverage an understanding of the language basics to build high-quality tooling that will be supportable by Blue Teams.

Debugging: Save time and frustration, easily identifying complex bugs in PowerShell through built-in debugging capabilities and Pester tests

Source Control: Become familiar with Git concepts to effectively manage version control

Lesson 1 12 hrs labs & lecture

Getting to Know PowerShell
Background and history
Why PowerShell is such a good fit for Blue Teams
How to use commands and find them
Objects and pipelines as PowerShell differentiators
Extending PowerShell with .NET

Lesson 2 12 hrs lab and Lecture

Blue Team Use Cases
Network inspection
Triage at the operating system level
File discovery and inspection
Language Basics

Lesson 3 12 hrs labs and lecture

Variables, data structures, and flow control
Input and output
Functions and script blocks
PowerShell Environment
Customizing the console
Common development environments

Lesson 4 12 hr labs and lecture

Debugging
Static code analysis
Tracing and breakpoints
Helpful tools like Pester and PSScriptAnalyzer
Source Control
Git terminology

Lesson 5 12 hr labs and Lecture

Creating repositories and branches
Managing code with pull requests
Driving release pipelines from source control

Lesson 6 12hr labs and Lecture

Exercises
Offensive PowerShell: Build a fileless keylogger that automatically exfiltrates keystrokes to cloud storage
Controlling PowerShell: Analyze the impact of a stronger security posture surrounding PowerShell usage in the enterprise.
Efficient Log Analysis: Understand how to efficiently analyze and filter Windows events and plaintext log files, and find attacks within sample log files

Parsing and Discovery: Build tools to extract important data from unstructured text-based logs and use these same techniques for sensitive data discovery

DevOps: Leverage PowerShell as an orchestration engine, building containers for automated web application scanning and identifying potentially compromised containers in the environment

Lesson 7 12 hr Labs and Lecture

Offensive PowerShell

Common tactics used by attackers leveraging PowerShell

Fileless implementation techniques

NET utilization by PowerShell-based attack tools

Controlling PowerShell

Limiting attack surface on PowerShell-enabled systems

Controlling, not attempting to block, PowerShell in the enterprise

Just Enough Administration for enabling secure usage of administrative PowerShell sessions

Log Analysis

Enabling appropriate logging

Reading and filtering Windows Event Logs

Reading and filtering plaintext logs

Text Parsing

Regular expressions and string operations to enable efficient parsing

DevOps

Automating static and dynamic application security testing

Pipeline assurance automation

Container interaction, security assessment, and triage

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery Certificate of Cloud Security Knowledge (CCSK & CCSK Plus) Class



As organizations migrate to the cloud, they need information security professionals who are cloud-savvy. The CCSK certificate is widely recognized as the standard of expertise for cloud security and gives you a cohesive and vendor-neutral understanding of how to secure data in the cloud. The CCSK credential is the foundation to prepare you to earn additional cloud credentials specific to certain vendors or job functions.

This class provides the foundational knowledge needed to utilize cloud services and enables you to gain critical insights into topics such as data security, key management, and identity and access management and speak with confidence about cloud security concerns.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	41 hr Lecture 31 hr labs
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Labs& Quizzes Fail > 95% Attendance
Text Materials:	labs, SU Pen Testing Materials, resource CD's and attack handouts

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. Machines a Dual Core 16M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Who Is This Program For?

Cloud Computing Analyst, Cloud Administrator, Cloud Architect, Cloud Engineer, Enterprise Architect, Security Administrators, Security Architect and Systems Engineer are cloud security job roles.

What you will learn:

Introduction to Information Security within Cloud Computing

Selecting secure cloud services begins with understanding business requirements. This course will teach you to identify and select secure cloud services based upon business requirements.

The Certificate of Cloud Security Knowledge, enables you to gain critical insights into topics such as data security, key management, and identity and access management. You'll have the skills and knowledge of Managing Cloud Security and Risk needed to reduce risks to an acceptable degree to the business. With an expanding array of cloud services being offered daily it is easy for the inexperienced to lack awareness of security functions in cloud offerings. In this course, Introduction to Information Security within Cloud Computing, you'll learn to identify and select secure cloud services based upon business requirements. First, you'll explore the detailed definition of cloud computing. Next, you'll discover the deployment and service models of cloud computing. Finally, you'll learn how to use a matrix to review the controls enacted by a cloud provider. When you're finished with this course, you'll have the skills and knowledge of, Introduction to Information Security within Cloud Computing needed to select secure cloud services that meet business requirements.

Introduction:

Lesson 1: 8 hr lab and lecture:

Defining Cloud Computing and Essential Characteristics

Chapter 13: Security as a Service

Chapter 14: Related Technologies

Chapter 15: ENISA Cloud Computing: Benefits, Risks and Recommendations for Security

Chapter 3: Legal Issues, Contracts, and Electronic Discovery

Defining Cloud Computing and Essential Characteristics

Standard Definition of the Cloud

NIST Definition of Cloud Computing
ISO IEC 17788: Definition of Cloud Computing
Summary

Lesson 2: 10 hr labs and lecture:

Understanding Cloud Deployment and Service Models
Chapter 6: Management Plan E and Business Continuity
Chapter 7: Infrastructure Security
Cloud Deployment Models
Cloud Service Models
CSA'S Logical Model
M3 C4 Summary

Lesson 3: 16 hrs lab and lecture:

Establishing a Secure Cloud Architecture
Chapter 8: Virtualization and Containers
Chapter 9: Incident Response
Chapter 10: Application Security
Chapter 11: Data Security and Encryption
Chapter 12: Identity, Entitlement, and Access Management
CSA Enterprise Architecture
CSA-BOSS Pillar
CSA-ITOS Pillar
CSA-Services Pillar
CSA-Risk Management Pillar
NIST Cloud Computing Reference Architecture
Using the Cloud Control Matrix
Selecting a CSP
Summary and labs

Lesson 4: 12 lab and lecture:

Understanding Governance and Enterprise Risk Management in the Cloud
Chapter 1: Cloud Computing Concepts and Architectures
Chapter 2: Governance and Enterprise Risk Management
Understanding Governance and Enterprise Risk Management In the Cloud
Review of Governance Frameworks Cloud Governance Tools
Enterprise Risk Management Frameworks
Risks Related to Service and Deployment Models
Summary and labs

Lesson 5: 12 lab and lecture:

Maintaining Compliance and Audit Management in the Cloud
Appendix A: Cloud Security Lexicon
Appendix B: Cloud Security Standards and Certifications
Appendix C: Sample Cloud Policy
Compliance Objectives
Industry Specific Compliance
Cloud Audit Management
Attestation of Cloud Controls
Certification of Cloud Controls

Summary

Lesson 6: 9 hr lab and lecture:

Compiling Legal Issues, Contract, and Electronic Discovery
Chapter 4: Compliance and Audit Management
Chapter 5: Information Governance

Common Concerns for Cloud Data Privacy
Country and Regional Data Privacy Laws
European Union and European Economic Area
The Americas
Electronic Discovery
Cloud Data Security Lifecycle

Summary

Earning the CCSK will provide you with the knowledge to effectively develop a holistic cloud security program relative to globally accepted standards. It covers key areas, including best practices for IAM, cloud incident response, application security, data encryption, SecaaS, securing emerging technologies, and more. If you want to learn more, you can the CCSK guide.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President.

Advanced CCSK –

36 hours of in-depth discussion of cloud platform technologies; giving you a look into how the services are built and managed, and the security implications. We will then quickly start building out a sandbox environment and deploying security controls.

Some of the topics and techniques covered will include (at a minimum):

- Use of accounts for managing blast radius.
- Building out advanced cloud virtual networks.
- Leveraging inherent cloud capabilities for network security.
- Use of DNS management, auto scale groups, load balancers, and other technologies for immutable infrastructure.
- Advanced Identity and Access management for cloud, including setting up SAML federation across providers.
- Privileged user management, MFA, and other access essentials.
- Securing serverless, PaaS and mixed IaaS/PaaS architectures.

This next 36 hours focuses on designing secure architectures, integrate with evOps, and build your own SecDevOps toolkit for managing cloud security at scale:

- Fundamentals of SecDevOps.
- Building secure deployment pipelines.
- Integrating automated security testing into deployment pipelines.
- Cloud security architectural patterns for major application types.
- Cloud data security and encryption.
- Automating continuous security monitoring and alerting using cloud native capabilities.
- Security automation through the console.
- Security automation through code.
- Scaling your security operations to hundreds (or thousands) of accounts through automation.

Students should have basic familiarity with at least one public cloud provider (Amazon or Azure) and hands-on experience launching and managing basic instances/services. They should also be comfortable with the command line and basic scripting. Additionally we highly encourage students to understand basic Ruby programming for the coding portions. Code snippets will be provided, so students with experience in other languages should be able to keep up. This is a very broad, advanced training that requires a diverse skills set to complete all the labs. Students may fall behind in certain sections due to the rapid pace but the labs can all be completed outside of the training environment if needed. Only about 10% of those who take the class have the background to complete every hands-on portion but we ensure through lecture that everyone gains the needed knowledge.

Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

An essential component in any comprehensive enterprise security program is the ability to detect when your networks or systems are being probed or attacked, or have been compromised in some manner. Intrusion detection systems give you this critical monitoring capability.

In this up-close, 72 hour class look at intrusion detection systems (IDS), you'll get a firm grip on everything from the leading IDS systems and attack signatures to creating a Threat Management Procedure. You will learn about the different types of intrusion detection systems, how they operate, how they should be managed, how and where they should be deployed, who the players are, and whether IDS is something that should be outsourced or kept in-house. After installing multiple IDS solutions, you will benefit from a demonstration of hacker attack methodologies and see for yourself how IDS can help to detect them. You will explore new directions in the IDS arena that promise to make intrusion detection systems easier to manage and a more effective part of your information security strategy. Through a wide array of exciting hands-on exercises you will not only install and configure IDS systems but you will observe first-hand many hacker "attacks" and exploits and how they appear to IDS systems. Implementation exercises will include of a representative sample of the latest IDS tools will include a combination of both freeware and commercial IDS tools. You will have the opportunity to create real attack scenarios to see how and learn from the best how to detect, read, react, and defend your network against from serious attacks.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 27 hr Lecture 35 hr labs
Prerequisites: Understanding of TCP/IP Protocols
Credits: 50 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and Practical Fail > 95% Attendance

Sample Job Title
IA Operational Engineer
IA Security Officer
IS Analyst/Administrator
IS Manager/ IS Specialist
IS Security Engineer
IS Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

KU Outcomes:

- * Students will be able to write a system security policy, Students will be able to describe and write various risk analysis methods.
- * Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses. * Students will be able to compare the advantages and disadvantages of various risk assessment methodologies.* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Who Should Attend: CIOs with responsibility for Computer Security, Network Administrators, Information Security Architects, Auditors, Consultants, and all others concerned with network perimeter security.

