Cybersecurity Essentials

1. ΕΙΣΑΓΩΓΗ

Το **Πρόγραμμα Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης E-Learning** του **ΕΚΠΑ** είναι από τις αρχές του 2025 **Επίσημη Ακαδημία** της Cisco με την ονομασία **E-Learning NKUA**. Η Cisco είναι ένας από τους κορυφαίους παρόχους τεχνολογικής εκπαίδευσης παγκοσμίως.
Στη συνέχεια, σας παρουσιάζουμε αναλυτικά το πρόγραμμα σπουδών για το πρόγραμμα επαγγελματικής επιμόρφωσης και κατάρτισης: **«Cybersecurity Essentials»**, τις προϋποθέσεις συμμετοχής σας σε αυτό, καθώς και όλες τις λεπτομέρειες που πιστεύουμε ότι είναι χρήσιμες, για να έχετε μια ολοκληρωμένη εικόνα του προγράμματος.

2. ΣΚΟΠΟΣ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Το πρόγραμμα έχει σχεδιαστεί ως η ιδανική αφετηρία για όσους επιθυμούν να ακολουθήσουν επαγγελματική σταδιοδρομία στον τομέα της Κυβερνοασφάλειας.

Σκοπός του προγράμματος είναι η ανάπτυξη δεξιοτήτων επαγγελματικής ετοιμότητας και η ενίσχυση των γνώσεων που απαιτούνται για την επιτυχή είσοδο στην αγορά εργασίας. Μέσω εκπαιδευτικών βίντεο και πλούσιου διαδραστικού περιεχομένου, οι εκπαιδευόμενοι/ες έχουν τη δυνατότητα να αποκτήσουν και να εφαρμόσουν κρίσιμες δεξιότητες, μέσα από προχωρημένες πρακτικές δραστηριότητες και προσομοιώσεις, οι οποίες ενισχύουν τη βιωματική μάθηση και τη συστηματική κατανόηση της ύλης.

Το πρόγραμμα εξοπλίζει τους/τις συμμετέχοντες/ουσες με δεξιότητες εισαγωγικού επιπέδου σε τρεις βασικούς τομείς της κυβερνοασφάλειας:

- **Ασφάλεια Τερματικών Συσκευών (Endpoint Security)**
- **Άμυνα Δικτύου (Network Defense)**
- **Διαχείριση Κυβερνοαπειλών (Cyber Threat Management)**

Αυτοί οι τομείς προσφέρουν μια ολοκληρωμένη και ενσωματωμένη μαθησιακή εμπειρία για τον ρόλο του **Junior Cybersecurity Analyst.**

Η επιτυχής ολοκλήρωση του προγράμματος, προετοιμάζει τους/τις συμμετέχοντες/ ουσες για την απόκτηση της πιστοποίησης **Cisco Certified Support Technician (CCST) Cybersecurity,** εισαγωγικού επιπέδου**.**

3. ΚΑΤΗΓΟΡΙΕΣ ΥΠΟΨΗΦΙΩΝ ΠΟΥ ΓΙΝΟΝΤΑΙ ΔΕΚΤΟΙ ΣΤΟ ΠΡΟΓΡΑΜΜΑ - ΤΡΟΠΟΣ ΕΝΤΑΞΗΣ

Αίτηση συμμετοχής μπορούν να υποβάλλουν:

- **απόφοιτοι Πανεπιστημίου/ΤΕΙ της ημεδαπής και της αλλοδαπής**
- **απόφοιτοι δευτεροβάθμιας εκπαίδευσης με συναφή στο αντικείμενο εργασιακή εμπειρία**

Η αίτηση συμμετοχής υποβάλλεται ηλεκτρονικά, μέσω της ιστοσελίδας:

https://elearningekpa.gr/

4. ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

Τα προαπαιτούμενα για την παρακολούθηση του Προγράμματος από τους εκπαιδευόμενους είναι:

- Πρόσβαση στο Διαδίκτυο
- Κατοχή προσωπικού e-mail
- Βασικές γνώσεις χειρισμού ηλεκτρονικών υπολογιστών
- Απαιτείται γνώση της Αγγλικής Γλώσσας σε επίπεδο Β2
- Γνώση δικτύωσης TCP/IP, συμπεριλαμβανομένων των πρωτοκόλλων δικτύου, υπηρεσιών, διαδικασιών και βασικής ρύθμισης συσκευών δικτύου όπως δρομολογητές (routers) και διακόπτες (switches)

5. ΑΠΑΙΤΟΥΜΕΝΟΣ ΕΞΟΠΛΙΣΜΟΣ

Οι πρακτικές ασκήσεις απαιτούν υπολογιστές ικανούς να εκτελούν λογισμικό εικονικοποίησης (VirtualBox ή UTM) με τουλάχιστον 4GB μνήμης RAM και 20GB ελεύθερο χώρο στο δίσκο. Οι ασκήσεις που απαιτούν πιο σύνθετα δίκτυα χρησιμοποιούν το εργαλείο προσομοίωσης δικτύου Packet Tracer. Άλλες εκπαιδευτικές δραστηριότητες απαιτούν επικεντρωμένη έρευνα μέσω διαδικτύου και την ολοκλήρωση εγγράφων εργαστηρίων.

