

---

# CyberOps Associate

---

## 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 ΝΚΥΑ**. 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: «**CyberOps Associate**», 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

Σκοπός του προγράμματος είναι η εκπαίδευση των συμμετεχόντων/ουσών σε βασικές γνώσεις και δεξιότητες αρχικού επιπέδου για την ανίχνευση, ανάλυση και διαχείριση απειλών στον τομέα της κυβερνοασφάλειας. Ειδικότερα, οι εκπαιδευόμενοι/ες θα εξοικειωθούν με έννοιες όπως η λειτουργία των λειτουργικών συστημάτων Windows και Linux, η ανάλυση πρωτοκόλλων και υπηρεσιών δικτύου, καθώς και η χρήση εργαλείων ανοιχτού κώδικα για την παρακολούθηση και αντιμετώπιση απειλών. Το πρόγραμμα επιδιώκει την κριτική κατανόηση ζητημάτων που αφορούν την ασφάλεια δικτύων και συστημάτων, καθώς και την εφαρμογή μοντέλων διαχείρισης περιστατικών ασφάλειας, μέσα σε περιβάλλοντα εργασίας όπως το Security Operations Center (SOC). Με αυτόν τον τρόπο, οι συμμετέχοντες/ουσες θα είναι σε θέση να εφαρμόζουν τις γνώσεις και τις δεξιότητές τους σε πραγματικά σενάρια κυβερνοασφάλειας, προετοιμάζοντάς τους για επαγγελματική εξέλιξη στον τομέα.

Η επιτυχής ολοκλήρωση του προγράμματος, προετοιμάζει τους/τις συμμετέχοντες/ ουσες για την απόκτηση της πιστοποίησης **Cisco Certified Cybersecurity Associate**.

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

Το πρόγραμμα απευθύνεται σε απόφοιτους Πανεπιστημιακής Εκπαίδευσης/ΤΕΙ της ημεδαπής και της αλλοδαπής, καθώς και σε απόφοιτους Δευτεροβάθμιας Εκπαίδευσης με συναφή στο αντικείμενο εργασιακή εμπειρία καθώς και σε απόφοιτους Μεταλυκειακής Εκπαίδευσης με σπουδές συναφούς αντικειμένου.

Ειδικότερα, το πρόγραμμα απευθύνεται σε επαγγελματίες του **κλάδου της Πληροφορικής και των Θετικών Επιστημών**, οι οποίοι επιδιώκουν να εξειδικευθούν στον τομέα της κυβερνοασφάλειας και ειδικότερα στον ρόλο του **Αναλυτή Ασφαλείας (Security Analyst)** στο πλαίσιο λειτουργίας **Επιχειρησιακών Κέντρων Ασφάλειας (Security Operations Centers – SOC)**.

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
- ▶ Απαιτείται γνώση της Αγγλικής Γλώσσας σε επίπεδο B2
- ▶ Βασικές γνώσεις λειτουργικών συστημάτων Windows και Linux
- ▶ Βασικές γνώσεις υπολογιστικών δικτύων (επίπεδο CCNA ITN), οι οποίες αφορούν τη βασική θεωρία δικτύων (OSI Model, TCP/IP, IP Addressing, Basic device configuration)
- ▶ Βασικές γνώσεις δυαδικού και δεκαεξαδικού συστήματος

## 5. ΑΠΑΙΤΟΥΜΕΝΟΣ ΕΞΟΠΛΙΣΜΟΣ

**Βασικό Πακέτο Εξοπλισμού:**

Υπολογιστές (PCs) - ελάχιστες προδιαγραφές συστήματος

- CPU: Intel Pentium 4, 2.53 GHz ή ισοδύναμο με υποστήριξη virtualization
- Λειτουργικά Συστήματα (Operating Systems), όπως Microsoft Windows, Linux, και Mac OS
- 64-bit επεξεργαστής (processor)
- RAM: 8 GB
- Αποθηκευτικός χώρος (Storage): 40 GB ελεύθερου χώρου δίσκου
- Ανάλυση οθόνης (Display resolution): 1024 x 768
- Γραμματοσειρές (fonts) υποστηρίζοντας κωδικοποίηση Unicode (Unicode encoding) (για προβολή σε γλώσσες εκτός των Αγγλικών)
- Οι πιο πρόσφατοι οδηγοί κάρτας γραφικών (video card drivers) και ενημερώσεις λειτουργικού συστήματος (operating system updates)