Learning Objectives different types of intrusion detection systems, how they operate, how they should be managed, how and where they should be deployed, who the players are, and whether IDS is something that should be outsourced or kept in-house. After installing multiple IDS solutions, you will benefit from a demonstration of hacker attack methodologies and see for yourself how IDS can help to detect them. *Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts. Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation* Tools for class, Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan

Class Lesson Plan : 39 Lecture/ 33 Labs

Lesson 1

Role and Operating Characteristics of IDS

2 hr Lecture 1 hr labs

- Identifying major IDS functions
- Defining the role of IDS related to firewalls and other network perimeter security safeguards

1. Choosing an Intrusion Detection System

2 hr Lecture 2 hr labs

- Host-based vs. network-based IDS
- Key attributes for positioning IDS in the network
- Determining who administers the IDS

2. **Lesson 2**
IDS Architecture
2 hr Lecture 2 hr labs
 - Integrating IDS and firewalls
 - Sensors
 - Collectors
 - Management consoles
 - IDS in the weeds
3. **Lesson 3**
IDS Operation
2 hr Lecture 3 hr labs
 - Sensors
 - Definition of anomalous traffic
 - Minimizing false positives
 - Correlation with other SMTP sources
 - Multiple security management consoles
 - Hands-on exercises: installing and configuring a sample of prominent IDS products (SNORT, Cisco Secure Intrusion Detection, ISS Real Secure, and **Enterasys** Dragon IDS)
4. **Threat Management: Reacting to the Attack 2 hr Lecture 2 hr labs**
 - Best practices for defining responsibility
 - Establishing a law enforcement contact
 - The role of an overall IDS coordinator
5. **Lesson 4**
The Role of IDS in Threat Management
2 hr Lecture 2 hr labs
 - Using IDS as forensic gathering tool
 - Early warning systems
 - Escalation procedures
 - Creating a framework for IDS alert criteria and response center
6. **Document Security Policy and Procedures**
2 hr Lecture 3 hr labs
 - IDS alarm severity levels
 - Incident response sources
7. **Lesson 5**
Real-Time Reaction to Threats
2 hr Lecture 3 hr labs
 - Integrating IDS and firewalls
 - IDS case studies
 - Developing an effective incident response capability
 - Hands-on exercises: Creating a template for managing the people and the processes for IDS Defense Procedures.
8. **Validating the Threats: Looking at Hacker Attack Methods**
3 hr Lecture 3 hr labs
 - Hacker attacks
 - Bug exploitation
 - Buffer overruns
 - Attack Scenarios
 - Common types of attacks that an IDS can help detect
 - Network scans
 - Port scans
 - Denials-of-service: Smurf, Land, Trin00, Stacheldraht
 - "DE-synching" an IDS
 - Fragmentation
 - What an IDS might not detect
 - CGI exploits
 - Malformed URL's
 - Other application-layer attacks
 - Race condition
 - Trust exploitation
 - Social engineering
 - Physical access
 - Hands-on exercises:
 - Real-time TCP/IP monitoring
 - Live signature review and analysis

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

Project Manager Professional Certification PMP



SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, CASP, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practical)
<i>SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission assurance.</i>
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA CMMC Cybersecurity Maturity Model Certification class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum
PMP Project Manager Professional Certification Class & Exam

Get results using time-tested strategies and practical, hands-on tools to execute and succeed in project management. You'll learn how to scope projects effectively, improve time budgeting and resource allocation, and get the project done on time and within budget.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 Lecture hrs
Prerequisites:	None
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: System administrators, security administrators, Security auditors. Unix box owners. Anyone who has a vested interest in managing their projects. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions.

KU Outcomes:

- * Students will be able to describe potential system attacks and the actors that might perform them.
- * Students will be able to describe cyber defense tools, methods and components.
- * Students will be able to apply cyber defense methods to prepare a system to repel attacks.
- * Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives: 72hrs Lecture

Students will gain a general understanding of how to manage projects.

Lesson 1 14hrs Organizing the Project and Its Components On the surface, project management seems straightforward. However, at best, only 80% of projects end up being economically successful. The remaining 20% of projects usually cost more than estimated, run late, or fail to satisfy goals or meet objectives. In this course, Instructors shares clear, understandable, and practical methods for achieving better results. You will practice breaking down a project into pieces that can be scheduled, tracked, and controlled. While this is not a

prep course for a project management certification, it will be quite valuable for anyone who is interested in pursuing one. This program will equip you with the concepts, tools, and language of project management that can be applied to any size and type of project. The course is not specific to any formal project management software (e.g. Microsoft Project), but will require that learners have Microsoft Excel with its free Solver add-on installed.

Lesson 2 14 hrs Planning and Managing Resources . Students will identify strategies to integrate resource availability constraints into project planning, scheduling, and control. This course is designed for project managers who seek better practical results for aligning available resources with tasks and bringing activities to completion on time. Students will examine compression strategies for bringing a project that's running late back on track and will explore how to handle common types of project creep, such as handling customer requests that require extra time, and working with team members who decide independently to invest extra effort in a task. This course combines a focus on formal project management mechanisms with an emphasis on the human element: what can project managers do to resolve issues brought about in the normal course of working with customers, team members, and stakeholders?

Lesson 3 14 hrs Assessing, Managing, and Mitigating Project Risk Risk management is a key function in project management. Project managers should be able to apply a variety of risk-management tools in their work, including performing risk identification, quantification, response, monitoring, and control. In this course you will examine the nature and types of project risk and learn to apply specific mitigation strategies. You'll have an opportunity to analyze a past project you've worked on and assess what the risks might have been and why. Then you'll analyze the outcomes: Did the known risks come to fruition? What were the leading indicators? What could they have done for contingency planning at the beginning? By asking these questions, you'll then be able to perform several calculations to compute the probability that a project will finish on time.

Lesson 4 14 hrs Using Earned Value Management for Project Managers -Project managers need to keep things on track by keeping a close eye on the scope of and resources invested in a project. Forecasting, adjusting, and applying corrective measures during the project lifecycle are also key functions of a project manager. This set of processes and protocols that help ensure project success is called earned value management (EVM). Every project manager should have at least a working knowledge of EVM and its theoretical underpinnings. This course is designed for project managers who seek an introduction to EVM to achieve better practical results for implementing project controls, including financial controls and schedule controls. The calculations presented here are meant for any experienced project manager, including those who are not engineers, to apply to any size project. Students in this course will be most successful if they have a foundational understanding of standard project management tools and processes including project networks, project budgets and schedules, and work breakdown structures.

Lesson 5 15hrs Agile Project Management Approaches In traditional project management, we tend to make assumptions: the customer knows precisely what they want, or the team's workflow and tasks will go according to plan and in sequence. Practically speaking, this is rarely the case. Sometimes the customer doesn't know what they need until they see an early iteration of your team's work and can provide feedback. Because of this, work is usually done incrementally. We must build flexibility, even agility, into the model in order to succeed. This course is designed for project managers who want to get better practical results with adaptive approaches to projects. Students in this course will be most successful if they have a foundational understanding of traditional project management tools and processes including project networks, budgets and schedules.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

ITIL V3 Certification



ITIL stands for Information Technology Infrastructure Library. ITIL is a set of best practice processes for delivering IT services to your organization's customers. ITIL has its foundations in the IT world, but its principles can easily be used outside of it, within Facilities or HR departments, for instance. You can maximize value to the business by aligning your organization's processes and services with your business needs. Applying ITIL offers multiple advantages by: Giving input for process improvements and helping to solve service delivery issues. Stimulating process-based thinking and working, while making the effects of doing this visible. Introducing a general terminology used by service providers and customers, so that everyone is always on the same page

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, CASP, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practical)
<i>SU Q/IAP®</i> Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/CSO, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission <i>assurance</i> .
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA CMMC Cybersecurity Maturity Model Certification class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum
PMP Project Manager Professional Certification Class & Exam
SU Q/ISO Qualified/ Chief Information Security Officer Certification Class & Exam

Get results using best practices for delivering IT services to your clients. You'll learn how to scope projects effectively, improve time budgeting and resource allocation, and improve IT services within budget.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 Lecture hrs
Prerequisites:	None
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: System administrators, security administrators, Security auditors. Unix box owners. Anyone who has a vested interest in managing their projects. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions.

KU Outcomes:

- * Students will be able to describe best practice processes for delivering IT services to your organization's customer.
- * Students will be able to apply a framework in your organization.

Learning Objectives: 72hrs Lecture

Students will gain a general understanding of how to manage lifecycle Technical frameworks.

Lesson 1 20hrs ITIL V3 – the five lifecycle stages

ITIL V3 was introduced in 2011. In this latest iteration, the framework consists of five lifecycle stages. These stages are split up into multiple processes relying on service principles, processes, roles and performance measures.

The five lifecycle stages are:

Service Strategy: focuses on defining your organization's strategy to serve customers, and how to maintain and implement that strategy. The goal of this lifecycle stage is to make your organization think and act in a strategic manner.

Service Design: focuses on converting the Service Strategy into reality, by designing and developing new service offerings, or improving your organization's existing offerings.

Service Transition: focuses on bringing together all assets within a service and ensuring these are integrated and tested. Also focuses on the quality of a new or changed service before it becomes operational.

Service Operation: focuses on ensuring that there are robust best practices that support responsive services. For instance, Incident Management and your organization's service desk are part of this stage.

Continual Service Improvement: focuses on improving the effectiveness and efficiency of your organization's IT processes and services.

Basically, this lifecycle stage continuously improves the other four stages

Problem Management: can ITIL fix the problem?

Lesson II 22hrs Six guidelines for successfully implementing ITIL

TOP desk believes that you should apply the parts of ITIL that help your organization offer better services.

Keep the following six guidelines in mind when applying the framework in your organization:

Realize ITIL is a theory, not a goal in itself. It is a theoretical framework, not a best practice. It's a means to an end.

Start from your daily practice. Use a concrete problem when applying the stages and processes. Don't start from the theories themselves.

Give your employees the knowledge they need. Because ITIL V3 is much more comprehensive than V2, it's no longer worth sending your organization's employees to a complete Foundation training.

Dare to choose. Which processes do you need and, more importantly, in which order do you want to use them?

Don't overestimate your organization's maturity. In some organizations, basic call or change management workflows can still be improved. It's better to focus on that, instead of implementing ITIL as soon as possible.

Low priorities don't mean a process isn't important. Some processes, such as setting up a Service Catalogue, aren't prioritized highly in the Service Design lifecycle phase. This doesn't mean a Service Catalogue isn't important.

Lesson III 20 hrs What is ITSM?

What is ITIL?

What is Shift Left?

What is Incident Management?

What is IT Asset Management?

What is IT Change Management?

What is Workforce Enablement?