Προαιρετικός Εξοπλισμός Εργαστηρίου:

- Υπολογιστής με Microsoft Windows

Λογισμικό:

- Oracle VirtualBox ή UTM

- Αρχείο OVA για εικονική μηχανή εργαστηρίου
- Packet Tracer 8.2.1 ή νεότερη έκδοση

6. ΤΡΟΠΟΣ ΔΙΕΞΑΓΩΓΗΣ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ, ΕΞΕΤΑΣΗΣ ΚΑΙ ΒΑΘΜΟΛΟΓΗΣΗΣ

Η διδασκαλία του προγράμματος «**Cybersecurity Essentials»** διεξάγεται εξ αποστάσεως στη Cisco, μέσω της επίσημης πλατφόρμα της, προσφέροντας στον εκπαιδευόμενο αυτονομία, δηλαδή τη δυνατότητα μελέτης ανεξαρτήτως περιοριστικών παραγόντων, όπως η υποχρέωση της φυσικής του παρουσίας σε συγκεκριμένο χώρο και χρόνο.

Το πρόγραμμα περιλαμβάνει **τέσσερις (4) διαδικτυακές συναντήσεις (live streaming)**, οι οποίες οργανώνονται κατά τη διάρκεια του εκπαιδευτικού κύκλου και λειτουργούν υποστηρικτικά προς τη μαθησιακή διαδικασία

Το εκπαιδευτικό υλικό του προγράμματος διατίθεται σταδιακά ανά θεματική ενότητα, στην αγγλική γλώσσα. Παράλληλα, παρέχεται **πλήρης εκπαιδευτική υποστήριξη** στην ελληνική γλώσσα. Ο/Η εκπαιδευόμενος/η μπορεί να επικοινωνεί ηλεκτρονικά με τον αρμόδιο εκπαιδευτή, μέσω ενσωματωμένου συστήματος επικοινωνίας στην πλατφόρμα, για την άμεση επίλυση αποριών.

Το πρόγραμμα αποτελείται από **είκοσι επτά (27) θεματικές ενότητες**. Περιλαμβάνει εβδομήντα πέντε (75) ασκήσεις, διαδραστικές δραστηριότητες, κουίζ αυτοαξιολόγησης και επτά (7) εξετάσεις ενδιάμεσου ελέγχου (Checkpoint Exam). Όλες οι παραπάνω δραστηριότητες παρέχουν άμεση ανατροφοδότηση και έχουν σχεδιαστεί για την αξιολόγηση του βαθμού κατανόησης και απόκτησης δεξιοτήτων από τους συμμετέχοντες/ουσες. Στο τέλος του προγράμματος, όσοι εκπαιδευόμενοι/ες επιθυμούν μπορούν να λάβουν μέρος σε μια **τελική αξιολόγηση**.

Η πρακτική εφαρμογή του εκπαιδευτικού υλικού υποστηρίζεται από το περιβάλλον προσομοίωσης **Cisco® Packet Tracer**, το οποίο προσφέρει τη δυνατότητα στους/στις συμμετέχοντες/ουσες να εξασκηθούν σε ελεγχόμενα σενάρια, ενισχύοντας δεξιότητες κριτικής σκέψης και επίλυσης προβλημάτων, που είναι απαραίτητες στον τομέα της κυβερνοασφάλειας.

Η απόκτηση ψηφιακού **Badge** από την **Cisco Networking Academy** προϋποθέτει την επιτυχή ολοκλήρωση μιας **τελικής αξιολόγησης** με ελάχιστη βαθμολογία **70/100.** Οι συμμετέχοντες/ουσες που ολοκληρώνουν επιτυχώς το πρόγραμμα και αποκτούν το Badge, έχουν τη δυνατότητα —εφόσον το επιθυμούν— να συμμετάσχουν, με καταβολή επιπλέον κόστους, στις επίσημες εξετάσεις για την απόκτηση της πιστοποίησης **Cisco Certified Support Technician (CCST) Cybersecurity**, εισαγωγικού επιπέδου.

