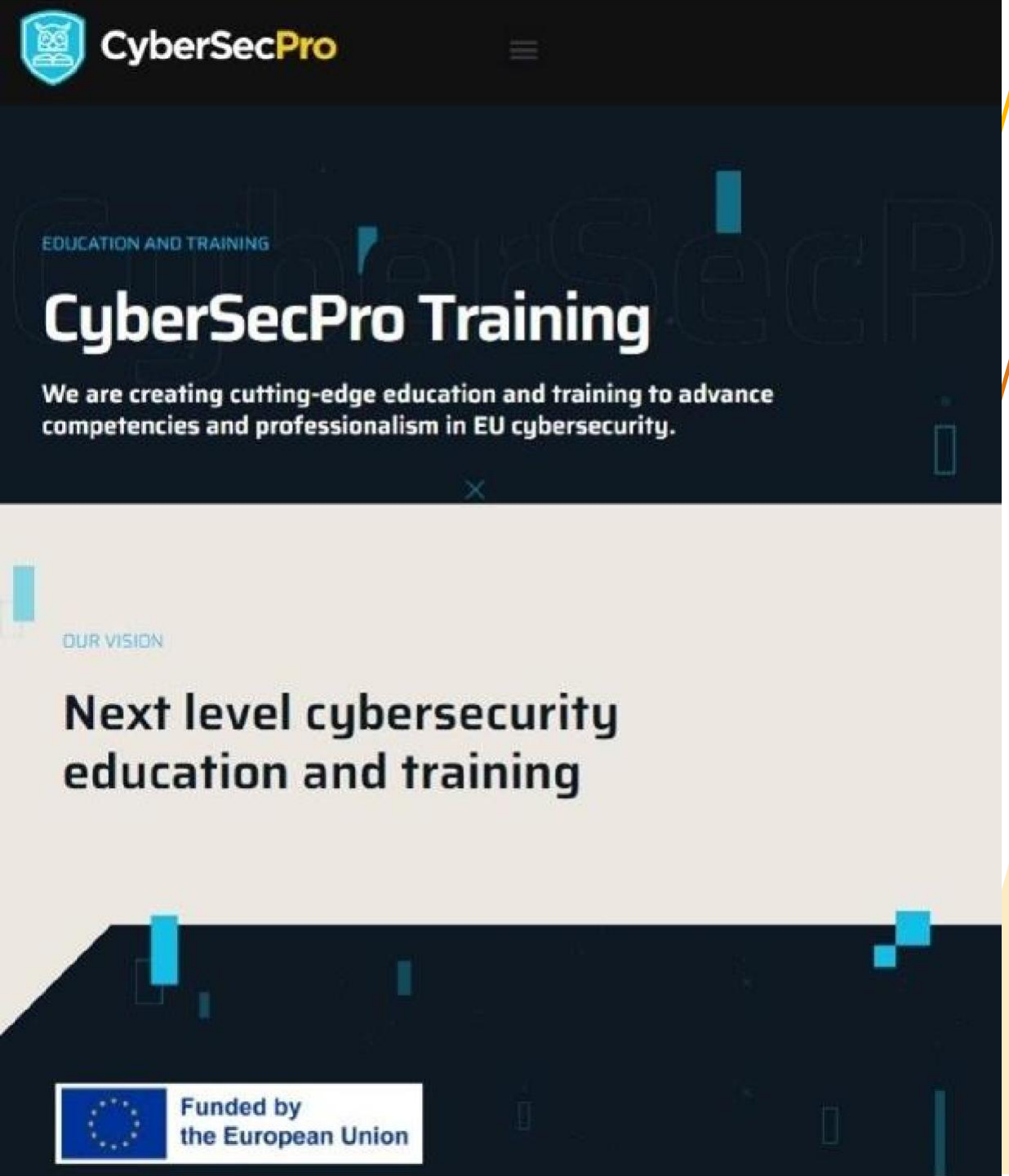


Ψηφιακή εγκληματολογία στον τομέα της υγείας

CSP_012_SA_H

ΠΑΡΟΥΣΊΑΣΗ ΑΠΌ: ΟΝΟΜΑΣΜΕΝΟΙ ΕΚΠΑΙΔΕΥΤΏΝ

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Τεχνολογίες προστασίας δεδομένων και απορρήτου στην υγειονομική περίθαλψη