What is Agile Service Management?

What is Knowledge Management?

Best practices for your IT Service Management department

Agile Project Management Approaches In traditional project management, we tend to make assumptions: the customer knows precisely what they want, or the team's workflow and tasks will go according to plan and in sequence. Practically speaking, this is rarely the case.

Sometimes the customer doesn't know what they need until they see an early iteration of your team's work and can provide feedback.

Because of this, work is usually done incrementally. We must build flexibility, even agility, into the model in order to succeed. This course is designed for project managers who want to get better practical results with adaptive approaches to projects. Students in this course will be most successful if they have a foundational understanding of traditional project management tools and processes including project networks, budgets and schedules.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course.

However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

CMMC Cybersecurity Maturity Model Certification



To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. With its streamlined requirements, CMMC 2.0: Cuts red tape for small and medium sized businesses Sets priorities for protecting DoD information Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

Overview of the CMMC Program - The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements. The framework has three key features: Tiered Model: CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.

Assessment Requirement: CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.

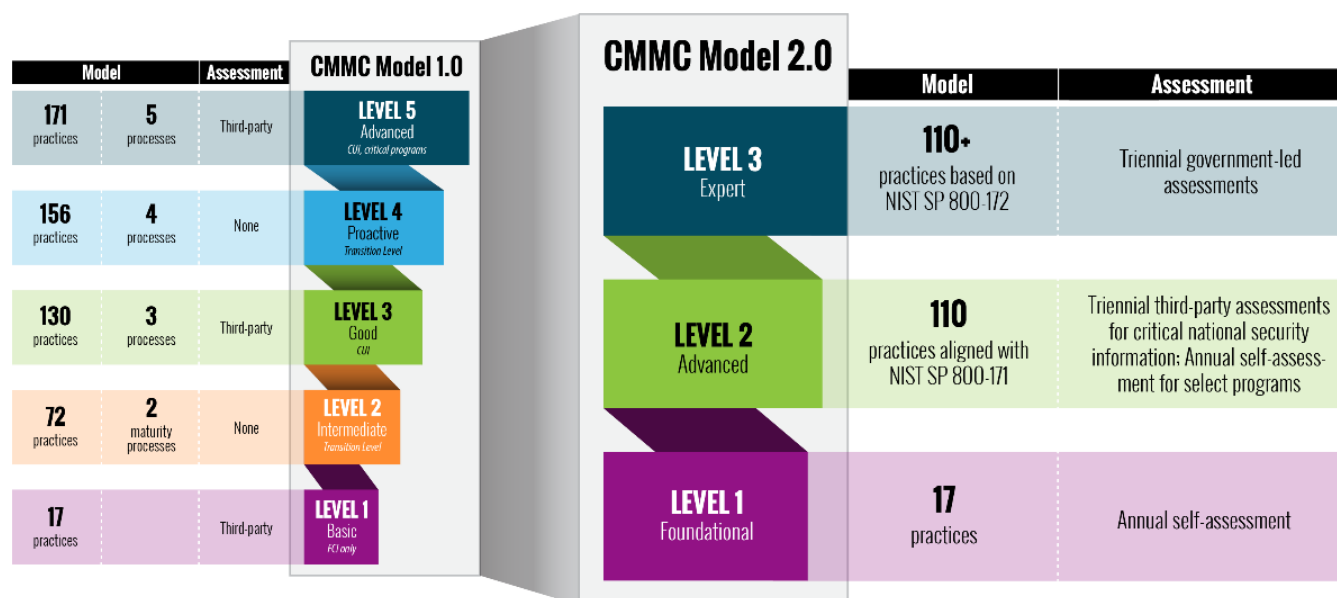
Implementation through Contracts: Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 72 Lecture hrs
Prerequisites: None
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD - EXAM
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

In 2019 the Department of Defense (DoD) announced the creation of the Cybersecurity Maturity Model Certification (CMMC) to govern the Defense Industrial Base (DIB). Cybersecurity Maturity Model Certification (CMMC) relies on self-assessments and third party assessors. The CMMC builds from NIST 800-171 but also includes controls from other cybersecurity frameworks. Where CMMC differs is in both the maturity model and the role of third-party assessors.



With the implementation of CMMC 2.0, the Department is introducing several key changes that build on and refine the original program

requirements. These are: Introduction to the CMMC, Understanding the Supply Chain, Protecting Sensitive Data, Understanding the CMMC Methodology, Building Business Better Through Cybersecurity, Network Diagrams and Scope

Learning Objectives: 72 hrs Lecture

Students will gain a general understanding of how to audit for CMMC Compliance.

On the surface, project management seems straightforward. However, at best, only 80% of projects end up being economically. Spirit of collaboration: Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification. Added flexibility and speed: Allows waivers to CMMC requirements under certain limited circumstances. On November 4, 2021 the Department of Defense unveiled an update to the Cybersecurity Maturity Model Certification framework – CMMC 2.0 – to streamline compliance, increase flexibility, and lower cost for manufacturers and IT providers. About CMMC 2.0

You will learn the 5 Step Guide to Understand:

- How to leverage your NIST 800-171 compliance efforts in preparation for CMMC 2.0
- The relationship between NIST 800-171 and CMMC 2.0
- What should your System Security Plan (SSP) include?
- What is a Plan of Action & Milestone (POAM) and how are they best used?
- How can I implement the requirements in a way that enables CMMC 2.0 validation?

Modules 72 hrs lecture

Lesson 1: 10 hrs Level I Introduction to Cybersecurity Maturity Model Certification / History and Players of CMMC

Lesson 2: 10 hrs Securing Sensitive Data

Lesson 3: 10 hrs CMMC Implementation Level 1-3

Lesson 4: 10 hrs Identity and Access Management

Lesson 5: 10 hrs CMMC Methodology

Lesson 6: 10 hrs CMMC Implementation Level 4

Lesson 8: 12 hrs CMMC Implementation Level 5 network diagrams and scope

DFARS Clause 252.204-7012 and NIST 800-171 cybersecurity requirements for primes and subcontractors are no longer voluntary and DoD audits, coupled with the Cybersecurity Maturity Model Certification (CMMC) version 2.0 will require all companies conducting business with the DoD to be certified by a third party. Audit ready, third party verified compliance with DFARS/NIST 800-171 involves much more than documentation and accomplishing it cost-effectively for your business requires an approach informed by the experience gained from hundreds of implementations. CyberSheath created this easy to follow 5 Step Guide informed by real world implementation experience to enable you to quickly and efficiently comply and pass any audit.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books -

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, CASP, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practical)
SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission <i>assurance</i> .
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA Qualified/ CMMC Cybersecurity Maturity Model Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
PMP® Project Manager Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementation Certification Class & Exam
Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

SCRUM MASTER Certification class



Our Certified ScrumMaster (CSM) workshop is a dynamic and engaging 72 hours of immersion into Scrum. We will learn Scrum by doing Scrum through experiential hands-on exercises, peer discussion, and self-learning. Your trainer will share practical experiences and proven techniques for successfully implementing Scrum in your workplace. You will become eligible to take the test upon completion of the course, and you will be fully prepared to pass with flying colors. Students to attend our workshops have a very high pass rate!

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, CASP, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practical)
<i>SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission assurance.</i>
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA Qualified/ CMMC Cybersecurity Maturity Model Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
PMP® Project Manager Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementation Certification Class & Exam
Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum

The Scrum Master Certification program will prepare you to master the most popular Agile project management methodology in industry. With this online SSGI Scrum Master certification, you will position yourself as an Agile expert who has the ability to develop and deliver quality products to customers.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 Lecture hrs
Prerequisites:	None
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
 Information Assurance (IA) Operational Engineer
 Information Assurance (IA) Security Officer
 Information Security Analyst/Administrator
 Information Security Manager or Specialist
 Information Systems Security Engineer
 Information Systems Security Manager
 Platform Specialist/ Security Administrator
 Security Analyst/ Security Control Assessor
 Security Engineer

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: The Scrum Master Certification course is intended for: project managers, team leads, management, Scrum team members, Six Sigma professionals and other business professionals interested in pursuing in-demand Scrum Master Certification.

Our Certified ScrumMaster (CSM) workshop is a dynamic and engaging 72 hours of immersion into Scrum. We will learn Scrum by doing Scrum through experiential hands-on exercises, peer discussion, and self-learning. Your trainer will share practical experiences and proven techniques for successfully implementing Scrum in your workplace. You will become eligible to take the test upon completion of the course, and you will be fully prepared to pass with flying colors. The program has been designed for professionals who are seeking a

management role or currently maintain a leadership position.

Learning Objectives: 72hrs Lecture

Students will gain a general understanding of how to create agile scrum.

Lesson 1: 12 hr Introduction and

Lesson 2: 12 hrs Frameworks & Methodologies

Lesson 3: 12 hrs Extreme Programming

Lesson 4: 12 hrs Lean

Lesson 5: 12 hrs Kanban

Lesson 6: 12 hrs Scrum Framework

Lessons 1-6 include:

2. Project Management Frameworks

3. Agile Methodology

4. Waterfall Methodology

5. Scrum Framework

6. How Scrum Works

7. Product Owner

8. Scrum Master

9. Development Team

10. User Stories

11. Product Backlog

12. Release Planning

13. Sprint Planning and Backlog

14. Estimation and Velocity

15. Technical Debt

16. Sprints

17. Daily Scrum

18. Sprint Review

19. Sprint Retrospective

20. Summary

As a Scrum Master, you will enable your Scrum Team to realize its full potential. Once you complete this program, you will acquire necessary skills to run your Scrum Team using the Agile/Scrum Framework. You will also learn about team roles, events, artifacts, rules, and how to apply them in your daily job. Through experiential hands-on exercises, peer discussions and self-learning techniques. There is a course workbook packed with bonus content and learning resources. Gain practical experiences and proven techniques for successfully Scrum out team.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

CIPP Certified Information Privacy Professional Certification Class* 



If you're pursuing your Certified Information Privacy Professional/United States (CIPP/US) certification, you'll need to study hard. That's The IAPP is the largest, global information privacy community for professionals who want to develop and advance their careers managing data privacy. The ANSI/ISO accredited certification programs for privacy professionals, including the CIPP/US.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 72 hr Lecture
Prerequisites: None
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and Practical Fail > 95% Attendance

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage an Contingency Planning program.