#### Λογισμικό:

- Oracle VM VirtualBox Manager (έκδοση 6.1 ή νεότερη)
- CyberOps Workstation VM
  - Διαθέσιμο για λήψη από το πρόγραμμα
  - Απαιτεί 1 GB RAM, 20 GB χώρο στο δίσκο
- Security Onion VM
  - Διαθέσιμο για λήψη από το πρόγραμμα
  - Απαιτεί 4 GB RAM (ελάχιστο), 8 GB RAM (ισχυρή σύσταση), 20 GB χώρο στο δίσκο

## 6. ΤΡΟΠΟΣ ΔΙΕΞΑΓΩΓΗΣ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Η διδασκαλία του προγράμματος «**CyberOps Associate**» 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 **δεκαοκτώ (18) 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 οκτώ (28) θεματικές ενότητες**. Περιλαμβάνει συνολικά τριάντα (30) βίντεο, σαράντα έξι (46) εργαστήρια (Labs) πρακτικά (hands-on) και θεωρητικά (paper labs), καθώς και έξι (6) δραστηριότητες που υποστηρίζονται από το περιβάλλον προσομοίωσης **Cisco® Packet Tracer**. Οι δραστηριότητες αυτές στοχεύουν στην εξερεύνηση, απόκτηση και ενίσχυση δεξιοτήτων.

Στο πλαίσιο του προγράμματος περιλαμβάνονται εννέα (9) διαδραστικές δραστηριότητες και προσφέρονται σαράντα έξι (46) αυτοδιαγνωστικά κουίζ **Check Your Understanding**. Τα κουίζ αυτά έχουν σχεδιαστεί ώστε να επιτρέπουν στους/στις εκπαιδευόμενους/ες να αξιολογούν την

κατανόηση του εκπαιδευτικού υλικού και δεν επηρεάζουν τη συνολική τους βαθμολογία, καθώς έχουν διαγνωστικό χαρακτήρα.

Επιπρόσθετα, το πρόγραμμα περιλαμβάνει είκοσι οκτώ (28) **τεστ ενότητων (Module Quizzes)**, τα οποία αποτελούν αυτοαξιολογήσεις και ενσωματώνουν τις έννοιες και δεξιότητες που διδάχθηκαν οι συμμετέχοντες/ούσες σε όλη τη σειρά των διδακτικών ενότητων κάθε θεματικής ενότητας.

Παράλληλα, το πρόγραμμα περιλαμβάνει εννέα (9) εξετάσεις (Checkpoint Exam), οι οποίες αξιολογούν το περιεχόμενο πολλαπλών θεματικών ενότητων. Συγκεκριμένα, οι εξετάσεις οργανώνονται ως εξής:

1. Θεματικές ενότητες 1–2: Threat Actors and Defenders Group Exam
2. Θεματικές ενότητες 3–4: Operating System Overview Group Exam
3. Θεματικές ενότητες 5–10: Network Fundamentals Group Exam
4. Θεματικές ενότητες 11–12: Network Infrastructure Security Group Exam
5. Θεματικές ενότητες 13–17: Threats and Attacks Group Exam
6. Θεματικές ενότητες 18–20: Network Defense Group Exam
7. Θεματικές ενότητες 21–23: Cryptography and Endpoint Protection Group Exam
8. Θεματικές ενότητες 24–25: Protocols and Log Files Group Exam
9. Θεματικές ενότητες 26–28: Analyzing Security Data Group Exam

Με την ολοκλήρωση του προγράμματος οι εκπαιδευόμενοι/ες οφείλουν να υποβάλουν:

- Την εξέταση **Cisco Cybersecurity Associate v1.2 Certification Practice Exam**, η οποία αποτελεί προσομοίωση της επίσημης εξέτασης που απαιτείται για την απόκτηση της πιστοποίησης **Cisco Certified Cybersecurity Associate**.
- Την εξέταση **CyberOps Associate 1.0 Practice Final Exam** που αποτελεί προσομοίωση της τελικής εξέτασης.
- Την τελική εξέταση **CyberOps Associate 1.0 Final Exam**.

Σημειώνεται ότι τα αποτελέσματα των δύο πρώτων εξετάσεων δεν επηρεάζουν τη βαθμολογία της τελικής εξέτασης.

