Ψηφιακή εγκληματολογία στην ενέργεια

CSP012_S_E

ΠΑΡΟΥΣΊΑΣΗ ΑΠΌ:

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

Ψηφιακή Εγκληματολογία στη Ναυτιλία

Περίγραμμα κατάρτισης:

Θέμα-01 - Εισαγωγή στην ψηφιακή εγκληματολογία

Κατανόηση της ψηφιακής εγκληματολογίας

Οφέλη και διαδικασία της ψηφιακής εγκληματολογίας

Λεπτομερής διαδικασία ψηφιακής εγκληματολογίας

Σενάριο περίπτωσης χρήσης

1. Εισαγωγή στην ψηφιακή εγκληματολογία

Πλαίσιο

- Ορισμός της ψηφιακής εγκληματολογίας
- Σημασία στον τομέα της ενέργειας
- Βασικοί στόχοι της ψηφιακής εγκληματολογίας

2. Οφέλη και διαδικασία της ψηφιακής εγκληματολογίας

Πλαίσιο

- Οφέλη: Προστατεύει κρίσιμες υποδομές, βοηθά σε νομικές διαδικασίες, υποστηρίζει μέτρα κυβερνοασφάλειας
- Επισκόπηση της διαδικασίας:
- Αναγνώριση
- Διατήρηση
- Ανάλυση
- Παρουσίαση

3. Διαδικασία ψηφιακής εγκληματολογίας λεπτομερώς

Πλαίσιο

- Αναγνώριση: Εντοπισμός ψηφιακών αποδεικτικών στοιχείων.
- Διατήρηση: Ασφαλές: Διασφάλιση των αποδεικτικών στοιχείων.
- Συλλογή: Συλλογή ψηφιακών αποδεικτικών στοιχείων.
- Εξέταση: Αναλύοντας τα αποδεικτικά στοιχεία.
- Ανάλυση: Ερμηνεία δεδομένων.
- Παρουσίαση: Αναφορά ευρημάτων.

4. Περίπτωση χρήσης: στον τομέα της ενέργειας

Πλαίσιο

- Σενάριο: Εντοπίστηκε ανεξουσιοδοτημένη πρόσβαση σε ένα έξυπνο δίκτυο.
- Μέτρα που έχουν ληφθεί: Ταυτοποίηση, διατήρηση, συλλογή, εξέταση, ανάλυση και παρουσίαση των αποδεικτικών στοιχείων.

Περίγραμμα κατάρτισης:

Θέμα-02 - Εργαλεία Ψηφιακής Εγκληματολογίας στον Ενεργειακό Τομέα

Εργαλεία υλικού για ψηφιακή
Εγκληματολογία Εργαλεία λογισμικού
για ψηφιακή εγκληματολογία
Επικύρωση εργαλείων
Διασφάλιση ποιότητας στην ψηφιακή εγκληματολογία
Σενάριο περίπτωσης χρήσης

1. Εργαλεία υλικού για την ψηφιακή εγκληματολογία

Πλαίσιο

- Σημασία των εργαλείων υλικού
- Τύποι εργαλείων υλικού: Μπλοκαδόροι εγγραφής, ιατροδικαστικές συσκευές αντιγραφής, συσκευές ανάκτησης δεδομένων

2. Εργαλεία λογισμικού για την ψηφιακή εγκληματολογία

Πλαίσιο

- Σημασία των εργαλείων λογισμικού
- Τύποι εργαλείων λογισμικού: FTK (Forensic Toolkit - λογισμικό ανάλυσης ψηφιακών εγκληματολογικών δεδομένων)
  ENCase (λογισμικό ψηφιακής εγκληματολογίας - forensics tool για ανάλυση δεδομένων και ψηφιακών πειστηρίων)

3. Επικύρωση των εγκληματολογικών εργαλείων

Πλαίσιο

- Ανάγκη για επικύρωση
- Μέθοδοι επικύρωσης: Δοκιμές σε ελεγχόμενα περιβάλλοντα, με διαφορετικά .