o1. Στόχοι: Ποιος – Τι – Γιατί χρειάζεται να παρακολουθήσετε αυτή την εκπαίδευση

o2. Οργανωτικά στοιχεία εκπαίδευσης: Πότε – Πού – Πώς

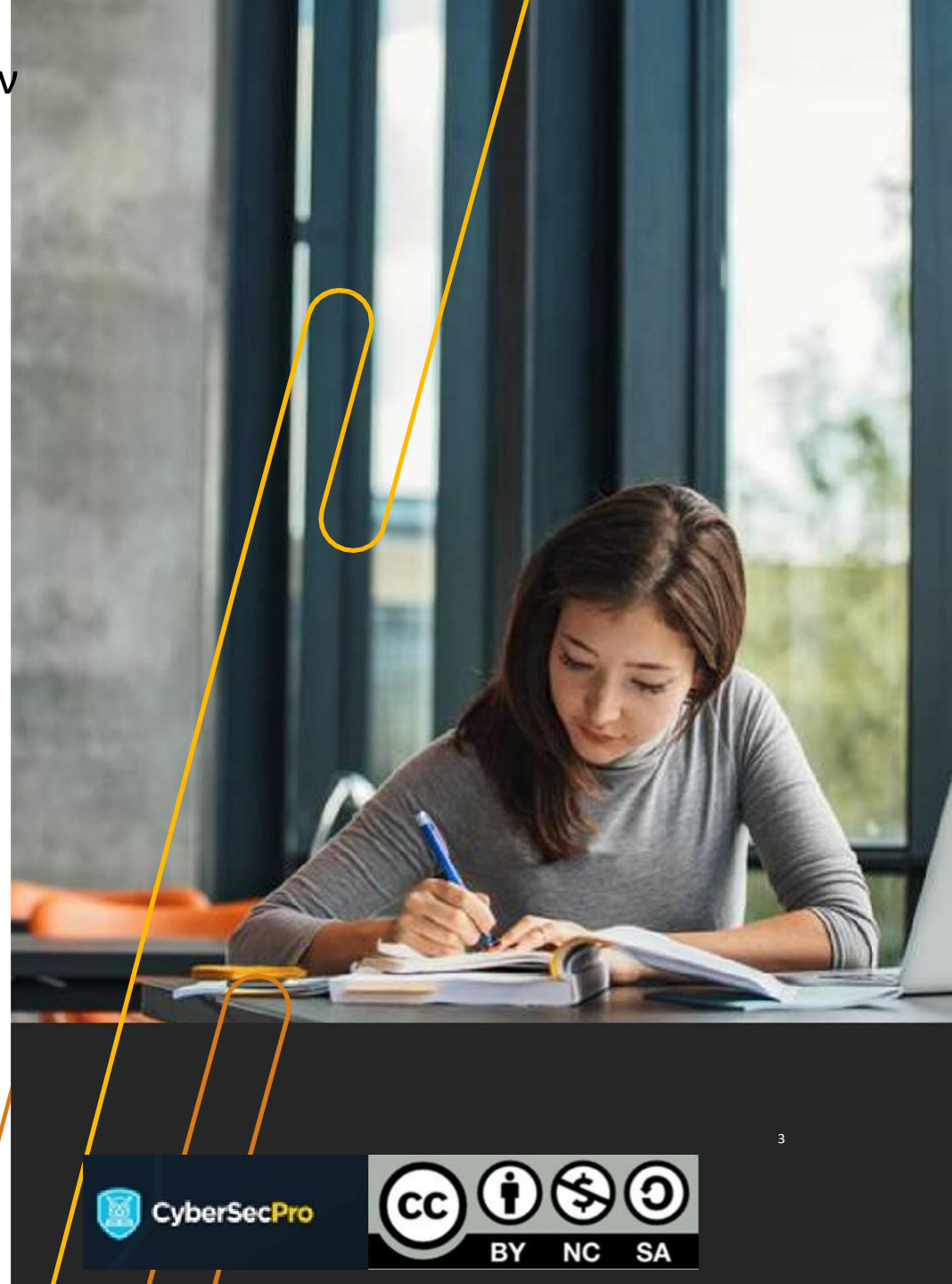
o3. Μαθησιακά αποτελέσματα

o4. Δομή εκπαίδευσης

o5. Λεπτομέρειες ασκήσεων

o6. Πρακτικές πληροφορίες και απαιτήσεις

o7. Πληροφορίες εγγραφής και στοιχεία επικοινωνίας

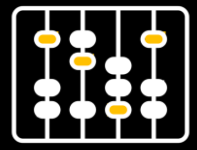


Στόχοι: Να αποκτήσετε επάρκεια στην ανάλυση δεδομένων, να συνθέσετε χρονοδιαγράμματα συμβάντων και να εκτελέσετε διαδικασίες εγκατάστασης και εκτέλεσης εφαρμογών σε περιβάλλον παραγωγής.

ΠΟΙΟΣ

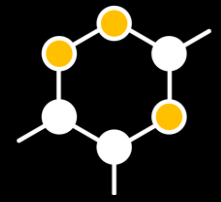
Για την εγγραφή δεν απαιτείται τεχνικό υπόβαθρο. Αυτό το μάθημα καλύπτει βασικά και προχωρημένα θέματα που απευθύνονται σε κάθε ενθουσιώδη χρήστη (άτομα με ενδιαφέρον σε νέα τεχνολογία).

ΤΙ



Μάθετε τα θεμέλια της ψηφιακής εγκληματολογίας και πώς επηρεάζουν τον τομέα της υγείας με πραγματικά σενάρια.