Τέλος, το πρόγραμμα περιλαμβάνει:

- Ένα (1) Εργαστήριο Αξιολόγησης Δεξιοτήτων (Skills Assessment Lab)
- Ένα (1) ερωτηματολόγιο (End-of-Course Feedback) για την παροχή ανατροφοδότησης σχετικά με το περιεχόμενο του προγράμματος.

Η απόκτηση του **ψηφιακού Badge** από την Cisco Networking Academy προϋποθέτει την επιτυχή ολοκλήρωση της τελικής εξέτασης με ελάχιστη βαθμολογία 70/100 καθώς και την υποβολή του ερωτηματολογίου αξιολόγησης (end-of-course survey).

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 Cybersecurity Associate**.

Η επιτυχής ολοκλήρωση του προγράμματος συνοδεύεται και από την έκδοση **Βεβαίωσης Συμμετοχής** από το Πρόγραμμα Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης E-Learning του ΕΚΠΑ.

## **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 τηλεφωνικά 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 **28 θεματικές ενότητες (μαθήματα)**.

### **ΠΕΡΙΓΡΑΦΗ ΘΕΜΑΤΙΚΩΝ ΕΝΟΤΗΤΩΝ**

Θεματική ενότητα - The Danger

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: War Stories**

**Διδακτική Ενότητα 3: Threat Actors**

**Διδακτική Ενότητα 4: Threat Impact**

**Διδακτική Ενότητα 5: The Danger Summary**

Θεματική ενότητα - Fighters in the War Against Cybercrime

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: The Modern Security Operations Center**

**Διδακτική Ενότητα 3: Becoming a Defender**

**Διδακτική Ενότητα 4: Fighters in the War Against Cybercrime Summary**

### Θεματική 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 - Network Protocols

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Network Communications Process**

**Διδακτική Ενότητα 3: Communications Protocols**

**Διδακτική Ενότητα 4: Data Encapsulation**

**Διδακτική Ενότητα 5: Network Protocols Summary**

## Θεματική Ενότητα - Ethernet and Internet Protocol (IP)

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Ethernet**

**Διδακτική Ενότητα 3: IPv4**

**Διδακτική Ενότητα 4: IP Addressing Basics**

**Διδακτική Ενότητα 5: Types of IPv4 Addresses**

**Διδακτική Ενότητα 6: The Default Gateway**

**Διδακτική Ενότητα 7: IPv6**

**Διδακτική Ενότητα 8: Ethernet and IP Protocol Summary**

## Θεματική Ενότητα - Connectivity Verification

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: ICMP**

**Διδακτική Ενότητα 3: Ping and Traceroute Utilities**

**Διδακτική Ενότητα 4: Connectivity Verification Summary**

## Θεματική Ενότητα - Address Resolution Protocol

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: MAC and IP**

**Διδακτική Ενότητα 3: ARP**

**Διδακτική Ενότητα 4: ARP Issues**

**Διδακτική Ενότητα 5: Address Resolution Protocol Summary**

## Θεματική Ενότητα - The Transport Layer

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Transport Layer Characteristics**

**Διδακτική Ενότητα 3: Transport Layer Session Establishment**

**Διδακτική Ενότητα 4: Transport Layer Reliability**

**Διδακτική Ενότητα 5: The Transport Layer Summary**

## Θεματική Ενότητα - Network Services

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: DHCP**

**Διδακτική Ενότητα 3: DNS**

**Διδακτική Ενότητα 4: NAT**

**Διδακτική Ενότητα 5: File Transfer and Sharing Services**

**Διδακτική Ενότητα 6: Email**

**Διδακτική Ενότητα 7: HTTP**

**Διδακτική Ενότητα 8: Network Services Summary**

## Θεματική Ενότητα - Network Communication Devices

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Network Devices**

**Διδακτική Ενότητα 3: Wireless Communications**

**Διδακτική Ενότητα 4: Network Communication Devices Summary**

## Θεματική Ενότητα - Network Security Infrastructure

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Network Topologies**

**Διδακτική Ενότητα 3: Security Devices**

**Διδακτική Ενότητα 4: Security Services**

**Διδακτική Ενότητα 5: Network Security Infrastructure Summary**

## Θεματική Ενότητα - Attackers and Their Tools

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Who is Attacking Our Network?**