4. Διασφάλιση ποιότητας στην ενεργειακή ψηφιακή εγκληματολογία

Πλαίσιο

- Σημασία της Διασφάλισης Ποιότητας
- Βήματα για τη διασφάλιση της ποιότητας: Λειτουργικά πρότυπα, τακτική βαθμονόμηση εργαλείων, συνεχής εκπαίδευση.

5. Περίπτωση χρήσης: Επικύρωση εργαλείων και διασφάλιση ποιότητας

Πλαίσιο

- Σενάριο: SC.
- Μέτρα που έχουν ληφθεί: Επιλογή εργαλείων, ελεγχόμενες δοκιμές,
  υλοποίηση των διαδικασιών QA.

Περίγραμμα κατάρτισης:

Θέμα-03 - Συλλογή Δεδομένων / Πειστηρίων

Κατανόηση των μορφότυπων

αποθήκευσης δεδομένων/επικτήσεων

Επικτήσεις εργαλεία και μέθοδοι

Επικύρωση της επικτήσης

Περίπτωση χρήσης: Grid: Επικτήσεις σε περιστατικό έξυπνου δικτύου

1. Εισαγωγή στην επικτήση δεδομένων/αποδεικτικών στοιχείων

Πλαίσιο

- Ορισμός της ψηφιακής επικτήσης στην ψηφιακή εγκληματολογία
- Σημασία στον τομέα της ενέργειας
- Βασικοί στόχοι

2. Μορφές αποθήκευσης δεδομένων

Πλαίσιο

- Κοινές μορφές: FAT32, NTFS New Technology File System - σύστημα αρχείων των Windows) .λπ.
- Ειδικές μορφές για τον τομέα της ενέργειας: ADA, δεδομένα έξυπνων μετρητών

3. Επικτήσεις εργαλεία και μέθοδοι

Πλαίσιο

- Εργαλεία: FTK (Forensic Toolkit - λογισμικό ανάλυσης ψηφιακών εγκληματολογικών δεδομένων)
- Μέθοδοι: επικτήσεις, στατική απόκτηση

4. Επικύρωση της επικτήσης

Πλαίσιο

- Σημασία της επικύρωσης
- Τεχνικές: MD5, SHA-1), cross-επαλήθευση

5. Περίπτωση χρήσης: Grid: Επικτήσεις σε περιστατικό έξυπνου δικτύου

Πλαίσιο

- Σενάριο: σε έξυπνο δίκτυο δικτύου
- Μέτρα που έχουν ληφθεί: Αναγνώριση δεδομένων, επικτήσεις
  χρησιμοποιώντας FTK (Forensic Toolkit - άλυσης ψηφιακών εγκληματολογικών δεδομένων)

Περίγραμμα κατάρτισης:

Θέμα-04 - Νομικές Διαστάσεις της Ψηφιακής Εγκληματολογίας

Εισαγωγή στις νομικές
πτυχές Νόμοι και κανονισμοί
Νομικός αντίκτυπος
Συντήρηση της αλυσίδας φύλαξης
Περίπτωση χρήσης: Νομική συμμόρφωση σε εγκληματολογικές έρευνες

1. Εισαγωγή στις νομικές πτυχές

Πλαίσιο

- Σημασία των νομικών γνώσεων στην ψηφιακή εγκληματολογία
- Βασικές νομικές αρχές: Παραδεκτό, επιμέλεια

2. Νόμοι και κανονισμοί

Πλαίσιο

- Εθνικοί νόμοι: Νόμοι για την ασφάλεια στον κυβερνοχώρο, νόμοι για την προστασία των δεδομένων
- Διεθνή πρότυπα: GDPR, ISO/IEC

3. Νομικός αντίκτυπος

Πλαίσιο

- Επιρροή στη συλλογή αποδεικτικών στοιχείων
- Επιρροή στην ανάλυση και την αναφορά

4. Συντήρηση της αλυσίδας φύλαξης

Πλαίσιο

- Ορισμός και σημασία
- Βήματα: Βήματα: Τεκμηρίωση, ασφαλές αποθηκευτικό σύστημα, ελεγχόμενη πρόσβαση