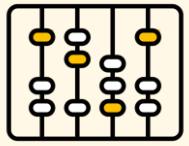
ΓΙΑΤΙ



Οι συμμετέχοντες θα αποκτήσουν τις πρώτες γνώσεις σχετικά με τον τρόπο προστασίας των περιουσιακών τους στοιχείων για την αποτροπή μελλοντικών περιστατικών.

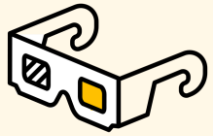
CSP Εκπαίδευση Λογιστική: Πότε-Πού-Πώς

ΠΟΤΕ



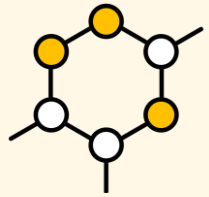
Χρονοπρόγραμμα: 2024

ΠΟΥ



TBD

ΠΩΣ



Βιντεοεπιδείξεις και ζωντανά διαδικτυακά εργαστήρια με ρεαλιστικά σενάρια.

Οφέλη για τους συμμετέχοντες

- Επίπεδο εκπαιδευτικής ενότητας: Ενότητα καλύπτει τόσο βασικά όσο και προχωρημένα σενάρια.
- Επαγγελματική κατάρτιση από επαγγελματίες ασφαλείας
- Προγραμματισμός και Ανάπτυξη Λογισμικού
- Ρίζες στο ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας
- Γνωριμίες αιχμής από ειδικούς του κλάδου και ακαδημαϊκούς εμπειρογνώμονες
- Αποκτήστε πρακτική εμπειρία σε ρεαλιστικά και παραγωγικά σενάρια.