Η επιτυχής ολοκλήρωση του προγράμματος συνοδεύεται και από την έκδοση **Βεβαίωσης Συμμετοχής** από το Πρόγραμμα Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης E-Learning του Κ.Ε.ΔΙ.ΒΙ.Μ. του Ε.Κ.Π.Α..

7. ΛΟΙΠΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΕΚΠΑΙΔΕΥΟΜΕΝΩΝ – ΠΡΟΫΠΟΘΕΣΕΙΣ ΧΟΡΗΓΗΣΗΣ ΒΕΒΑΙΩΣΗΣ ΣΥΜΜΕΤΟΧΗΣ

Πέρα από την επιτυχή ολοκλήρωση του προγράμματος για τη χορήγηση της βεβαίωσης συμμετοχής απαιτούνται τα εξής:

► **Συμμετοχή του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Ταυτοποίησης** Η διαδικασία Δειγματοληπτικού Ελέγχου Ταυτοποίησης Εκπαιδευόμενου στοχεύει στη διασφάλιση της ποιότητας των παρεχομένων εκπαιδευτικών υπηρεσιών. Συγκεκριμένα, εξουσιοδοτημένο στέλεχος του Κέντρου Επιμόρφωσης και Δια Βίου Μάθησης του ΕΚΠΑ, επικοινωνεί τηλεφωνικώς με ένα τυχαίο δείγμα εκπαιδευόμενων, προκειμένου να διαπιστωθεί εάν συμμετείχαν στις εκπαιδευτικές διαδικασίες του προγράμματος, εάν αντιμετώπισαν προβλήματα σε σχέση με το εκπαιδευτικό υλικό, την επικοινωνία με τον ορισμένο εκπαιδευτή τους, καθώς και με τη γενικότερη μαθησιακή διαδικασία. Η τηλεφωνική επικοινωνία διεξάγεται με την ολοκλήρωση του εκάστοτε προγράμματος, ενώ η μέση χρονική διάρκειά της συγκεκριμένης διαδικασίας είναι περίπου 2-3 λεπτά. Σε περίπτωση μη συμμετοχής του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Ταυτοποίησης, εφόσον κληθεί, ή μη ταυτοποίησής του κατά τη διεξαγωγή της, δεν χορηγείται η βεβαίωση συμμετοχής, ακόμα και αν έχει ολοκληρώσει επιτυχώς την εξ αποστάσεως εκπαιδευτική διαδικασία.

► **Συμμετοχή του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Εγγράφων**

Ο δειγματοληπτικός έλεγχος εγγράφων διασφαλίζει την εγκυρότητα των στοιχείων που έχει δηλώσει ο εκπαιδευόμενος στην αίτηση συμμετοχής του στο Πρόγραμμα και βάσει των οποίων έχει αξιολογηθεί και εγκριθεί η αίτηση συμμετοχής του σε αυτό. Κατά τη διάρκεια ή μετά το πέρας του προγράμματος, πραγματοποιείται δειγματοληπτικός έλεγχος εγγράφων από τη Γραμματεία. Ο εκπαιδευόμενος θα πρέπει να είναι σε θέση να προσκομίσει τα απαραίτητα δικαιολογητικά τα οποία πιστοποιούν τα στοιχεία που έχει δηλώσει στην αίτηση συμμετοχής (Αντίγραφο Πτυχίου, Αντίγραφο Απολυτήριου Λυκείου, Βεβαίωση Εργασιακής Εμπειρίας, Γνώση Ξένων Γλωσσών κ.τ.λ.). Σε περίπτωση μη συμμετοχής του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Εγγράφων, εφόσον κληθεί, ή μη ύπαρξης των δικαιολογητικών αυτών, δεν χορηγείται η βεβαίωση συμμετοχής, ακόμα και αν έχει ολοκληρώσει επιτυχώς την εξ αποστάσεως εκπαιδευτική διαδικασία.

► **Αποπληρωμή του συνόλου των διδάκτρων**

Ο εκπαιδευόμενος θα πρέπει να μην έχει οικονομικής φύσεως εκκρεμότητες. Σε περίπτωση που υπάρχουν τέτοιες, η βεβαίωση συμμετοχής διατηρείται στο αρχείο της Γραμματείας, μέχρι την ενημέρωση της για τη διευθέτηση της εκκρεμότητας.

Αναλυτική περιγραφή των παραπάνω υπάρχει στον Κανονισμό Σπουδών:
https://elearningekpa.gr/regulation

8. ΠΩΣ ΔΙΑΜΟΡΦΩΝΕΤΑΙ Η ΥΛΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Το πρόγραμμα επαγγελματικής επιμόρφωσης και κατάρτισης περιλαμβάνει **27 θεματικές ενότητες (μαθήματα)**.

