TESTIMONIALS

just wanted to drop by and show my appreciation for the good work you put into this course. It now helps me to explain to I currently do which I did not know I was doing.

Jonathan Adrian
United States

This course was a massive help in understanding the different tools used in a SOC. I just wanted to use this medium to say thank you. Great resource!

Paul Udor
United Kingdom

If you are standing up your own SOC or managing an existing one, I'm sure you will take away many valuable info that will help make your life easier.

Mike O'Leary
United States

Excellent course. Compete training.

Alessandro Volpe
Italy

This is a fantastic course on Security Operations Center (SOC).

Kalyan Chakravarthy
India

I just got recruited as an Infosec Analyst in a bank and as a newbie. I have been overwhelmed by the great number of solutions being used to manage our operations and this course gave me insight into each solution and why it's put in place. From Web Application Firewall (WAF) to Data Leakage Prevention (DLP) to perimeter firewalls. The course is great!

Davids Olumide
Nigeria

CYBER DEFENSE ANALSYT

5	40	Laptop
Day Program	CPEs	Required

Cyberation LLC aims to address cyber security talent shortage by developing market ready resources. As a cybersecurity education partner of the United States National Initiative for Cybersecurity Careers and Studies (NICCS), its practitioner-focused, work role-based training programs are developed in alignment with the National Initiative for Cybersecurity Education's (NICE) Cybersecurity Workforce Framework.

Knowledge is transferred over the course of this 5-day period of intensive training while students will acquire skills by solving real-world cyber defense challenges, which include over 200 questions and solutions, during and after the 5-day training. These practical exercises are completed in our cyber defense lab where learners will be using the tools used by security professionals on the job.

Students also get to demonstrate abilities, developed through acquisition of knowledge and skills, as they collaborate to solve real world security problems. The activities (in the form of mini projects) are designed based on what cyber security professionals face on the job every day.

Unlike the cyber defense challenges solved individually, learners will be completing mini projects as team members. The thinking behind this is that no professional is an island in the real world - ideas are typically bounced off team members when addressing cyber security issues.

Available Trainings Formats
www.cyberation.io

Online Training
OnDemand
https://academy.cyberation.io/p/cyber-defense-analyst

Enterprise Training
Instructor-Led Training
http://academy.cyberation.io/p/cyber-defense-analyst-instructor-led

Cyberation
A Digiss LLC Company

Liberation through Cyber Security

Cyberation, the training division of Digiss LLC, aims to liberate the unemployed and underemployed by opening up the path to a fulfilling cyber security career.

Section Descriptions

SECTION 1: Cyber Security Essentials

Overview

This section of the course provides an overview of the NICE cybersecurity workforce framework, which establishes a taxonomy and common lexicon that describes cybersecurity profession and professionals. Additionally, students will learn about why cyber security matters to any organization regardless of its sector, the importance of people, process, and technology in cyber defense, as well as computer networking fundamentals to include concepts such as the OSI and TCP/IP models, network traffic analysis, the 3-way handshake and common networking services and protocols.

Section Learning Objectives

At the end of this course, learners will be able to

- Discuss the NICE Cybersecurity Workforce framework and its important elements
- Define cyber security as it pertains to digital information and key cyber security terms
- Examine popular cyber security certifications to determine the most appropriate ones to pursue.
- Recall and recognize sources of very useful cyber security resources and study materials as they build on the knowledge gained from this course
- Describe the roles of people, process, and technology in any cyber security program
- Define information security policy and discuss its importance
- Explain the importance of security standards to any cyber security program
- Demonstrate understanding of computer networking concepts
- Recall common networking services and protocols
- Describe how the OSI Model works and recall its 7 layers
- Perform network packet capture analysis with Wireshark
- Demonstrate an understanding of the Cisco Three-Layer Hierarchical Model
- Briefly explain the defense-in-depth model

SECTION 2: Cyber Threats, Vulnerabilities, And Cyber Attacks

Overview

In this module, we continue to lay the foundation upon which knowledge, skills, and ability will be built by gaining a good understanding of cyber threats, threat actors, vulnerabilities, and cyber-attacks. Among other things, students will learn about threat modelling and vulnerability lifecycle management. We will examine some cyber security breaches that were big enough to make the headlines in recent years, and the conditions that made them possible. Students will also learn about the tactics, techniques and procedures of cyber adversaries, the cyber kill chain, the Mandiant attack lifecycle and MITRE ATT&CK Framework.

Section Learning Objectives

At the end of this course, learners will be able to

- Discuss common types of cyber threats and their relevance
- Categorize cyber threat actors based on their objectives
- Discuss threat modelling and its importance to cyber defense
- Demonstrate good understanding of vulnerabilities
- Explain how vulnerabilities are rated
- Explain the role of vulnerabilities in cyber attacks
- Recall common types of vulnerabilities and sources
- Explain the vulnerability management lifecycle
- Discuss the global cyber threat landscape
- Explain the cyber kill chain and Mandiant attack lifecycle
- Discuss the MITRE ATT&CK Framework while recalling its key tactics and techniques
- Discuss each covered breach case study in terms of
  - What happened and how it happened
  - Its business and/or reputational impact
  - The enabling conditions (i.e., conditions that made it happened)
  - How it could have been prevented

SECTION 3: Protective Cyber Security Technologies

Overview

This section provides an overview of the NIST cybersecurity framework, but its main focus is on different types of technology solutions that can be implemented to create cyber defensive layers around information systems. In total, sixteen (16) different security technology solutions across five cyber defense domains, namely application security, cloud security, data security, endpoint security, and network security will be examined.