ΠΟΙΟΣ

Προφίλ των συμμετεχόντων στην κατάρτιση

- Διευθυντές και ηγέτες
- Επαγγελματίες κυβερνοασφάλειας
- Ενθουσιώδεις χρήστες (άτομα με ενδιαφέρον σε νέα τεχνολογία)
- Όποιος θέλει να μάθει

ΠΟΙΟΣ

Εκπαιδευτής: Θάνος Αποστολίδης

- Προγραμματιστής λογισμικού αναλυτής ασφάλειας Zelus
- Λάτρης της ασφάλειας στον κυβερνοχώρο
- Ανταγωνιστικός παίκτης του "Capture Flag (CTF)".

TI

Θέματα κατάρτισης

- Εισαγωγή στην ψηφιακή εγκληματολογία
- Απειλές και Ευπάθειες στον κυβερνοχώρο στην υγειονομική περίθαλψη
- Περίπτωση χρήσης έρευνας ψηφιακής εγκληματολογίας
- Προετοιμασία, αντίδραση και ανθεκτικότητα

ΓΙΑΤΙ

Μαθησιακά αποτελέσματα

- Ενημερωθείτε για τους ορισμούς και τις μεθοδολογίες που χρησιμοποιούνται στην ψηφιακή εγκληματολογία.
- Μάθετε για το τοπίο των απειλών στον κυβερνοχώρο που αντιμετωπίζει η υγειονομική περίθαλψη μαζί με τα κοινά Ευπάθεια.
- Αποκτήστε γνώσεις από ρεαλιστικές βήμα προς βήμα επιδείξεις με τη χρήση εργαλείων οπτικοποίησης εγκληματολογίας.
- Μάθετε τις βέλτιστες πρακτικές που αποσκοπούν στην ενίσχυση της κατάστασης κυβερνοασφάλειας των ICT (Information and Communication Technology - Τεχνολογίες Πληροφορικής και Επικοινωνιών) στον τομέα της υγειονομικής περίθαλψης.

Περίγραμμα εκπαίδευσης

Ημέρα 1

Θέμα-1: Εισαγωγή στην ψηφιακή εγκληματολογία

Εισαγωγή στους ορισμούς και τις μεθοδολογίες που χρησιμοποιούνται στην ψηφιακή εγκληματολογία

Θέμα-2: Απειλές και Ευπάθειες στον κυβερνοχώρο στην Υγεία

Επισκόπηση του τοπίου των νήματα στον κυβερνοχώρο που είναι πρόσωπα (face recognition - αναγνώριση προσώπου μέσω TN όπως Face ID)
υγειονομική περίθαλψη μαζί με τα κοινά ευάλωτα σημεία.

Περίγραμμα εκπαίδευσης: Ημέρα-2

Θέμα-3: χρήσης μιας ψηφιακής έρευνας εγκληματολογίας

Επισκόπηση και πρακτικές επιδείξεις σε ρεαλιστικά περιστατικά στον τομέα της υγείας, ακολουθούμενες από βήμα προς βήμα προσέγγιση για την ανάλυση και τον μετριασμό των απειλών με εργαλεία οπτικοποίησης.

Θέμα-4: Προετοιμασία, αντίδραση και ανθεκτικότητα

Εισαγωγή στις βέλτιστες πρακτικές που αποσκοπούν στην ενίσχυση της ασφάλειας στον κυβερνοχώρο στάση των ICT (Information and Communication Technology - Τεχνολ περίθαλψης.

Περίγραμμα κατάρτισης: Ημέρα-3

Πρακτικές ασκήσεις: Χρήση περιπτώσεων ψηφιακής έρευνας εγκληματολογίας

- **Προσομοίωση έρευνας παραβίασης δεδομένων:** Δοκιμαστικό σεναριολόγιο για την έρευνα σεναρίου παραβίασης δεδομένων σε μια οργάνωση υγειονομικής περίθαλψης. Προσδιορίστε το σημείο εισόδου, αναλύστε τα παραβιασμένα συστήματα και τεκμηριώστε τα ευρήματα.