Practicing Privacy – Understanding Laws and Concepts -Show the world you know data privacy laws and regulations and how to apply them. Demonstrate your mastery of jurisdictional laws, regulations and enforcement models, plus legal requirements for handling and transferring data. * Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives:

42 hrs lecture/ 30 hrs labs:

Phase I 20 hrs lecture 5 hr labs

The CIPP/US curriculum provides an in-depth view of U.S. federal and state privacy statutes; detailed analysis of sectoral laws, civil and criminal enforcement; and an overview of the EU's General Data Protection Regulation and the California Consumer Privacy Act. The U.S. Privacy Environment
Data Use by Sector
Government and Court Access to Data
Workplace Privacy
State Privacy and Breach Notification Laws Course Lesson Plans

Phase II — Establishing Baseline 20 hrs Lecture 4 hr Labs

Our privacy training programs can help:

- Reduce risk of a data breach by making privacy a shared business objective
- Improve decision-making among employees who handle data
- Facilitate collaboration and communication across departments
- Demonstrate your commitment to data privacy and protection to customers, partners, regulators and staff

Phase II — Using the Tools and Creating an Effective Plan 15 hrs Lecture 8 hr Labs

This is the hands-on phase where students will apply contingency planning principles they have learned while using the tools we have surveyed to begin a contingency plan for their organization.

Self-assess—Each IAPP exam comes with two tools for determining how ready you are:

The [body of knowledge](#) is an outline of the information covered in the exam and represents the breadth of knowledge qualified candidates should possess on the topic. Use it to identify subjects you know well and those you should study more deeply.

The [exam blueprint](#) tells you how many questions to expect on each topic. Use it to map out a study strategy—allowing more time for topics with many questions, for example.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery



SU Q/ISO Qualified/ Chief Information Security Officer Certification Class*



If you're pursuing your Q/CISO Qualified/ Chief Information Security Officer Certification class, you'll need to study hard. This class is a comprehensive review of executive levels of information security & industry best practices merged with a comprehensive exam preparation for the Q/CISO exam. Bringing together all the components required for a C-Level positions, the CCISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital to leading a highly successful IS program.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 hr Lecture
Prerequisites:	None
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance + Labs and Practical Fail > 95% Attendance

Sample Job Title Contracting Officer (CO) Contracting Officer Technical Representative (COTR) Information Assurance (IA) Manager Information Assurance (IA) Program Manager Information Assurance (IA) Security Officer Information Security Program Manager Information Systems Security Manager (ISSM) Information Systems Security Officer (ISSO) Information Systems Security Operator

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage an Contingency Planning program.

How much does a Chief Information Security Officer make in the United States? The average Chief Information Security Officer salary in the United States is **\$230,204** as of April 26, 2022, but the range typically falls between **\$201,017** and **\$265,867**. Salary ranges can vary widely depending on many important factors, including education, certifications, additional skills, the number of years you have spent in your profession. With more online, real-time compensation data than any other website, Salary.com helps you determine your exact pay target.

Chief information security officers may have been best known for being thrown under the bus in the aftermath of a data breach. Now they're making a reputation for themselves as tech's most wanted, and highest paid. And rightfully so. Cybercrime Magazine recently caught up with [Jeremy King](#), president and founder at [Benchmark Executive Search](#), for a discussion about CISOs at the world's largest companies. It used to be that a cyberattack was a CISO's worst nightmare, and a sure-fire sign that a pink slip would follow. In 2020, it's a fact that [every company has been hacked](#) (or will be). Major corporations globally, with the help of law enforcement and private sector cyber defenders, have come to the realization that it's not the CISO's fault, and ousting one will only open up another can of worms — namely recruiting a replacement in a highly competitive market that is suffering through a [severe workforce shortage](#). Instead, CISOs are being heralded for their ability to plan for the worst, and to react calmly, legally, methodically, and swiftly, in response to cyber intrusions.

Learning Objectives:

50 hrs lecture/ 22 hrs labs:

10 hrs lecture 2 hrs labs

Domain 1: Governance (Policy, Legal, and Compliance)
Information Security Management Program
Defining an Information Security Governance Program
Regulatory and Legal Compliance
Risk Management

Management

Designing, deploying, and managing security controls
Understanding security controls types and objectives
Implementing control assurance frameworks
Understanding the audit management process

10 hrs Lecture 4 hr Labs

Domain 2: IS Management Controls and Auditing

10 hrs Lecture 6 hr Labs

Domain 3: Security Program Management & Operations
The role of the CISO

Information Security Projects
Integration of security requirements into other operational processes

10 hrs Lecture 3 hr Labs

Domain 4: Information Security Core Concepts

Access Controls
Physical Security
Disaster Recovery and Business Continuity Planning
Network Security
Threat and Vulnerability Management
Application Security
System Security
Encryption
Vulnerability Assessments and Penetration Testing

10 hrs Lecture 7 hr Labs

Domain 5: Strategic Planning, Finance, & Vendor Management

Security Strategic Planning
Alignment with business goals and risk tolerance
Security emerging trends
Key Performance Indicators (KPI)
Financial Planning
Development of business cases for security
Analyzing, forecasting, and developing a capital expense budget
Analyzing, forecasting, and developing an operating expense budget
Return on Investment (ROI) and cost-benefit analysis
Vendor management
Integrating security requirements into the contractual agreement and procurement process

****Note:** If required student information is not brought to class a "practice set" of information will be available. **Grades** -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. **Books** - No books are required for this course. However, you may want to supplement your preparation.

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CoM / non degree
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA CMMC Cybersecurity Maturity Model Certification class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum
PMP Project Manager Professional Certification Class & Exam
SU Q/ISO Qualified/ Chief Information Security Officer Certification Class & Exam

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery



Q/CSO Qualified/Cyber Security Officer Certification Class*



If you're pursuing your Q/CSO Qualified/ Cyber Security Officer Certification class, you'll need to study hard. This class is a comprehensive review of executive levels of information security & industry best practices merged with a comprehensive exam preparation for the Q/CISO exam. Bringing together all the components required for a C-Level positions, the CCISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital to leading a highly successful IS program.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 hr Lecture labs
Prerequisites:	None
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance + Labs and Practical Fail > 95% Attendance

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage a cyber risk program.

It used to be that a cyberattack was a CISO's worst nightmare, and a sure-fire sign that a pink slip would follow. In 2020, it's a fact that [every company has been hacked](#) (or will be). Major corporations globally, with the help of law enforcement and private sector cyber defenders, have come to the realization that it's not the CISO's fault, and ousting one will only open up another can of worms — namely recruiting a replacement in a highly competitive market that is suffering through a [severe workforce shortage](#). Instead, CISOs are being heralded for their ability to plan for the worst, and to react calmly, legally, methodically, and swiftly, in response to cyber intrusions.

Discussions: CISO Compensation Strategies for recruiting and retaining security leaders

Discussions Compensation -“Money, of course, is something that every CISO wants to hear about,” says King, a serial connector in the cybersecurity space, and a board member for several non-profit organizations related to our field.

Some Fortune 500 and Global 2000 corporations are giving their information security head honchos — oftentimes those with military backgrounds — [seven-figure pay packages](#). One company paid a [\\$3.89 million annual salary](#) to fill its CISO position. The Los Angeles Times reports that big companies are paying big bucks to its top cyber fighters. Another company paid a \$650,000 salary to fill its CISO role in 2012, and last year they bumped the pay up to [\\$2.5 million](#) for a new recruit in the same position. In 2016, annual CISO compensation in the largest U.S. cities was topping out at between [\\$380,000](#) and [\\$420,000](#). Cybersecurity Ventures has observed a gradual uptick of those figures, and we expect to see an increase in the number of organizations that will move the needle to the \$500,000 to \$1 million range over the next five years.

Discussion ROI: -If a \$1 billion company suffers a breach resulting in a \$700 million post-hack market valuation, then how much less is their CISO worth? What about a CISO who prevents such cyber catastrophes from happening in the first place — how much more is she or he worth?

These are the types of questions that C-suite executives and HR chiefs are well-advised to be answering for themselves. Over the next several years we'll be seeing more large organizations dishing out 7-figure pay packages to “A-players” who get A-results. Now even boardroom executives and shareholders are concerned with the possibility of a cyber intrusion that can lead to a plummeting stock price.

Discussion -where are you in the Org Chart -Cybersecurity Ventures forecasts that 100 percent of large corporations (Fortune 500, Global 2000) globally will have a CISO or equivalent position by the end of 2021 (up from 70 percent in 2018), although many of them will be unfilled due to a lack of experienced candidates. “We may see the CISO position mandated,” If that comes to pass, then the big concern is placing unqualified candidates into the positions. Every big company wants the best

CISO, but there's not enough of even the mediocre players to go around. There's also the issue of who should be taking attendance of the CISOs. There is no clear-cut place for security leaders on the org chart. Who they report to varies by company and it can be the chief compliance officer, the chief information officer (CIO), or the chief legal officer. While the idea of elevating the CISO role to new heights and rebranding them as chief risk officers or chief resilience officers (CROs) who report directly to the CEO is a nice one, the market doesn't seem ready for it.

Discussion Military Experience - "A lot of large enterprise CISOs come from the (U.S.) military. They have a longer track record of protecting data, or the new oil," says King, referring to a statement from IBM's former chairman and CEO Ginni Rometty: "We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true — even inevitable — then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."

A recent study by Cybersecurity Ventures calculated 13 percent of Fortune 500 CISOs served in the U.S. military. Altogether, 66 alumni of the United States Armed Forces currently serve as CISOs for the largest companies in the U.S.

If data becomes so important that it's the lifeblood of an organization, then companies will spare no expense in hiring the best person for the CISO job. Cybersecurity Ventures expects this will lead to an uptick in the number of security professionals with military backgrounds being placed as Fortune 500 and Global 2000 CISOs.

King notes that military personnel with substantial cybersecurity experience will see a 2X to as much as 5X bump in pay when they switch over to the private sector. But, it's not about the money for these women and men. "It's about the mission of protecting companies related to national security — there's a passion that never leaves them — it's in their blood," he says.

Discussion Turnover is rampant when it comes to chief information security officers at the largest companies in the U.S.

The average tenure for CISOs has been estimated at 18 to 26 months by various sources. By comparison, The average tenure for a CIO at the top 1,000 U.S. companies is 54 months, according to Korn Ferry. What explains the CISO merry-go-round at large enterprises? "The demand is so high and the job is so darn tough,". "The stress level is off the roof because a CISO can be right 99 out of 100 times, and a cybercriminal only has to be right once." And when the cybercriminal is right, it can be front-page news. Being in the news is not good for a CISO's career, or resume. At least not if they're captaining the ship when their organization suffers a high profile cyberattack or data breach. If you're a security leader who gets the budget, invests it, and still has the same persistent threats, then it's going to be a very stressful job. "When they (CISOs) quit for no apparent reason, it's usually personal,"

Recruiting -It's predicted that there will be 3.5 million unfilled cybersecurity jobs by 2027 —And the talent supply is so thin that deputy CISOs are being lured away by headhunters in order to fill the number one positions. CISOs also have their own teams to recruit and retain, which is perhaps their most difficult challenge of all. Whether you think CISOs are underappreciated or overpaid, the times are a-changin', and it's a good time to be one.