4. Συντήρηση της αλυσίδας φύλαξης

Πλαίσιο

- Σενάριο: Διερεύνηση παραβίασης σε εταιρεία ενέργειας
- Μέτρα που έχουν ληφθεί: Συλλογή αποδεικτικών στοιχείων, συντήρηση αλυσίδα επιτήρησης, τεκμηρίωση

Περίγραμμα κατάρτισης:

Θέμα-05 - Αναλύσεις Ψηφιακής Εγκληματολογίας

Εισαγωγή στις αναλύσεις ψηφιακής εγκληματολογίας Ανάλυση κακόβουλου λογισμικού
Ανάλυση πτητικής μνήμης Ανάλυση χρονοδιαγράμματος
Ανάλυση εισβολής
Περίπτωση χρήσης: Ανάλυση εισβολής σε σύστημα

1. Εισαγωγή στις αναλύσεις ψηφιακών εγκλημάτων

Πλαίσιο

- Ορισμός και σημασία
- Βασικοί τομείς: Ανάλυση κακόβουλου λογισμικού, πτητική μνήμη
  ανάλυση, ανάλυση χρονοδιαγράμματος, ανάλυση

2. Ανάλυση κακόβουλου λογισμικού

Πλαίσιο

- Ορισμός και τύποι κακόβουλου λογισμικού
- Τεχνικές ανάλυσης: Στατική ανάλυση, δυναμική ανάλυση

3. Ανάλυση πτητικής μνήμης

Πλαίσιο

- Σημασία της ανάλυσης RAM
- Εργαλεία και τεχνικές: Memoryze

4. Ανάλυση χρονοδιαγράμματος

Πλαίσιο

- Σκοπός και οφέλη
- Εργαλεία και μέθοδοι: Log2Timeline,

5. Ανάλυση εισβολής

Πλαίσιο

- Προσδιορισμός δεικτών συμβιβασμού IOC)
- Μέθοδοι: Μέθοδοι: Με βάση την υπογραφή, με βάση την ανωμαλία

6. Περίπτωση χρήσης: Ανάλυση εισβολής σε σύστημα SCADA

Πλαίσιο

- Σενάριο: Ανίχνευση και ανάλυση μιας εισβολής σε ένα δίκτυο SCADA
- Μέτρα που έχουν ληφθεί: της μεταβλητότητας και Log2Timeline για ανάλυση

Θέμα-06 - Έρευνα Πληροφοριακών Συστημάτων και Διαχείριση Ψηφιακών Εγκλημάτων

Εισαγωγή στην Υπολογιστική Εισαγωγή

στην Επιστήμη του Υπολογισμού

Μοντέλο διαδικασίας ψηφιακής

εγκληματολογίας

Τεκμηρίωση σκηνής και αποδεικτικών στοιχείων

Αλυσίδα φύλαξης

Κλωνοποίηση εγκληματολογικών στοιχείων

Ολοκληρώνω την ακεραιότητα των αποδεικτικών στοιχείων και των αναφορών

Περίπτωση χρήσης: Ενεργειακό έγκλημα στον κυβερνοχώρο

1. Εισαγωγή στην Υπολογιστική Έρευνα

Πλαίσιο

- Ορισμός και πεδίο εφαρμογής
- Σημασία στον τομέα της ενέργειας

2. Μοντέλο ψηφιακής εγκληματολογίας

Πλαίσιο

- Βήματα: Προετοιμασία, ταυτοποίηση, διατήρηση, συλλογή, εξέταση, ανάλυση, αναφορά

3. Τεκμηρίωση σκηνής και αποδεικτικών στοιχείων

Πλαίσιο

- Σημασία της ακριβούς τεκμηρίωσης
- Τεχνικές Φωτογραφικά στοιχεία, εγγραφές καταγραφές, φύλαξης

4. Αλυσίδα φύλαξης

Πλαίσιο

- Ορισμός και σημασία
- Βήματα: Αρχική συλλογή, μεταφορά, αποθήκευση,
παρουσίαση στο δικαστήριο