- **Άσκηση ανάλυσης κακόβουλου λογισμικού:** Αναλύστε ένα κομμάτι κακόβουλου λογισμικού που ανακαλύφθηκε σε δίκτυο υγειονομικής περίθαλψης. Χρησιμοποιήστε εγκληματολογικά εργαλεία για να αναλύσετε το κακόβουλο λογισμικό, να κατανοήσετε τη συμπεριφορά του και τον αντίκτυπό του δεδομένα των ασθενών.

- **Άσκηση ανάκτησης διαγραμμένων αρχείων:** Αποδώστε πρακτική άσκηση ανάκτησης διαγραμμένων αρχείων από ψηφιακή συσκευή που χρησιμοποιείται σε περιβάλλον υγειονομικής περίθαλψης. Επικυρώστε τα ανακτηθέντα δεδομένα για να διασφαλίσετε την ολοκλήρωσή τους και τη σχετικότητά τους με την έρευνα.

- **Ιατροδικαστική απεικόνιση ψηφιακών συσκευών:** Δημιουργία εγκληματολογικών εικόνων διαφόρων ψηφιακών συσκευών που χρησιμοποιούνται συνήθως στην υγειονομική περίθαλψη, όπως υπολογιστές και κινητές συσκευές. Διασφαλίστε ότι η διαδικασία εικόνας ακολουθεί τις βέλτιστες πρακτικές για τη συντήρηση της ακεραιότητας των αποδεικτικών στοιχείων.

Θέμα-1: Εισαγωγή στην ψηφιακή εγκληματολογία

Θα καλύψουμε αυτές τις δεξιότητες

- Εισαγωγή στην ψηφιακή εγκληματολογία, ορισμοί και μεθοδολογίες.
- **Συλλογή και διατήρηση αποδεικτικών στοιχείων:** Μάθετε τις βέλτιστες πρακτικές για τον εντοπισμό, τη συλλογή και τη διατήρηση ψηφιακών αποδεικτικών στοιχείων
- **Ανάκτηση και ανάλυση δεδομένων:** Απόκτηση δεξιοτήτων ανάκτησης διαγραμμένων ή κατεστραμμένων δεδομένων από διάφορες ψηφιακές συσκευές και την ανάλυσή τους για σχετικές πληροφορίες.
- **Εγκληματολογικά εργαλεία και τεχνικές:** Αποκτήστε πρακτική εμπειρία με τα πρότυπα εργαλεία και τεχνικές ψηφιακής εγκληματολογίας που χρησιμοποιούνται για τη διερεύνηση εγκλημάτων στον κυβερνοχώρο.
- **Νομικά και ηθικά ζητήματα:** Κατανόηση των πλαισίων λογισμικού, των ζητημάτων δεοντολογίας και των κατευθυντήριων γραμμών που διέπουν τις ψηφιακές εγκληματολογικές έρευνες, διασφαλίζοντας τη συμμόρφωση με τους νόμους και τα επαγγελματικά πρότυπα.

Θέμα-2:

Απειλές και Ευπάθειες στον κυβερνοχώρο στην υγειονομική περίθαλψη

Θα καλύψουμε αυτές τις δεξιότητες

- **Προσδιορισμός κοινών απειλών στον κυβερνοχώρο:** Μάθετε να αναγνωρίζετε και να κατανοείτε τους διάφορους τύπους απειλών στον κυβερνοχώρο που στοχεύουν ειδικά τα συστήματα υγειονομικής περίθαλψης, όπως Ransomware, Phishing και Insider Threats.
- **Ευπά:** Αποκτήστε δεξιότητες για τη διενέργεια διεξοδικών αξιολογήσεων ευπάθειας για τον εντοπισμό αδυναμιών στις υποδομές ΤΠ της υγειονομικής περίθαλψης που θα μπορούσαν να εκμεταλλευτούν από επιτιθέμενους στον κυβερνοχώρο.
- **Υλοποίηση μέτρων ασφαλείας:** Κατανόηση και εφαρμογή βέλτιστων πρακτικών για την υλοποίηση ισχυρών μέτρων ασφαλείας, συμπεριλαμβανομένης της κρυπτογράφησης, των ελέγχων πρόσβασης και της ασφάλειας δικτύου, για την προστασία ευαίσθητων δεδομένων υγειονομικής περίθαλψης.
- **Αντιμετώπιση και διαχείριση περιστατικών:** Ανάπτυξη λογισμικού για την αποτελεσματική αντιμετώπιση και διαχείριση περιστατικών κυβερνοασφάλειας, συμπεριλαμβανομένης της ανίχνευσης παραβιάσεων, του μετριασμού των ζημιών και της εξασφάλισης ταχείας ανάκαμψης για τη διατήρηση των υπηρεσιών υγειονομικής περίθαλψης.