Learning Objectives:

10 hrs lecture 2 hrs labs

Domain 1: Governance (Policy, Legal, and Compliance), Information Security Management Program, Defining an Information Security Governance Program, Regulatory and Legal Compliance, Risk Management

10 hrs Lecture 4 hr Labs

Domain 2: Security Program Management & Operations, The role of the CISO, Information Security Projects, Integration of security requirements into other operational processes

10 hrs Lecture 6 hr Labs

Domain 3: Information Security Core Concepts, Access Controls, Physical Security, Disaster Recovery and Business Continuity Planning, Network Security, Threat and Vulnerability Management, Application Security, System Security, Encryption Vulnerability Assessments and Penetration Testing

10 hrs Lecture 3 hr Labs

Domain 4: IS Management Controls and Auditing Management, Designing, deploying, and managing security controls, Understanding security controls types and objectives, Implementing control assurance frameworks, Understanding the audit management process

10 hrs Lecture 7 hr Labs

Domain 5: Strategic Planning, Finance, & Vendor Management, Security Strategic Planning, Alignment with business goals and risk tolerance.



Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

TCP/IP and Key Features of Wireshark Course



TCP/IP and Key Features of Wireshark Course

One of the critical things for anyone who wants to learn either how to defend or even attack a network, is the ability to find and analyze system or network vulnerabilities. Wireshark is a free open-source packet analyzer that is the number one tool for network analysis, troubleshooting, software and communications protocol development, and related education in networking. When you are finished with this course, you will be able to perform network analysis for communications troubleshooting and forensics. Students will learn the contents & concepts of TCP/IP and Wireshark and how they should work together to provide true in-depth cyber security.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 21 hr Lecture 51 labs
Prerequisites: Understanding of TCP/IP Protocols.
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: register at Pearson Vue Testing Center
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Completion of Labs and Practical for CPoM Fail > 95% Attendance

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider/ Cybersecurity Officer
Enterprise Security Officer /Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect/ Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: SU CISSP Class handbook, labs, online quizzes SU resource CD's and 500 exam questions.

No tools for this class, students bring on their own laptop machines with [www.freepractice](http://www.freepractice.com) test.com and exam force pre installed.

Becoming a Wireshark Certified Network Analyst™ validates your ability to use Wireshark to perform network analysis for communications troubleshooting and forensics. Achieving Wireshark certification also demonstrates that you have experience troubleshooting, optimizing, and securing a network based on evidence found by analyzing traffic captured with Wireshark. It indicates your aptitude in TCP/IP network communications and is an ideal complement to CISSP, CCIE, CompTIA Network+, and other industry certifications.

Who Should Attend? Anyone interested in learning to troubleshoot and optimize TCP/IP networks and analyze network traffic with Wireshark, especially network engineers, information technology specialists, security analysts, and those preparing for the Wireshark Certified Network Analyst exam.

About Wireshark: Wireshark is a widely deployed open-source program that enables users to inspect hundreds of protocols and perform live capture and offline analysis. It has a broad set of features and runs on a variety of platforms, including Windows, OS X, and Linux. With more than 500,000 downloads per month, the Wireshark network analyzer is quickly becoming the industry standard.

Our Wireshark Training Optimize TCP/IP networks with Wireshark®. This hands-on, in-depth course provides the skills to isolate and fix network performance issues. Learn how Wireshark can solve your TCP/IP network problems by improving your ability to analyze network traffic. Our course emphasizes hands-on labs (27 in all) and real-world scenarios that will help you put theory into practice and give you the classroom experience to implement what you learn as soon as you get back to the office. Our Wireshark training class includes traffic capturing and filtering, 10 key troubleshooting steps, and case studies delivered by instructors with years of packet-level experience.

The certification exam is based on four, primary areas:

- Wireshark functionality
- TCP/IP network communications
- Network troubleshooting
- Network security

Required Exams -You'll take one action-packed course to prepare for the Wireshark Certified Network Analyst Exam. In addition, through a simple Wireshark experiment, you will see the TCP/IP packets and security systems in action that are serving your PC/laptop, that serves you.

Here's an overview of what we cover in our TCP/IP Prep Training Course:

Lesson 1. 2 hr lab 1 hr lecture

Introduction to Network Analysis and Wireshark
TCP/IP Analysis Checklist
Top Causes of Performance Problems
Get the Latest Version of Wireshark
Capturing Traffic
Opening Trace Files
Processing Packets
The Qt Interface Overview
Using Linked Panes
The Icon Toolbar
Master the Intelligent Scrollbar
The Changing Status Bar
Right-Click Functionality
General Analyst Resources
Your First Task When You Leave Class

2. 2 hr lab 1 hr lecture

Learn Capture Methods and Use Capture Filters
Analyze Switched Networks
Walk-Through a Sample SPAN Configuration
Analyze Full-Duplex Links with a Network TAP
Analyze Wireless Networks
USB Capture
Initial Analyzing Placement
Remote Capture Techniques
Available Capture Interfaces
Save Directly to Disk
Capture File Configurations
Limit Your Capture with Capture Filters
Examine Key Capture Filters

3. 2 hr lab 1 hr lecture

Customize for Efficiency: Configure Your Global Preferences
First Step: Create a Troubleshooting Profile
Customize the User Interface
Add Custom Columns for the Packet List Pane
Set Your Global Capture Preferences
Define Name Resolution Preferences
Configure Individual Protocol Preferences

4. 2 hr lab 1 hr lecture

Navigate Quickly and Focus Faster with Coloring Techniques
Move Around Quickly: Navigation Techniques
Find a Packet Based on Various Characteristics
Build Permanent Coloring Rules
Identify a Coloring Source
Use the Intelligent Scrollbar with Custom Coloring Rules
Apply Temporary Coloring
Mark Packets of Interest

5. 2 hr lab 1 hr lecture

Spot Network and Application Issues with Time Values and Summaries
Examine the Delta Time (End-of-Packet to End-of-Packet)
Set a Time Reference
Compare Timestamp Values
Compare Timestamps of Filtered Traffic
Enable and Use TCP Conversation Timestamps
Compare TCP Conversation Timestamp Values
Determine the Initial Round Trip Time (iRTT)
Troubleshooting Example Using Time
Analyze Delay Types

6. 2 hr lab 1 hr lecture

Create and Interpret Basic Trace File Statistics
Examine Trace File Summary Information
View Active Protocols
Graph Throughput to Spot Performance Problems Quickly
Locate the Most Active Conversations and Endpoints
Other Conversation Options
Graph the Traffic Flows for a More Complete View
Burst Statistics
Numerous Other Statistics are Available
Quick Overview of VoIP Traffic Analysis
SIP and RTP Analysis Overview
SIP Call Setup
Analyzing Call Setup with SIP
Session Bandwidth and RTP Port Definition

7. 4 hr lab 1 hr lecture

Focus on Traffic Using Display Filters
Display Filters
Filter on Conversations/Endpoints
Build Filters Based on Packets
Display Filter Syntax
Use Comparison Operators and Advanced Filters
Filter on Text Strings
Build Filters Based on Expressions
Watch for Common Display Filter Mistakes
Share Your Display Filters

8. 4 hr lab 1 hr lecture

TCP/IP Communications and Resolutions Overview
TCP/IP Functionality
When Everything Goes Right
The Multi-Step Resolution Process
Resolution Helped Build the Packet
Where Faults Can Occur
Typical Causes of Slow Performance

9. 4 hr lab 1 hr lecture

Analyze DNS Traffic

DNS Overview
DNS Packet Structure
DNS Queries
Filter on DNS Traffic
Analyze Normal/Problem DNS Traffic

10. 4 hr lab 1 hr lecture

Analyze ARP Traffic
ARP Overview
ARP Packet Structure
Filter on ARP Traffic
Analyze Normal/Problem ARP Traffic

11. 4 hr lab 1 hr lecture

Analyze IPv4 Traffic
IPv4 Overview
IPv4 Packet Structure
Analyze Broadcast/Multicast Traffic
Filter on IPv4 Traffic
IP Protocol Preferences
Analyze Normal/Problem IP Traffic

12. 4 hr lab 1 hr lecture

Analyze ICMP Traffic
ICMP Overview
ICMP Packet Structure
Filter on ICMP Traffic
Analyze Normal/Problem ICMP Traffic

13. 3 hr lab 1 hr lecture Analyze UDP Traffic

UDP Overview
Watch for Service Refusals
UDP Packet Structure
Filter on UDP Traffic
Follow UDP Streams to Reassemble Data
Analyze Normal/Problem UDP Traffic

14. 4 hr lab 1 hr lecture

Analyze TCP Protocol
TCP Overview
The TCP Connection Process
TCP Handshake Problem
Watch Service Refusals
TCP Packet Structure
The TCP Sequencing/Acknowledgment Process
Packet Loss Detection in Wireshark
Fast Recovery/Fast Retransmission Detection in Wireshark
Retransmission Detection in Wireshark
Out-of-Order Segment Detection in Wireshark
Selective Acknowledgement (SACK)
Window Scaling
Window Size Issue: Receive Buffer Problem

Window Size Issue: Unequal Window Size Beliefs
TCP Sliding Window Overview
Troubleshoot TCP Quickly with Expert Info
Filter on TCP Traffic and TCP Problems
Properly Set TCP Preferences
Follow TCP Streams to Reassemble Data 16. Examine
Advanced Trace File Statistics
Build Advanced IO Graphs
Graph Round Trip Times
Graph TCP Throughput
Find Problems Using TCP Time-Sequence Graphs

15. 2 hr lab 1 hr lecture

Graph Traffic Characteristics
Advanced I/O Graphing
Graph Round Trip Times
Graph TCP Throughput
Find Problems Using TCP Time Sequence Graphs

16. 4 hr lab 1 hr lecture

Analyze HTTP Traffic
HTTP Overview
HTTP Packet Structure
Filter on HTTP Traffic
Reassembling HTTP Objects
HTTP Statistics
HTTP Response Time
Overview of HTTP/2
HTTP/2 Analysis Fundamentals
HTTP /2 Frame Format
Analyze Normal/Problem HTTP Traffic

17. 4 hr lab 1 hr lecture

Analyze TLS-Encrypted Traffic (HTTPS)
Analyze HTTPS Traffic
Encrypted Alerts
Decryption Steps
Filter on SSL


18. 1 hr lab 1 hr lecture Review Your 10 Key Troubleshooting Steps

Baseline "NormalTraffic"
Use Color
Look Who's Talking: Examine Conversations and Endpoints
Focus by Filtering
Create Basic IO Graphs
Examine Delta Time Values
Examine the Expert System
Follow the Streams
Graph Bandwidth Use, Round Trip Time, and TCP
Time/Sequence Information
Watch Refusals and Redirections

All of our hybrid instructor-led courses are taught by our expert instructors and fulfill the required 72 contact hours of cyber education training. Mock TCP/IP final project. Peer review and instructor-led review