5. Κλωνοποίηση εγκληματολογικών στοιχείων

Πλαίσιο

- Ορισμός και σκοπός
- Εργαλεία: dd, FTK (Forensic Toolkit - λογισμικό ανάλυσης ψηφιακών εγκληματολογικών δεδομένων)

6. Ολοκληρώνω την ακεραιότητα των αποδεικτικών στοιχείων και των αναφορών

Πλαίσιο

- Διασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων
- Αποτελεσματική αναφορά: Σαφής, συνοπτική, τεκμηριωμένη

7. Περίπτωση χρήσης: Ενεργειακό έγκλημα στον κυβερνοχώρο

Πλαίσιο

- Σενάριο: Διερεύνηση επίθεσης στονστην υποδομή ΤΠ ενεργειακής εταιρείας
- Μέτρα που έχουν ληφθεί: Τεκμηρίωση σκηνής, αποδεικτικά στοιχεία
  συλλογή, κλωνοποίηση, αλυσίδα φύλαξης

Περίγραμμα κατάρτισης:

Θέμα-07 Δικτυακή Εγκληματολογία και Απόκριση σε Περιστατικά

Εισαγωγή στην εγκληματολογία δικτύου Διερεύνηση εισβολών σε ενεργειακό δίκτυο Διαδικασίες αντιμετώπισης περιστατικών

Συλλογή αποδεικτικών στοιχείων στην δικτυωμένη εγκληματολογία

Περίπτωση χρήσης: σε δίκτυο είναι δικτυωμένο

1. Εισαγωγή στην δικτυωμένη εγκληματολογία

Πλαίσιο

- Ορισμός και σημασία
- Βασικοί στόχοι στον τομέα της ενέργειας

2. Διερεύνηση εισβολών σε δίκτυα ενέργειας

Πλαίσιο

- Συνήθεις τύποι επιθέσεων δικτύου: DDoS, MITM, υποκλοπή πακέτων δεδομένων
- Τεχνικές ανίχνευσης: IDS (Intrusion Detection System - Σύστημα ανίχνευσης εισβολών) ανίχνευση

3. Διαδικασίες αντιμετώπισης περιστατικών

Πλαίσιο

- Βήματα: Εξάλειψη, αποκατάσταση, μάθηση

4. Συλλογή αποδεικτικών στοιχείων στην δικτυωμένη εγκληματολογία

Πλαίσιο

- Εργαλεία: Wireshark, Tcpdump (εργαλείο σύλληψης και ανάλυσης πακέτων δικτύου)
- Βέλτιστες πρακτικές: Διασφάλιση της ακεραιότητας των δεδομένων,
  διαδικασία συλλογής εγγράφων

5. Περίπτωση χρήσης: σε ένα δίκτυο που είναι δικτυωμένο

Πλαίσιο

- Σενάριο: σε δίκτυο έξυπνου δικτύου
- Μέτρα που έχουν ληφθεί: Χρήση IDS (Intrusion Detection System - Σύστημα ανίχνευσης εισβολών) για ανίχνευση,
  περιορισμός και ανάλυση με το Wireshark

Περίγραμμα κατάρτισης:

Θέμα-08 Σύνταξη και Παρουσίαση Πορισμάτων Ψηφιακής Εγκληματολογίας

Σημασία της αναφοράς στην ψηφιακή εγκληματολογία

Εγγραφή ολοκληρωμένων εγκληματολογικών εκθέσεων

Παρουσίαση ψηφιακών αποδεικτικών στοιχείων με αποτελεσματικό τρόπο

Οπτικοποίηση σύνθετων εγκληματολογικών δεδομένων

Περίπτωση χρήσης: Ενεργειακού Τομέα: Ιατροδικαστική αναφορά για περιστατικό στον κυβερνοχώρο

1. Σημασία της αναφοράς στην ψηφιακή εγκληματολογία

Πλαίσιο

- Ορισμός και σκοπός
- Σημασία σε νομικά και τεχνικά πλαίσια

2. Εγγραφή ολοκληρωμένων εγκληματολογικών αναφορών

Πλαίσιο

- Δομή: Συμπέρασμα: Περίληψη, μεθοδολογία, ευρήματα, συμπεράσματα, παραρτήματα
- Βέλτιστες πρακτικές: σαφήνεια, συντομία, ακρίβεια