Θέμα-3:
Περιπτώσεις χρήσης μιας ψηφιακής έρευνας εγκληματολογίας

Θα καλύψουμε αυτές τις δεξιότητες

- **Διερεύνηση παραβιάσεων δεδομένων:** Μάθετε πώς να διεξάγετε διεξοδικές έρευνες για παραβιάσεις δεδομένων, συμπεριλαμβανομένου του εντοπισμού της πηγής, της μεθόδου επίθεσης και της έκτασης των δεδομένων που έχουν τεθεί σε κίνδυνο.
- **Αναλύοντας επιθέσεις κακόβουλου λογισμικού:** Αποκτήστε δεξιότητες στην ανάλυση και κατανόηση κακόβουλου λογισμικού, εντοπίζοντας την προέλευση, τη συμπεριφορά και τον αντίκτυπο στα επηρεαζόμενα συστήματα για την πρόληψη μελλοντικών επιθέσεων.
- **Ανάκτηση διαγραμμένων αρχείων:** τεχνικές ανάκτησης και ανάλυσης διαγραμμένων, κρυμμένων ή αρχείων για την αποκάλυψη κρίσιμων στοιχείων κατά τη διάρκεια ψηφιακών εγκληματολογικών ερευνών.
- **Εξέταση ψηφιακών συσκευών:** Προγραμματισμός λογισμικού για την εξέταση διαφόρων ψηφιακών συσκευών, όπως υπολογιστές, κινητά τηλέφωνα και συσκευές IoT, για την εξαγωγή και ανάλυση αποδεικτικών στοιχείων σχετικών με ποινικές έρευνες και νομικές υποθέσεις.

Θέμα-4:

Προετοιμασία, αντίδραση και ανθεκτικότητα

Θα καλύψουμε αυτές τις δεξιότητες

- **Προγραμματισμός λογισμικού αντιμετώπισης περιστατικών:** Μάθετε να δημιουργείτε ολοκληρωμένα σχέδια αντιμετώπισης περιστατικών που περιγράφουν τα βήματα που πρέπει να ακολουθηθούν όταν συμβεί ένα περιστατικό κυβερνοασφάλειας, εξασφαλίζοντας γρήγορη και αποτελεσματική δράση.
- **Διεξαγωγή εκτιμήσεων κινδύνου:** Αποκτήστε δεξιότητες στην επίδοση λεπτομερών αξιολογήσεων κινδύνου για τον εντοπισμό δυνητικών απειλών και ευπαθειών, βοηθώντας στην ιεράρχηση των προσπαθειών και των πόρων ασφάλειας.
- **Οικοδόμηση ανθεκτικότητας στον κυβερνοχώρο:** Κατανοήστε τις στρατηγικές για την οικοδόμηση ανθεκτικότητας στον κυβερνοχώρο σε μια οργάνωση, εστιάζοντας στην ικανότητα γρήγορης και αποτελεσματικής ανάκαμψης από επιθέσεις και ανατροπές .