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΩΝ

Θεματική Ενότητα - Cybersecurity Threats, Vulnerabilities, and Attacks

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Common Threats

Διδακτική Ενότητα 3: Deception

Διδακτική Ενότητα 4: Cyber Attacks

Διδακτική Ενότητα 5: Wireless and Mobile Device Attacks

Διδακτική Ενότητα 6: Application Attacks

Διδακτική Ενότητα 7: Cybersecurity Threats, Vulnerabilities, and Attacks Summary

Θεματική Ενότητα - Securing Networks

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Current State of Affairs

Διδακτική Ενότητα 3: Who is Attacking Our Network?

Διδακτική Ενότητα 4: Securing Networks Summary

Θεματική Ενότητα - Attacking the FoundationΔιδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: IP PDU Details

Διδακτική Ενότητα 3: IP Vulnerabilities

Διδακτική Ενότητα 4: TCP and UDP Vulnerabilities

Διδακτική Ενότητα 5: Attacking the Foundation Summary

Θεματική Ενότητα - Attacking the Foundation

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: IP Services

Διδακτική Ενότητα 3: Enterprise Services

Διδακτική Ενότητα 4: Mitigating Common Network Attacks

Διδακτική Ενότητα 5: Attacking What We Do Summary

Θεματική Ενότητα - Wireless Network Communication

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Wireless Communications

Διδακτική Ενότητα 3: WLAN Threats

Διδακτική Ενότητα 4: Secure WLANs

Διδακτική Ενότητα 5: Wireless Network Communication Summary

Θεματική Ενότητα - Network Security Infrastructure

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Security Devices

Διδακτική Ενότητα 3: Security Services

Διδακτική Ενότητα 4: Network Security Infrastructure Summary

Θεματική ή Ενότητα - The Windows Operating System

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Windows History

Διδακτική Ενότητα 3: Windows Architecture and Operations

Διδακτική Ενότητα 4: Windows Configuration and Monitoring

Διδακτική Ενότητα 5: Windows Security

Διδακτική Ενότητα 6: The Windows Operating System Summary

Θεματική Ενότητα - Linux Overview

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Linux Basics

Διδακτική Ενότητα 3: Working in the Linux Shell

Διδακτική Ενότητα 4: Linux Servers and Clients

Διδακτική Ενότητα 5: Basic Server Administration

Διδακτική Ενότητα 6: The Linux File System

Διδακτική Ενότητα 7: Working with the Linux GUI

Διδακτική Ενότητα 8: Working on a Linux Host

Διδακτική Ενότητα 9: Linux Basics Summary

Θεματική Ενότητα - System and Endpoint Protection

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Defending Systems and Devices

Διδακτική Ενότητα 3: Antimalware Protection

Διδακτική Ενότητα 4: Host-Based Intrusion Prevention

Διδακτική Ενότητα 5: Application Security

Διδακτική Ενότητα 6: System and Endpoint Protection Summary

Θεματική Ενότητα - Cybersecurity Principles, Practices, and Processes

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: The Three Dimensions

Διδακτική Ενότητα 3: States of Data

Διδακτική Ενότητα 4: Cybersecurity Countermeasures

Διδακτική Ενότητα 5: Cybersecurity Principles, Practices, and Processes Summary

Θεματική Ενότητα - Understanding Defense

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Defense-in-Depth

Διδακτική Ενότητα 3: Cybersecurity Operations Management

Διδακτική Ενότητα 4: Security Policies, Regulations, and Standards

Διδακτική Ενότητα 5: Understanding Defense Summary

Θεματική Ενότητα - System and Network Defense

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Physical Security

Διδακτική Ενότητα 3: Application Security

Διδακτική Ενότητα 4: Network Hardening: Services and Protocols

Διδακτική Ενότητα 5: Network Hardening: Segmentation

Διδακτική Ενότητα 6: Hardening Wireless and Mobile Devices

Διδακτική Ενότητα 7: Cybersecurity Resilience

Διδακτική Ενότητα 8: Embedded and Specialized Systems

Διδακτική Ενότητα 9: System and Network Defense Summary

Θεματική Ενότητα - Access Control

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Access Controls

Διδακτική Ενότητα 3: Access Control Concepts

Διδακτική Ενότητα 4: Account Management

Διδακτική Ενότητα 5: AAA Usage and Operation

Διδακτική Ενότητα 6: Access Control Summary

Θεματική Ενότητα - Access Control Lists

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Introduction to Access Control Lists