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery CPoM / non degree-	
Q/SA® Qualified/ Security Analyst Penetration Tester Certification Class & Exam	
Q/PTL® Qualified/ Penetration Tester License workshop	
Q/EH® Qualified/ Ethical Hacker Certification Class & exam	
Q/ND® Qualified/ Network Defender Certification Class & Exam	
Q/FE® Qualified/ Forensic Expert Certification Class & Exam	
SU CISSP® Certified Information Security Systems Professional Class & Exam	
SU Security+® CompTIA Certification Class & Exam	
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam	
Linux/UNIX® Security Certification Class & Exam	
Cloud Computing Security Knowledge Certification (CCSK & Plus) Class & Exam	
Q/PTL® Qualified/ Penetration Tester License Practical required to graduate	
Q/ND® Qualified/ Network Defender Certification Practical required to graduate	
Q/FE® Qualified/ Forensic Expert Certification Class Practical required to graduate	

Q/WLANPD Qualified/ Wireless Local Area Network Planning and Design Practitioner

This class aims to provide students with fundamental knowledge into core concepts of the latest and next generation mobile and wireless networks. Throughout the course, students will be exposed to theoretical and practical aspects regarding the architecture and applications of Cellular, LTE, and 4G/5G systems. In addition, basic concepts of Wireless LAN (WLAN), Mobile Peer-to-Peer (MP2P), wireless sensor networks (WSN) and emerging opportunistically connected mobile/vehicular networks (MANET and VANET), will be explored.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	53 hr Lecture 19 hr labs
Prerequisites:	TCP/IP
Credits:	50 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass Attendance, Completion of Labs & quizzes Fail > 95% Attendance

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider
Cybersecurity Officer/Enterprise Security Officer
Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect /Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer.

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final Exam - passing the final exam is a requirement for graduation.

Introduction

The Q/WLANPD Wireless LAN Design course consists of instructor-led training applicable to the design of wireless LANs using the latest technologies including 802.11n and 802.11ac. The course goes in-depth into the design process and provides attendees with the knowledge needed to plan, deploy and test modern 802.11-based networks. It also prepares students for the Q/WLANPD examination. Students who complete the course will acquire the necessary skills for preparing, planning performing and documenting site surveys and wireless LAN design procedures.

53 hrs lab/ 19 hrs lecture

Course Outline- The following list contains the materials covered in the lecture portion of the course.
WLAN Design Overview

Lesson 1 2 hr labs 3 lecture

- Importance of good design
- Impact of bad design
- Design process
- Design skills
- Design toolkit
- Pre-planning
- Customer interaction
- Requirements gathering

- Government
- Healthcare
- Hospitality
- Education
- Retail
- Public hotspots
- Transportation
- Mobile offices

Lesson 2 2 hr labs 3 lecture

- Discovering existing systems
- Documenting the environment
- Defining constraints
- Creating documentation
- Client device types
- Application types
- Application-specific design
- High density design issues
- Standard corporate networks

Lesson 4 6 hr labs 1 lecture

- Outdoor and mesh
- Remote networks and branch offices
- Last-mile/ISP and bridging
- Defining vendor issues
- Operational planes
- Design models
- Understanding architecture differences
- RF spectrum
- RF behaviors
- Modulation and coding schemes
- RF accessories
- Throughput factors
- Antennas

Lesson 3 2 hr labs 1 lecture

- Industry-specific designs

802.11n and antennas
Choosing APs
Powering APs

Lesson 5 7 hr labs 1 lecture

Site survey tools
Site survey preparation
Predictive site surveys
Manual site surveys
Site survey principles and processes
Quality of Service (QoS) overview
QoS application points
Roaming support

Lesson 6 5 hr labs 1 lecture

Bad security
Authentication solutions
Encryption solutions
Security best practices
Intrusion prevention
Network health status
Troubleshooting and validation process
Troubleshooting and validation tools
Common problems

Lesson 7 6 hr labs 2 lecture

Requirements Analysis
Designing for Clients and Applications
Designing for Industry
Vendor Selection Processes

Lesson 8 6 hr labs 2 lecture

Radio Frequency Planning
WLAN Hardware Selection

Lesson 9 6 hr labs 2 lecture

Site Surveys
Designing for QoS
Designing for Security
Installation Testing, Validation and Troubleshooting
Design Troubleshooting

Lesson 1 6 hr labs 2 lecture

Case Studies are for groups to explore concepts learned in the lecture materials. Potential case studies include:

- Designing for future capacity
- Designing in a moderate interference environment
- Designing multiple SSID networks

Lesson 11 7 hr labs 1 lecture Dynamic Hands-on Lab

Exercises

Trainers may include hands-on lab time using any or all of the following tools:

- Spectrum analyzer
- Protocol analyzer
- Site survey software
- Diagramming software
- Various wireless adapters and antennas
- Various wireless AP

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

SU Q/WP® Qualified Wireless Professional Certificate of Mastery CoM non degree (4 Q/WP® + Security+®, CASP®)
Q/WAD® Qualified/ Wireless Analyst & Defender Class & Exam
Q/ WP® Qualified/ Wireless Professional Certification Class & Exam
Q/WSP® Qualified/ Wireless Security Professional Certification Class & Exam
Q/WAD® Qualified/ Wireless Analyst & Defender Practicum
Q/WP®/ Q/WSP® Bootcamp Class (CWNA™/ CWSP™ Qualified Wireless / Qualified Wireless Security Professional Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
PMP Project Manager Professional Certification & Exam
Q/WLANPD Qualified/ Wireless Local Area Network Planning & Design & Exam
Q/WLANPD Qualified/ Wireless Local Area Network Planning Design Practicum
Q/WNST Qualified/ Wireless Network and IoT Security Testing & Exam
Q/WDNO Qualified/ Wireless Deceptive Network Optimization & Exam

Q/WP Qualified/ Wireless Professional Certificate Program of Mastery

Q/WDNO Qualified/ Wireless Deceptive Network Optimization Class

Getting wireless certified with Security University shows your Qualified.

The IDC estimates that there would be 152,200 IoT devices connected every minute by 2025, indicating that there would be about 80 billion IoT devices connected annually. While IoT devices have numerous benefits and are immensely helpful for different purposes, they also pose as attractive vulnerabilities for cybercriminals. Be it insecure passwords, networks, ecosystem interfaces or any other vulnerability and weakness, once an IoT device is compromised, it can lead to major losses for any organization, and not just financially.

Questions & Quizzes /Full practice test

Class Fee: \$3,990

Time: 72 hrs

Learning Level: Intermediate

Contact Hours: 51 hr Lecture 21 hr labs

Prerequisites: Understanding of TCP/IP Protocols

Credits: 72 CPE / 3 CEU

Method of Delivery: Residential (100% face-to-face) or Hybrid

Instructor: TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab

Grading: Pass = Attendance, Labs and quizzes Fail > 95% Attendance

Sample Job Title

Network security engineers

Cybersecurity analysts

Network and security analysts

Full stack engineers

Information system security architects

Network security administrators

Product security analysts

IT security analysts

Security test engineers

Application security testers/analysts

Security delivery analysts, etc.

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

This class is about security testing and attack surface management to teach wireless Penetration Testing using a penetration testing and vulnerability management methodology. Its experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces, historically testing over 1 million assets to find 4 million unique vulnerabilities. This IoT security class also incorporates hands-on practical exercises for a thorough experiential and practical learning experience to the participants.

The course aims to cover the following:

Introduction to Wireless IoT security

Introduction to basic IoT

Terminology and initiatives

Device security and gateway security

Communication protocols

IoT cloud platforms and their security

IoT ecosystem and penetration testing approaches

Attack and fault trees

Threat modelling IoT systems, applications and hardware

IoT testing and security automation

IoT hacking

This course is highly recommended for current and aspiring:

IoT Exam Prep Daily Schedule 6 hr lecture 2 hr labs each day

- **Lesson 1** - Domain 4: IoT testing and security automation
- **Lesson 2** - Domain 1: Introduction to Wireless IoT security
- **Lesson 3** - Domain 2: Attack and fault tree
- **Lesson 4** - Domain 3: IoT ecosystem and penetration testing approaches
- **Lesson 5** Domain 5: IoT hacking
- **Lesson 6** Domain 6: Privacy and Security

- **Lesson 7** Domain 7: IoT Pen Testing

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Q/WP Qualified/ Wireless Professional Certificate Program of Mastery

Q/WNST Qualified/ Wireless Network and IoT Security Testing Class

Getting wireless certified with Security University shows your Qualified.

The IDC estimates that there would be 152,200 IoT devices connected every minute by 2025, indicating that there would be about 80 billion IoT devices connected annually. While IoT devices have numerous benefits and are immensely helpful for different purposes, they also pose as attractive vulnerabilities for cybercriminals. Be it insecure passwords, networks, ecosystem interfaces or any other vulnerability and weakness, once an IoT device is compromised, it can lead to major losses for any organization, and not just financially.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Intermediate
Contact Hours: 51 hr Lecture 21 hr labs
Prerequisites: Understanding of TCP/IP Protocol
Credits: 50 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance, Labs and quizzes Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Title

*Network security engineers
Cybersecurity analysts
Network and security analysts
Full stack engineers
Information system security architects
Network security administrators
Product security analysts
IT security analysts
Security test engineers
Application security testers/analysts
Security delivery analysts, etc.*

To the leader in enterprise penetration testing and attack surface management, today announced the launch of its IoT penetration testing services, which will be added to its existing suite of penetration, adversary simulation, and attack surface management capabilities. With the stark growth of IoT adoption over the past few years, pentesting is now a critical asset for companies to understand and assess the overall strength and accountability of their internet-connected systems against sophisticated and targeted cyber attacks.

This class teaches the following capabilities:

ATM Penetration Testing. Identify the security issues and common vulnerabilities on relevant ATM systems and provide actionable recommendations for improving the overall security posture. Learn more about ATM pentesting.

Automotive Penetration Testing. Identify security issues on relevant vehicles and provide recommendations to improve the current systems – at any stage of automotive development. Learn more about automotive pentesting.

Medical Device Penetration Testing. Through a combination of threat modeling and penetration testing, determine possible medical device security risks and identify whether devices meet or exceed the current standards and recommendations by the FDA Premarket Cybersecurity Guidelines. Learn more about medical device pentesting.

Operational Technology (OT) Architecture and Security Review. Identify industrial control system (ICS) vulnerabilities with a focus on the OT processes in a Defense in Depth strategy. Students will investigate the configuration and architecture of the systems and help address issues with asset inventory, network configuration, and segmentation. Learn more about OT architecture and security review. Embedded Penetration Testing. Identify embedded system vulnerabilities in a multitiered penetration test across multiple disciplines. Look for security gaps at all stages of embedded development that may affect each layer of the device. Learn more about embedded pentesting.