Πρακτικές ασκήσεις κατάρτισης

Πρακτικές ασκήσεις που απαιτούν τόσο προσωπική όσο και ομαδική προσπάθεια

	Τίτλος	Στόχος της άσκησης
Άσκηση-1 Ημέρα-3)	**Προσομοίωση έρευνας παραβίασης δεδομένων**	Δοκιμάστε μια δοκιμαστική έρευνα ενός σεναρίου παραβίασης δεδομένων σε μια οργάνωση υγειονομικής περίθαλψης. Προσδιορίστε το σημείο εισόδου, αναλύστε τα παραβιασμένα συστήματα και τεκμηριώστε τα ευρήματα
Άσκηση-2 Ημέρα-3)	**Άσκηση ανάλυσης κακόβουλου λογισμικού**	Αναλύστε ένα κομμάτι κακόβουλου λογισμικού που ανακαλύφθηκε σε ένα δίκτυο υγειονομικής περίθαλψης. Χρησιμοποιήστε εγκληματολογικά εργαλεία για να αναλύσετε το κακόβουλο λογισμικό, να κατανοήσετε τη συμπεριφορά του και να προσδιορίσετε τον αντίκτυπό του στα δεδομένα των ασθενών.
Άσκηση-3 Ημέρα-3)	**Άσκηση ανάκτησης διαγραμμένων αρχείων**	Αποδώστε μια πρακτική άσκηση ανάκτησης διαγραμμένων αρχείων από μια ψηφιακή συσκευή που χρησιμοποιείται σε ρυθμίσεις υγειονομικής περίθαλψης. Επικυρώστε τα ανακτηθέντα δεδομένα για να διασφαλίσετε την ολοκλήρωσή τους και τη σχετικότητά τους με την έρευνα.
Άσκηση-4 Ημέρα-3)	**Ιατροδικαστική απεικόνιση ψηφιακών συσκευών**	Δημιουργία εγκληματολογικών εικόνων διαφόρων ψηφιακών συσκευών που χρησιμοποιούνται συνήθως στην υγειονομική περίθαλψη, όπως υπολογιστές και κινητές συσκευές. Διασφαλίστε ότι η διαδικασία εικόνας ακολουθεί τις βέλτιστες πρακτικές για τη διατήρηση της ολοκλήρωσης των αποδεικτικών στοιχείων.

Μέθοδος αξιολόγησης

Περιγραφή των στοιχείων αξιολόγησης και τη διαδικασία αξιολόγησης

Στοιχεία αξιολόγησης	Πώς
Πολλαπλή επιλογή Κουίζ	Διαδικτυακά κουίζ
Εφαρμοσμένες εργασίες (ατομικές)	Η λύση του προβλήματος θα υποβληθεί αργότερα
Ομαδική συζήτηση	Κατά τη διάρκεια του εργαστηρίου

Ιστορική γνώση και προαπαιτούμενα

Γνώσεις υποβάθρου:

Η βασική κατανόηση των υπολογιστών και της δικτύωσης είναι ευπρόσδεκτη, αλλά δεν απαιτείται.

Προαπαιτούμενα:

Κανένα/δεν ορίζεται

CSP_012_SA_H: Ψηφιακή εγκληματολογία στον τομέα της υγείας

Τεχνικά εργαλεία και άλλες απαιτήσεις

Τεχνικά εργαλεία

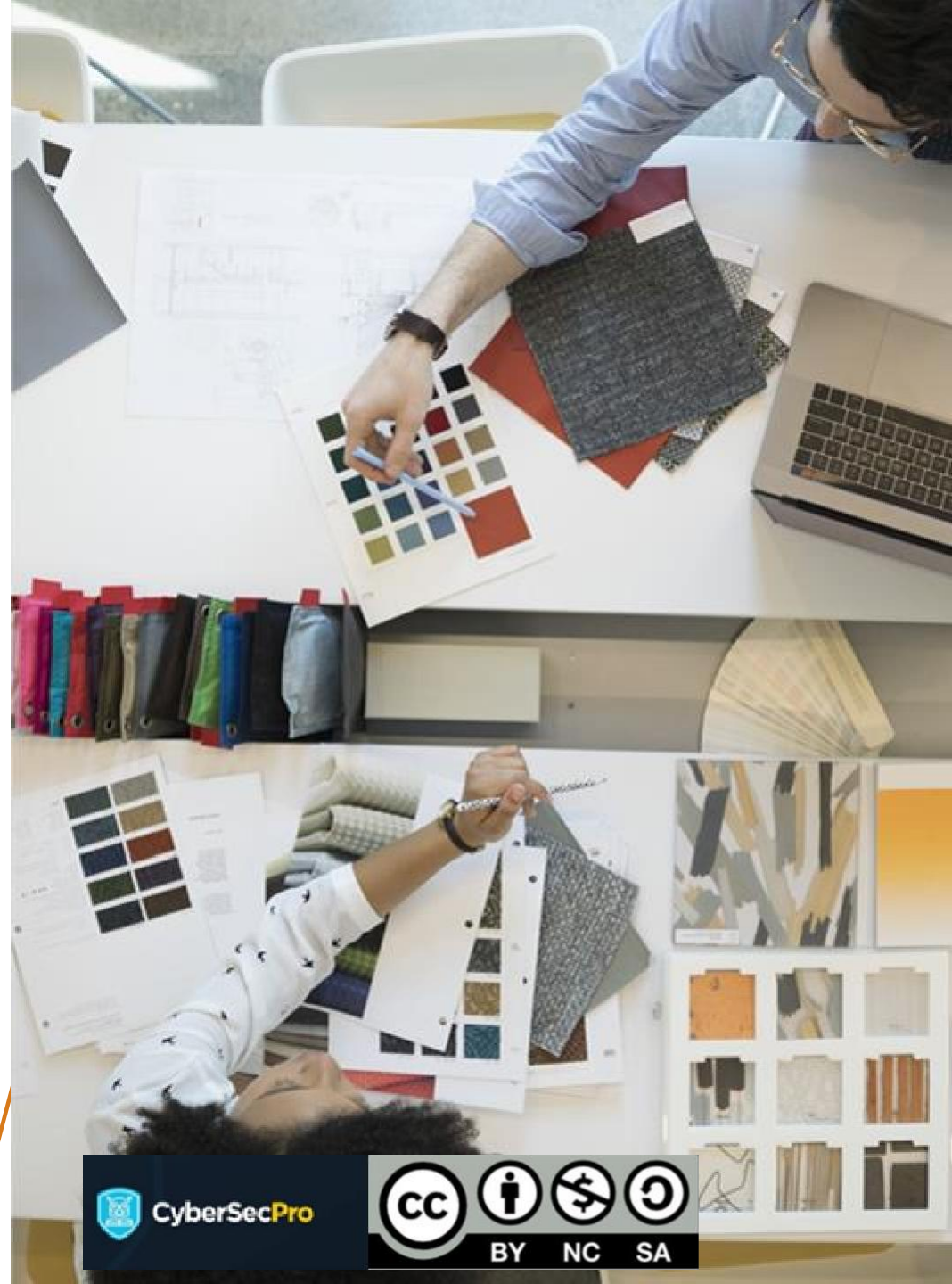
Υπολογιστής με πρόσβαση στο Ίντερνετ

Πρόσβαση στο πρόγραμμα περιήγησης στο Web

Τεχνικά εργαλεία: Kali Linux

Άλλες απαιτήσεις

Προθυμία για μάθηση και πειραματισμό Δραστηριότητα



Εγγραφή: Πώς να εγγραφείτε και άλλες πρακτικές πληροφορίες

Η συγκεκριμένη διαδικασία εγγραφής για την κατάρτιση "Ψηφιακή εγκληματολογία στον τομέα της υγείας" μπορεί να διαφέρει ανάλογα με τον πάροχο κατάρτισης ή το θεσμικό όργανο. Ωστόσο, τα γενικά βήματα είναι συνήθως απλά και μπορούν να ολοκληρωθούν διαδικτυακά ή αυτοπροσώπως.

1. Διαδικτυακή εγγραφή
2. Προσωπική εγγραφή

Σας ευχαριστώ

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση:
t.apostolidis@zelus.gr

CyberSecPro