3. Αποτελεσματική παρουσίαση ψηφιακών αποδεικτικών στοιχείων

Πλαίσιο

- Μέθοδοι: Οπτικά βοηθήματα, απλοποιημένες εξηγήσεις, εστίαση στα βασικά σημεία
- Εξέταση από το κοινό: Προσαρμογή της παρουσίασης σε τεχνικά και μη τεχνικά ακροατήρια

4. Οπτικοποίηση σύνθετων εγκληματολογικών δεδομένων

Πλαίσιο

- Εργαλεία: Γραφήματα, διαγράμματα,
- Παραδείγματα: Δίκτυα, χρονοδιαγράμματα

5. Περίπτωση χρήσης: Ενεργειακού Τομέα: Ιατροδικαστική αναφορά για περιστατικό στον κυβερνοχώρο

Πλαίσιο

- Σενάριο: Αναφορά σε επιθέσεις κακόβουλου λογισμικού σε σύστημα ελέγχου σταθμού παραγωγής ηλεκτρικής ενέργειας
- Μέτρα που έχουν ληφθεί: Δημιουργία ολοκληρωμένου αναφορά, οπτικά βοηθήματα για την παρουσίαση των ευρημάτων

Περίγραμμα κατάρτισης:

Θέμα-09 - Προχωρημένα Θέματα στην ψηφιακή εγκληματολογία

Εισαγωγή σε προχωρημένα θέματα στην ψηφιακή εγκληματολογία

Ψηφική εγκληματολογία νέφους

Ψηφιακή εγκληματολογία IoT

Αναδυόμενες τάσεις και προκλήσεις

Προηγμένες τεχνικές ψηφιακής εγκληματολογίας

Ψηφιακή εγκληματολογία νέφους και IoT στον τομέα της Ενέργειας

1. Εισαγωγή σε προχωρημένα θέματα ψηφιακής εγκληματολογίας

Πλαίσιο

- Επισκόπηση προχωρημένων θεμάτων
- Σχετικός με τον τομέα της ενέργειας

2. Εγκληματολογία νέφους

Πλαίσιο

- Ορισμός και σημασία
- Προκλήσεις: Προβλήματα: δικαιοδοσία δεδομένων, multi-tenancy,
  μεταβλητότητα δεδομένων
- Εργαλεία και τεχνικές: ENCase (λογισμικό ψηφιακής εγκληματολογίας - forensics tool για ανάλυση δεδομένων και ψηφιακών πειστηρίων)

3. Εγκληματολογία IoT

Πλαίσιο

- Ορισμός και σημασία
- Προκλήσεις: Δεδομένα: ετερογένεια συσκευών, δεδομένα
  όγκος, Ευπάθεια ασφαλείας
- Εργαλεία και τεχνικές: Foren6, IoT Inspector

4. Αναδυόμενες τάσεις και προκλήσεις

Πλαίσιο

- Τάσεις: Τεχνητή Νοημοσύνη και μάθηση στην εγκληματολογία
- Προκλήσεις: Κρυπτογράφηση, νόμοι περί απορρήτου δεδομένων

5. Προηγμένες τεχνικές ψηφιακής εγκληματολογίας

Πλαίσιο

- Τεχνικές: Αντίστροφη μηχανική, στεγανοανάλυση
- Εργαλεία: IDA Pro, Stegdetect

6. Περίπτωση χρήσης: Τρόπος νέφους και IoT Forensics στον τομέα της ενέργειας

Πλαίσιο

- Σενάριο: Διερεύνηση παραβίασης ασφάλειας που αφορά υπηρεσίες τρόπων νέφους και συσκευές IoT
- Μέτρα που έχουν ληφθεί: Διαχείριση δεδομένων, διεύθυνσιοδότηση με τρόπους νέφους και IoT forensics

Σας ευχαριστώ

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση: gehad@example.com