“IoT has become part of our daily lives, but these devices and systems are often overlooked from a security perspective. Tapping into our innovation-driven culture and our best-in-class technologies. This pentesting testing class is uniquely qualified to find and help fix the most critical security gaps in these systems,” to future-proofing IoT security worldwide.” To keep up with the growth of IoT and assist with the complexity in this space. There is currently a gap in the market to effectively monitor and assess the risks of these devices. This IoT security class also incorporates hands-on practical exercises for a thorough experiential and practical learning experience to the participants.

The course aims to cover the following:

Red Team Operations & Attack Surface Management

Simulated attacks through a red team engagement enhance your information security program. Red team operations put your organization's security controls, security policies, incident response, and cybersecurity training to the test. Attack Surface Management detects known, unknown, and potentially vulnerable public-facing assets, as well as changes to your attack surface that may introduce risk. How? Through a combination of powerful Attack Surface Management (ASM) technology platform, penetration testing experts, and 20+ years of pentesting expertise.

This course is highly recommended for system admins and pen testers:

Schedule 7.2 hr lecture & labs each lesson

- **Lesson 1** - Red Team simulations & Operation Models
- **Lesson 2**- Assumed breach | Black box testing
- **Lesson 3** – Identify and respond to threats RED TEAM OPS
- **Lesson 4** Attack Surface Management
- **Lesson 5** Identify and protect the unknown
- **Lesson 6** Continuous Penetration Testing
- **Lesson 7** Manual Exposure Triaging
- **Lesson 8** Asset Discovery with Attack Surface Monitoring
- **Lesson 9** Asset Intelligence
- **Lesson 10** High Risk Port Discovery

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practical in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

This fast-paced, 95% hands-on LABS class will teach you how to secure networks and protect a system from compromise. You'll learn how the attacks work and how to use hard-core hardening to defeat the bulk of them. You'll learn how to take your machines to a state of minimum necessary risk.

This hands-on class teaches you how to tighten all major aspects of the operating system for security, balancing this with the purpose of the system and the needs of your organization. You'll learn how to DEFEND, USING DNS, PKI and kernel and operating system parameters, deactivate components, and tighten the components that remain. You'll examine major server applications wireless and IDS tightening. Along the way, you'll understand how external and internal attackers use privilege escalation and how you can lessen their odds of gaining root. You'll also learn to apply key security concepts, from defense-in-depth, continuous monitoring, least privilege to risk evaluation, to determine what actions you should take and in what order of priority.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	72 Lecture hrs
Prerequisites:	None
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance +Lab & quizzes Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend:

System administrators, security administrators, security auditors. unix admins. Anyone who has a vested interest in keeping their systems from being compromised. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions. While others are welcome, complete lack of familiarity is too great a burden to overcome in a three day class.

*Text Materials: labs, SU Pen Testing & Linux Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 36M Ram, 350 Tdrives, running MS OS, linux, and VMWare Workstation*

Tools for class

Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Ncat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyprio tool, 'Curl'

What You Will Learn 5 hrs Lecture 35 hr Labs:

The mission of the CND class is to train the network defender on basic to advanced security concepts and techniques used to detect, recognize, identify, and mitigate network threats and vulnerabilities and how to report them.

Lesson 1 12 hrs lecture & Labs

1) Core Skills summary (like the Q/EH)

- Privilege Escalation
- Reconnaissance
- Scanning
- Enumeration

- Sniffing
- Password Cracking Techniques
- System Hacking
- Buffer Overflows
- Social Engineering
- SQL Injection
- Hacking Linux
- Virus Worms Trojans Rootkits
- IDS, Firewalls and Honeypots
- Denial of Service
- Cryptography
- Session Hijacking
- Web Application Vulnerabilities
- Hacking Web Servers
- Penetration Testing Methods
- DLL/Code injection
- ARP Poisoning
- Log Tampering
- Data Hiding and Evasion
- Alternate Data Streams
- Locked directories
- Special Shell Folder Locations
- Steganography
- Find/Grep Utilities
- Basic SQL
- File comparison
- Push/Pull logging
- Network mirroring /Port Mirroring/SPAN
- UNIX Epoch Time
- Network Traffic Analysis

2) Linux and Unix fundamentals

- Network Traffic Analysis
- Examine how to mitigate or eliminate general problems that apply to all
- Unix-like operating systems,
- vulnerabilities in the password
- authentication system,
- file system,
- virtual memory system,
- applications that commonly run on Linux and Unix.
- configuration guidance and practical, real-world examples,
- tips, and tricks.

Lesson 2 12 hrs lecture & Labs

Data Analysis tools and Fundamentals

IS.2. Learn how to create, edit, and manage changes to network access control lists on firewalls and IPS.

IS.3. Learn Anti-Virus or Audit/Remediation administration including installation, configuration, maintenance, and backup/restore.

- Data Correlation (Data Fusion)
- Logging Architectures and Data Sources
- IP Anomalies and Bogon Routing

- TCP Anomalies
- UDP Anomalie
- Data Correlation (Data Fusion)
- Logging Architectures and Data Sources
- IP , TCP, UDP, ICMP, HTTP Anomalies
- Reverse Shells
- Directory Traversals
- Unicode Exploits
- Command Injection
- IIS Web Service Logging Locations
- HTTP.sys Error Logging
- FTP Bouncing
- Active FTP
- Passive FTP
- SMTP & Unsolicited Mail
- SNMP ver1, 2 or 3?
- RDP Hijacking
- SSL/TLS and SSH Hijacking, with a twist of DNS and ARP Poisoning
- Back up and restore

Lesson 3 12 hrs lecture & Labs

Intrusion Analysis

IS.5. Learn how to manage and administer the updating of rules and signatures for specialized CND applications. (IDS/IPS, anti-virus, and content blacklists)

IS.6. Learn how to identify potential CND implementation conflicts (e.g., tool/signature testing and optimization).

IS.7. Learn how to build and administer CND test bed to evaluate new CND applications, rules/signatures, access controls, and configurations of CND-SP managed platforms.

A.2. How to analyze network alerts skills

A.3. How to validate network alerts

A.4. How to analyze log files from a variety of sources (host logs, network traffic logs, firewall logs, and IDS logs) or SIM

A.5. Learn how to identify anomalous activity and analyze network traffic and how they threaten network resources.

A.7. Learn to write signatures for CND network tools in response to new or observed threats.

A.8. Learn how to do event correlation from a variety of sources to gain situational awareness and determine the effectiveness of an observed attack.

A.9. Notify CND managers, CND incident responders, and other CND-SP team members of suspected CND incidents and articulate the event's history, status, and potential impact for further action.

- RDP Hijacking
- Analyze network alerts
- Validate network alerts
- Analyze log files from host logs, network traffic logs, IDS logs
- Identify anomalous activity and analyze network traffic & how they threaten resources
- Write signatures for network tools in response to new or observed threats
- Event correlation from a variety of sources to determine the effectiveness of the attack.

Lesson 4 12 hrs lecture & Labs

Basic Forensic tools and Fundamentals

IR.2. You will understand how to collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) to mitigate potential CND incidents.

IR.3. You will learn how perform initial, forensically sound collection of images to discern mitigation/ remediation.

IR.4. Learn how to coordinate with and provide expert technical support to resolve CND incidents.

IR.5. You will learn how to track and document CND incidents from initial detection through final resolution.

IR.6. You will learn the step by step process of CND incident triage to determine scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation.

IR.7. You will learn how to correlate incident data and perform CND trend analysis and reporting.

IR.8. You will coordinate with intelligence analysts to correlate threat assessment data.

IR.9. You will learn how to serve as technical experts to law enforcement for incident details & expert testimony

IR.10. You will perform real-time CND Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRT).

IR.11. You will learn how to maintain deployable CND toolkit (e.g., specialized CND software/hardware) to support IRT missions.

IR.12. You will learn who to write and publish CND guidance and reports on incident findings to appropriate constituencies.

- Data Breach Cases &, Intrusion Analysis
- U.S. Laws Investigators you should know
- Evidence Acquisition/Analysis/Preservation Laws and Guidelines
- Forensic Collection of Images
- Forensic Reports and Testimony
- Step by Step Forensics Methodology
- File System Essentials
- Evidence Integrity and Chain of Custody
- Advanced Forensic Evidence Acquisition and Imaging
- File System Timeline Analysis
- Key Forensic Acquisition/Analysis & Correlation Concepts
- Volatile Evidence Gathering and Analysis
- Forensic Analysis Key Methods
- Key Windows File System Analysis Concepts
- File System and Data Layer Examination
- Metadata and File Name Layer Examination
- Windows FAT File System Examination
- Windows NTFS File System Examination
- Linux/Unix File System Examination
- Image File Conversion (E01, Raw, AFF)
- Windows System Restore and Shadow Volume Copy Exploitation
- File Sorting and Hash Comparisons
- Live Response and Volatile Evidence Collection
- Windows Registry Analysis
- Windows Internal File Metadata
- Application Footprinting and Software Forensics
- Automated GUI Based Forensic Toolkits

Lesson 5 12 hrs lecture & Labs

Incident handling

AC.2. You will learn applicable CND policies, regulations, and compliance documents specifically related to CND auditing.

AC.3. You will learn how to do step by step CND vulnerability assessments.

AC.4. You will learn how to do step by step CND risk assessments.

AC.5. You will learn how to conduct authorized penetration testing of network assets.

AC.6. You will learn how to analyze site CND policies and configurations and evaluate compliance with regulations and enclave directives.

AC.7. You will learn how to prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.

- The step-by-step penetration tester assessment process and methodology workshops
- The latest cyber attack vectors defenses to stop them
- Proactive and reactive defenses of a computer attack with 12 live scenarios
- Scanning for, exploiting, and defending systems
- Strategies and tools for detecting each type of attack
- Attacks and defenses for Windows, Unix, switches, routers and other systems
- Application-level vulnerabilities, attacks, and defenses
- Developing an incident handling process and preparing a team for battle
- Legal issues in incident handling
- Recovering from computer attacks and restoring systems for business

Lesson 6 12 hrs lecture & Labs

Current Trends & developments / Qualified/ Network Defense Exercise QNDX

Scenario #1—Attacks with no perimeter to soft systems

Scenario #2—Defense with no perimeter and soft systems

Scenario #3—Attacks with no perimeter to hard systems

Scenario #4—Defense with no perimeter and hard systems

Scenario #5—Attacks through perimeter to hard systems

Scenario #6—Defense with perimeter and hard systems

Scenario #7—DOS attacks on hardened network

Scenario #8—DOS defenses with hardened network

Scenario #9—Concurrent attack/defense with no perimeter

Scenario #10—Concurrent attack/defense with perimeter

Scenario #11—Concurrent DOS attack/defense

Scenario #12—Ad Hoc: This scenario can be tailor-made to fit any specific learning objectives.