Διδακτική Ενότητα 3: Wildcard Masking

Διδακτική Ενότητα 4: Configure ACLs

Διδακτική Ενότητα 5: Named Standard IPv4 ACL Syntax

Διδακτική Ενότητα 6: Implement ACLs

Διδακτική Ενότητα 7: Mitigate Attacks with ACLs

Διδακτική Ενότητα 8: IPv6 ACLs

Διδακτική Ενότητα 9: Access Control Lists Summary

Θεματική Ενότητα - Firewall Technologies

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Secure Networks with Firewalls

Διδακτική Ενότητα 3: Firewalls in Network Design

Διδακτική Ενότητα 4: Firewall Technologies Summary

Θεματική Ενότητα - Zone-Based Policy Firewalls

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: ZPF Overview

Διδακτική Ενότητα 3: ZPF Operation

Διδακτική Ενότητα 4: Configure a ZPF

Διδακτική Ενότητα 5: Zone-Based Firewalls Summary

Θεματική Ενότητα - Cloud Security

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Virtualization and Cloud Computing

Διδακτική Ενότητα 3: The Domains of Cloud Security

Διδακτική Ενότητα 4: Cloud Infrastructure Security

Διδακτική Ενότητα 5: Cloud Application Security

Διδακτική Ενότητα 6: Cloud Data Security

Διδακτική Ενότητα 7: Protecting VMs

Διδακτική Ενότητα 8: Cloud Security Summary

Θεματική Ενότητα - Cryptography

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Confidentiality

Διδακτική Ενότητα 3: Obscuring Data

Διδακτική Ενότητα 4: Integrity and Authenticity

Διδακτική Ενότητα 5: Using Hashes

Διδακτική Ενότητα 6: Public Key Cryptography

Διδακτική Ενότητα 7: Authorities and the PKI Trust System

Διδακτική Ενότητα 8: Applications and Impacts of Cryptography

Διδακτική Ενότητα 9: Cryptography Summary

Θεματική Ενότητα - Technologies and Protocols

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Monitoring Common Protocols

Διδακτική Ενότητα 3: Security Technologies

Διδακτική Ενότητα 4: Technologies and Protocols Summary

Θεματική Ενότητα - Network Security Data

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Types of Security Data

Διδακτική Ενότητα 3: End Device Logs

Διδακτική Ενότητα 4: Network Logs

Διδακτική Ενότητα 5: Network Security Data Summary

Θεματική Ενότητα - Evaluating Alerts

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Sources of Alerts

Διδακτική Ενότητα 3: Overview of Alert Evaluation

Διδακτική Ενότητα 4: Evaluating Alerts Summary

Θεματική Ενότητα - Governance and Compliance

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Governance

Διδακτική Ενότητα 3: The Ethics of Cybersecurity

Διδακτική Ενότητα 4: IT Security Management Framework

Διδακτική Ενότητα 5: Governance and Compliance Summary

Θεματική Ενότητα - Network Security Testing

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Security Assessments

Διδακτική Ενότητα 3: Network Security Testing Techniques

Διδακτική Ενότητα 4: Network Security Testing Tools

Διδακτική Ενότητα 5: Penetration Testing

Διδακτική Ενότητα 6: Network Security Testing Summary

Θεματική Ενότητα - Threat Intelligence

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Information Sources

Διδακτική Ενότητα 3: Threat Intelligence Services

Διδακτική Ενότητα 4: Threat Intelligence Summary

Θεματική Ενότητα - Endpoint Vulnerability Assessment

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Network and Server Profiling

Διδακτική Ενότητα 3: Common Vulnerability Scoring System (CVSS)

Διδακτική Ενότητα 4: Secure Device Management

Διδακτική Ενότητα 5: Endpoint Vulnerability Assessment Summary

Θεματική Ενότητα - Risk Management and Security Controls

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Risk Management

Διδακτική Ενότητα 3: Risk Assessment

Διδακτική Ενότητα 4: Security Controls

Διδακτική Ενότητα 5: Risk Management and Security Controls Summary

Θεματική Ενότητα - Digital Forensics and Incident Analysis and Response

Διδακτική Ενότητα 1: Introduction

Διδακτική Ενότητα 2: Evidence Handling and Attack Attribution

Διδακτική Ενότητα 3: The Cyber Kill Chain

Διδακτική Ενότητα 4: The Diamond Model of Intrusion Analysis

Διδακτική Ενότητα 5: Incident Response

Διδακτική Ενότητα 6: Disaster Recovery

Διδακτική Ενότητα 7: Digital Forensics and Incident Analysis and Response Summary