**Διδακτική Ενότητα 3: Threat Actor Tools**

**Διδακτική Ενότητα 4: Attackers and Their Tools Summary**

## Θεματική Ενότητα - Common Threats and Attacks

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Malware**

**Διδακτική Ενότητα 3: Common Network Attacks - Reconnaissance, Access, and Social Engineering**

**Διδακτική Ενότητα 4: Network Attacks - Denial of Service, Buffer Overflows, and Evasion**

**Διδακτική Ενότητα 5: Using AI to Analyze Malware**

**Διδακτική Ενότητα 6: Common Threats and Attacks Summary**

## Θεματική Ενότητα - Network Monitoring and Tools

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Introduction to Network Monitoring**

**Διδακτική Ενότητα 3: Introduction to Network Monitoring Tools**

**Διδακτική Ενότητα 4: Network Monitoring and Tools Summary**

## Θεματική Ενότητα - Attacking the Foundation

**Διδακτική 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 What We Do

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: IP Services**

**Διδακτική Ενότητα 3: Enterprise Services**

**Διδακτική Ενότητα 4: Attacking What We Do Summary**

## Θεματική Ενότητα - Understanding Defense

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Defense-in-Depth**

**Διδακτική Ενότητα 3: Security Policies, Regulations, and Standards**

**Διδακτική Ενότητα 4: Understanding Defense Summary**

## Θεματική Ενότητα - Access Control

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Access Control Concepts**

**Διδακτική Ενότητα 3: AAA Usage and Operation**

**Διδακτική Ενότητα 4: Access Control 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 - Cryptography

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Integrity and Authenticity**

**Διδακτική Ενότητα 3: Confidentiality**

**Διδακτική Ενότητα 4: Public Key Cryptography**

**Διδακτική Ενότητα 5: Authorities and the PKI Trust System**

**Διδακτική Ενότητα 6: Applications and Impacts of Cryptography**

**Διδακτική Ενότητα 7: Cryptography Summary**

## Θεματική Ενότητα - Endpoint Protection

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: Antimalware Protection**

**Διδακτική Ενότητα 3: Host-Based Intrusion Prevention**

**Διδακτική Ενότητα 4: Application Security**

**Διδακτική Ενότητα 5: Endpoint Security**

**Διδακτική Ενότητα 6: Endpoint Protection 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: Information Security Management Systems**

**Διδακτική Ενότητα 6: Endpoint Vulnerability Assessment 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 - Working with Network Security Data

**Διδακτική Ενότητα 1: Introduction**

**Διδακτική Ενότητα 2: A Common Data Platform**

**Διδακτική Ενότητα 3: Investigating Network Data**

**Διδακτική Ενότητα 4: Enhancing the Work of the Cybersecurity Analyst**

**Διδακτική Ενότητα 5: Working with Network Security Data 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: Digital Forensics and Incident Analysis and Response Summary**

**Διδακτική Ενότητα 7: Prepare for Your Exam and Launch Your Career!**

## 9. ΥΠΟΔΕΙΓΜΑ ΧΟΡΗΓΟΥΜΕΝΗΣ ΒΕΒΑΙΩΣΗΣ



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
Εθνικών και Καποδιστριακών  
Πανεπιστημίων Αθηνών  
ΔΙΕΥΘΥΝΣΗ ΤΩ ΝΕΤ



Ημερομηνία .....

### ΒΕΒΑΙΩΣΗ ΣΥΜΜΕΤΟΧΗΣ

O/H .....

Παρακολούθησε επιτυχώς  
το εξ αποστάσεως Επιμορφωτικό Πρόγραμμα με τίτλο:

**«CyberOps Associate»**

από ..... έως .....

Το πρόγραμμα υλοποιήθηκε μέσω της επίσημης εκπαιδευτικής πλατφόρμας της Cisco, με τη μεθοδολογία και τη χρήση εγκεκριμένου εκπαιδευτικού υλικού της Cisco, στο πλαίσιο του Προγράμματος Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης E-Learning του Κ.Ε.ΔΙ.ΒΙ.Μ. του Ε.Κ.Π.Α., το οποίο λειτουργεί ως «Επίσημη Ακαδημία» της Cisco με την επωνυμία «E-Learning NKUA».

Ο Επιστημονικός Υπεύθυνος του Προγράμματος  
Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης (E-learning)

**Παναγιώτης Ε. Πετράκης**  
Ομ. Καθηγητής  
Τμήμα Οικονομικών Επιστημών Ε.Κ.Π.Α.