Each class builds networks with a secure channel (i.e., VPN) setup, start/stop times and dates, roles (attacker or defender), ROE, and learning objectives that will be drafted and published with the described pre-defined Q/ISP Project scenarios and SOW (Scope of Work) establish parameters of scenarios. These twelve scenarios and SOW will serve as the necessary administrative coordination between QNDX participants. Though the exact content of these scenario descriptions and SOW will not be finalized until approved, the generalized contents and descriptions follow.

The SOW will contain four main elements.

- 1) A statement regarding the intent of QNDX participation.
- 2) Elaboration regarding the mandatory implementation of a secure VPN tunnel between the participating networks.
- 3) Delineation of Qualified -exercise ethical conduct and ROE.
- 4) A statement indicating that each Major has notified their local IT authorities regarding the exercise, and that each side has taken measures to ensure that their SOW network activities will not adversely hinder routine network operations.



CySA+ Cybersecurity Analyst+ Certification Class & Exam

As attackers have learned to evade traditional signature-based solutions, an analytics-based approach has become extremely important. CompTIA CySA+ certification applies behavioral analytics to the IT security market to improve the overall state of IT security. Analytics have been successfully integrated into the business intelligence, retail and financial services industries for decades. Now they are also applied to IT security. Security analytics greatly improves threat visibility across a broad attack surface by focusing on network behavior, including an organization's interior network. Threats are better detected using analytics.

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr Lecture 32 hr labs
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance + labs and Practical Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: SU Cardwell Q/SA -CySA handbook, labs, online quizzes SU resource CD's and 500 exam questions. *No tools for this class, students bring on their own laptop machines with www.freepractice.com test.com and exam force pre installed. CySA+ addresses the increased diversity of knowledge, skills and abilities (KSAs) required of today's security analysts and validates what is currently necessary to perform effectively on the job. CySA+ certification reflects the KSAs needed to analyze the state of security within modern IT environments, including:*

Lesson	Description	Matching CySA+ Objectives (Samples)
6hr lecture/ Labs 1. Cyber Defense Analyst PR-DA-001	Uses data collected from a variety of cyber- defense tools (e.g., intrusion detection system (IDS) alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.	1.1 — Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes 1.2 — Given a scenario, analyze the results of a network reconnaissance 1.3 — Given a network-based threat, implement or recommend the appropriate response and countermeasure

6 hr Lecture/ Lab 2. Cyber Defense Infrastructure Support Specialist PR-INF-001	Tests, implements, deploys, maintains and administers the infrastructure hardware and software.	1.4 — Explain the purpose of practices used to secure a corporate environment 2.3 — Compare and contrast common vulnerabilities found in the following targets within an organization 4.3 — Given a scenario, review security architecture and make recommendations to implement compensating controls
10 hr Lecture/ Lab 3. Cyber Defense Incident Responder PR-IR-001	Investigates, analyzes and responds to cyber-incidents within the network environment or enclave.	3.1 — Given a scenario, distinguish threat data or behavior to determine the impact of an incident 3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation 3.3 — Explain the importance of communication during the incident response process 3.4 — Given a scenario, analyze common symptoms to select the best course of action to support incident response 3.5 — Summarize the incident recovery and post-incident response process
10 hr Lecture/ Lab 4. Vulnerability Assessment Analyst PR-VA-001	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy or local policy. Measures effectiveness of defense-in- depth architecture against known vulnerabilities.	2.1 — Given a scenario, implement an information security vulnerability management process 2.2 — Given a scenario, analyze the output resulting from a vulnerability scan 2.3 — Compare and contrast common vulnerabilities found in the following targets within an organization
10hr Lecture/ Lab 5. Warning Analyst AN-TA-001	Develops unique cyber-indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes and disseminates cyber-warning assessments.	1.1 — Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes 1.2 — Given a scenario, analyze the results of a network reconnaissance 3.3 — Explain the importance of communication during the incident response process
10hr Lecture/ Labs 6. Cyber Crime Investigator IN-CI-001	Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.	3.1 — Given a scenario, distinguish threat data or behavior to determine the impact of an incident 3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation 3.5 — Summarize the incident recovery and post-incident response process 4.1 — Explain the relationship between frameworks, common policies, controls and procedures 4.5 — Compare and contrast the

		general purpose and reasons for using various cybersecurity tools and technologies
10hr Lecture/ Labs 7. Forensics Analyst IN-FO-001	Conducts deep-dive investigations on computer- based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber-intrusion incidents.	<p>1.1 — Given a scenario, apply ironmental reconnaissance techniques using appropriate tools and processes</p> <p>3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation</p> <p>4.5 — Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies</p>
12hr Lecture/ Lecture 8. Cyber Defense Forensics Analyst IN-FO-002	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.	<p>2.2 — Given a scenario, analyze the output resulting from a vulnerability scan</p> <p>3.1 — Given a scenario, distinguish threat data or behavior to determine the impact of an incident</p> <p>3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation</p> <p>3.4 — Given a scenario, analyze common symptoms to select the best course of action to support incident response</p>

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery



Forensic Expert Practicum

How to detect the crime, track the criminal, and assemble the evidence practicum.

Finally, a tactical Forensics practicum that provides everything you need to know to be a Qualified/ Forensic Expert with an with a **90 day practical to validate & prove your forensic skills**. Learn everything relating to computer forensics & digital forensics rights. From how to establish a proper chain of custody that is admissible in a court of law to recovering files from intentionally damaged media.

Cyber crime is out performing traditional crime. Qualified/ Forensics Experts are needed by today's companies to determine the root cause of a hacker attack, collect evidence legally admissible in court, and protect corporate assets and reputation. High-profile cases of corporate malfeasance have elevated electronic evidence discovery as indispensable to your company. A recent law review claims: A lawyer or legal team without a Forensic Expert on their case is sure to lose in today's courtroom!

Learn more about [SU's Federation of Q/FE's Qualified/ Forensic Experts & Examiners](#)

Class Fee:	\$3,990
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	72 hr labs
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance and Practical Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: SU Course materials Forensic handbook, labs, online quizzes SU resource CD's and 500 exam questions. No tools for this class, students bring on their own laptop machines with www.freepractice.com test.com and exam force pre installed. CySA+ addresses the increased diversity of knowledge, skills and abilities (KSAs) required of today's security analysts and validates what is currently necessary to perform effectively on the job. CySA+ certification reflects the KSAs needed to analyze the state of security within modern IT environments, including

Forensic Expert Practicum

120 day practicum to analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Digital Forensics Practicum requirement tasks

- T0027: Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
- T0036: Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
- T0048: Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not

limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.

- T0049: Decrypt seized data using technical means.
- T0075: Provide technical summary of findings in accordance with established reporting procedures.
- T0087: Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.
- T0103: Examine recovered data for information of relevance to the issue at hand.
- T0113: Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
- T0165: Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.
- T0167: Perform file signature analysis.
- T0168: Perform hash comparison against established database.
- T0172: Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).
- T0173: Perform timeline analysis.
- T0175: Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
- T0179: Perform static media analysis.
- T0182: Perform tier 1, 2, and 3 malware analysis.
- T0190: Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).
- T0212: Provide technical assistance on digital evidence matters to appropriate personnel.
- T0216: Recognize and accurately report forensic artifacts indicative of a particular operating system.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.
- T0241: Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
- T0253: Conduct cursory binary analysis.
- T0279: Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
- T0285: Perform virus scanning on digital media.
- T0286: Perform file system forensic analysis.
- T0287: Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).
- T0288: Perform static malware analysis.
- T0289: Utilize deployable forensics toolkit to support operations as necessary.
- T0312: Coordinate with intelligence analysts to correlate threat assessment data.
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0397: Perform Windows registry analysis.
- T0398: Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.
- T0399: Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.
- T0400: Correlate incident data and perform cyber defense reporting.
- T0401: Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.
- T0432: Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
- T0532: Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.
- T0546: Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.

Skills

- S0032: Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.
- S0047: Skill in preserving evidence integrity according to standard operating procedures or national standards.
- S0062: Skill in analyzing memory dumps to extract information.
- S0065: Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
- S0067: Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).
- S0068: Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.

- S0069: Skill in setting up a forensic workstation.
- S0071: Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).
- S0073: Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
- S0074: Skill in physically disassembling PCs.
- S0075: Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).
- S0087: Skill in deep analysis of captured malicious code (e.g., malware forensics).
- S0088: Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).
- S0089: Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
- S0090: Skill in analyzing anomalous code as malicious or benign.
- S0091: Skill in analyzing volatile data.
- S0092: Skill in identifying obfuscation techniques.
- S0093: Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.
- S0131: Skill in analyzing malware.
- S0132: Skill in conducting bit-level analysis.
- S0133: Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.
- S0156: Skill in performing packet-level analysis.

Knowledge

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0004: Knowledge of cybersecurity and privacy principles.
- K0005: Knowledge of cyber threats and vulnerabilities.
- K0006: Knowledge of specific operational impacts of cybersecurity lapses.
- K0018: Knowledge of encryption algorithms
- K0021: Knowledge of data backup and recovery.
- K0042: Knowledge of incident response and handling methodologies.
- K0060: Knowledge of operating systems.
- K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- K0077: Knowledge of server and client operating systems.
- K0078: Knowledge of server diagnostic tools and fault identification techniques.
- K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).
- K0117: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
- K0118: Knowledge of processes for seizing and preserving digital evidence.
- K0119: Knowledge of hacking methodologies.
- K0122: Knowledge of investigative implications of hardware, Operating Systems, and network technologies.
- K0123: Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
- K0125: Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
- K0128: Knowledge of types and collection of persistent data.
- K0131: Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
- K0132: Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
- K0133: Knowledge of types of digital forensics data and how to recognize them.
- K0134: Knowledge of deployable forensics.
- K0145: Knowledge of security event correlation tools.
- K0155: Knowledge of electronic evidence law.
- K0156: Knowledge of legal rules of evidence and court procedure.
- K0167: Knowledge of system administration, network, and operating system hardening techniques.
- K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

- K0182: Knowledge of data carving tools and techniques (e.g., Foremost).
- K0183: Knowledge of reverse engineering concepts.
- K0184: Knowledge of anti-forensics tactics, techniques, and procedures.
- K0185: Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
- K0186: Knowledge of debugging procedures and tools.
- K0187: Knowledge of file type abuse by adversaries for anomalous behavior.
- K0188: Knowledge of malware analysis tools (e.g., Olly Debug, Ida Pro).
- K0189: Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).
- K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
- K0254: Knowledge of binary analysis.
- K0255: Knowledge of network architecture concepts including topology, protocols, and components.
- K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- K0304: Knowledge of concepts and practices of processing digital forensic data.
- K0347: Knowledge and understanding of operational design.
- K0624 : Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Abilities

- A0005: Ability to decrypt digital data collections.
- A0043: Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.