Section Learning Objectives

At the end of this course, learners will be able to

- Discuss the NIST cybersecurity framework and recall its functions and major categories
- Categorize certain cyber security vendors in accordance with the security domains addressed by their product
- Explain the importance of an effective application security program
- State the different types of application security testing techniques
- Explain the key functions of a web application firewall and its common deployment modes
- Explain the importance of an effective data security program
- Discuss various data leakage channels and how to protect data in its various states
- Distinguish between digital rights management and other forms of data security solutions
- Recall the features and functions of an endpoint protection platform
- Discuss the functions of various network security solutions such as the firewall, IPS/IDS, network access control, secure web gateway and secure email gateway
- Discuss cloud security and the shared responsibility matrix
- Explain how a CASB works and discuss the importance of cloud posture security manage

SECTION 4: Elements Of A Security Operations Center

Overview

In this section, we will examine the SOC, its supporting elements, and importance to any cyber security program. The SOC is a critical component of any security program. It is the place (physical or virtual) where security analysts monitor, detect, and respond to cyber security incidents. Students will learn about the role of a SOC analyst and the tools, operational processes, and procedures that are typically deployed in a value delivering SOC environment. Security analysts need to have an awareness of security events unfolding on their network. For this to happen, log sources must be identified and configured to audit, generate, and forward security events of interest to a central location where they can be processed and turned into alerts where necessary. All of these will become very clear to attendees of this course.

Section Learning Objectives

At the end of this course, learners will be able to

- Discuss the NIST cybersecurity framework and recall its functions and major categories
- Demonstrate very good understanding of the people, process, and technology elements of a SOC

Section Descriptions

- Itemize important log sources and explain the logging and log collection process
- Discuss the importance of a SIEM to a SOC
- Express their career progression options if they ever end up working in a SOC
- Demonstrate good understanding of security alerts
- Define alert use cases and describe how they are developed
- Discuss actionable reports and how to derive the best value out of them
- Demonstrate good understanding of the tasks undertaken by SOC analysts on daily basis
- Demonstrate good understanding of security incident response (IR)
- Recall all the phases of IR and what happens in each phase
- List some of the important tools to have in an IR jump kit
- State and discuss some of the key factors that affect incident categorization
- Use a SIEM tool to investigate security incidents
- Interpret an IR process workflow
- Demonstrate good understanding of key considerations for outsourcing and how to get the best out of managed security services
- Understand the importance of incident response retainer service
- Justify investment in third party security events monitoring and IR services

SECTION 5: Cyber Risk Management, Cyber Laws, And Security Governance

Overview

For most people in cyber security, this isn't very interesting due to the lack of technical component. However, it is important to bear in mind that the whole essence of cyber security is to reduce risk to information asset. This section of the training is the reason why other areas exist, therefore paying attention to it is very important. Most business leaders will not understand the SIEM, endpoint protection agent or CASB but they understand risk management, compliance, audit, and cyber laws. Developing keen interest in this area will make learners well-rounded professionals who are capable of speaking both technical and business languages.

Section Learning Objectives

At the end of this course, learners will be able to

- Demonstrate an understanding of key risk management terms and definitions
- Align cyber risk management efforts with an enterprise risk management program
- Discuss the risk assessment process
- Describe the process of risk analysis and the expected outcome of the exercise
- Demonstrate an understanding of risk appetite and risk tolerance
- Recall key considerations related to the creation of a risk assessment report
- List and explain each of the four common risk response actions
- Outline the importance of risk monitoring and demonstrate an understanding of the process
- Demonstrate basic understanding of intellectual property law and different type of intellectual property
- Demonstrate an understanding of the Sarbanes-Oxley Act and how to support related audit and compliance efforts from a cyber security standpoint
- Demonstrate good understanding of HIPAA and the EU GDPR
- Recall elements of cyber security governance
- List and discuss common factors that influence cyber defense efforts
- Demonstrate basic understanding of the functions of a cyber security steering committee
- Explain the roles of the audit compliance functions in cyber defense

SECTION 6: Cyber Defense Challenges (Lab)

- Scenario 1 - External Attack Against A Webserver
- Scenario 2 - Unauthorized Changes
- Scenario 3 - Suspected Unauthorized Access To Webserver
- Scenario 4 - Suspected Unauthorized Access To Webserver
- Scenario 5 - DDOS SYN Flood Attack
- Scenario 6 - Webshell Attack Detection and Analysis
- Scenario 7 - Client Side Attack - Drive by Download
- Scenario 8 - Suspicious Email Recieved From An Unknown Party
- Scenario 9 - Detection and Analysis of Reverse Shell Attack
- Scenario 10 - Data Breach Notification
- Scenario 11 - Malicious Command Execution
- Scenario 12 - Internal Reconnaisance Activities Observed
- Scenario 13 - Detect and Analyze Data Exfiltration
- Scenario 14 - Anomaly Detection and Investigation
- Scenario 15 - Lost or Stolen Laptop
- Scenario 16 - Suspicious URL Access by External IP
- Scenario 17 - Investigating Usage of Hacking Tools
- Scenario 18 - Detecting and Responding to a Ransomware Attack
- Scenario 19 - Malware Detection and Response
- Scenario 20 - Researching Suspicious Historical Events