Cybersecurity

Description

Σκοπός του Προγράμματος:

Ο σκοπός του προγράμματος είναι η κατάρτιση των ωφελούμενων, ώστε να μπορούν μεταξύ άλλων χρησιμοποιώντας το διαδίκτυο να επιτελούν τα εργασιακά τους καθήκοντα αναγνωρίζοντας την σπουδαιότητα και την αξία της κυβερνοασφάλειας, τόσο για τους οργανισμούς και τις επιχειρήσεις όσο και για τους ίδιους ως τελικούς χρήστες.

Σύντομη Περιγραφή του Προγράμματος Κατάρτισης:

Ως προσωπικό για ανίχνευση, διαχείριση και αντιμετώπιση καταστάσεων κυβερνοασφάλειας ορίζεται ο ειδικά ευαισθητοποιημένος εργαζόμενος, ο οποίος εργάζεται στο ιδιωτικό ή στον δημόσιο τομέα και μπορεί να αναλάβει θέσεις προκειμένου να ανιχνεύσει, διαχειριστεί και τελικά αντιμετωπίσει με αποτελεσματικότητα περιστατικά που άπτονται του αντικειμένου της κυβερνοασφάλειας. Η σπουδαιότητα ωστόσο του συγκεκριμένου εκπαιδευτικού προγράμματος είναι πως δεν επιχειρεί μόνο να ευαισθητοποιήσει τον κάθε εργαζόμενο στον τομέα της κυβερνοασφάλειας αλλά να του παρέχει και ενδεδειγμένες πρακτικές λύσεις για την επίτευξη του ως άνω σκοπού.

Μαθησιακά αποτελέσματα:

Στόχος Ικανότητας:

- Να αναγνωρίζει τις βασικές έννοιες κυβερνοασφάλειας
- Να διατυπώνει τις βασικές έννοιες κυβερνοασφάλειας
- Να διακρίνει την διαφορά του διαδικτύου με το διαδίκτυο των πραγμάτων

- Να επαληθεύει την διαφορά του διαδικτύου με το διαδίκτυο των πραγμάτων
- Να προσδιορίζει τα χαρακτηριστικά του κυβερνοχώρου
- Να κατανοεί την έννοια του κυβερνοεγκλήματος
- Να κατανοεί την έννοια του χακαρίσματος
- Να απαριθμεί τους τομείς- τύπους προστασίας για τα πληροφοριακά συστήματα
- Να επαληθεύει τους τομείς- τύπους προστασίας για τα πληροφοριακά συστήματα
- Να υιοθετεί τους τομείς- τύπους προστασίας για τα πληροφοριακά συστήματα
- Να ταξινομεί τις μεθόδους απειλών στην κυβερνοασφάλεια
- Να επαληθεύει μεθόδους απειλών στην κυβερνοασφάλεια
- Να απαριθμεί τους εμπλεκομένους φορείς στην Ελλάδα για την κυβερνοασφάλεια
- Να απαριθμεί τους εμπλεκομένους φορείς στην Ευρωπαϊκή Ένωση για την κυβερνοασφάλεια
- Να περιγράφει τις βασικές αρμοδιότητες των εμπλεκόμενων φορέων στην Ελλάδα για την κυβερνοασφάλεια.
- Να περιγράφει τις βασικές αρμοδιότητες των εμπλεκόμενων φορέων στην Ευρωπαϊκή Ένωση για την κυβερνοασφάλεια.
- Να προσδιορίζει τις βασικές αρμοδιότητες των εμπλεκομένων φορέων στην Ελλάδα για την κυβερνοασφάλεια.
- Να διακρίνει τους επιμέρους χώρους του διαδικτύου.
- Να κατανοεί την διαφοροποίηση του Surface Web, deep web και dark web.
- Να διατυπώνει την έννοια της κυβερνοτρομοκρατίας και των τρομοκρατικών οργανώσεων.
- Να προσδιορίζει τις διάφορες μορφές κυβερνοεπιθέσεων .
- Να απαριθμεί τις διάφορες μορφές κυβερνοεπιθέσεων.
- Να κατατάσσει τις διάφορες μορφές εγκληματικών οργανώσεων ανάλογα με την μορφή τους.
- Να επαληθεύει τα ιδιαίτερα χαρακτηριστικά της κυβερνοτρομοκρατίας.
- Να προσδιορίζει τις επιμέρους κατηγορίες των δραστών κυβερνοτρομοκρατικών περιστατικών.
- Να απαριθμεί τις συχνότερες μεθόδους που χρησιμοποιούν οι κυβερνοεγκληματίες για να πετύχουν τους σκοπούς τους.
- Να εφαρμόζει τις πολιτικές προστασίας κατά της κυβερνοτρομοκρατίας κατά την εργασία του.
- Να επεξηγεί σε άλλους τις βασικές πολιτικές κατά τις κυβερνοτρομοκρατίας.
- Να υιοθετεί τις πολιτικές προστασίας κατά της κυβερνοτρομοκρατίας κατά την εργασία του.
- Να αναγνωρίζει τα βασικα ευρωπαϊκά και εθνικά νομοθετήματα που αφορούν την

κυβερνοτρομοκρατία .

- Να κατανοεί το βασικό ισχύον νομοθετικό ευρωπαϊκό και εθνικό πλαίσιο κατά της κυβερνοτρομοκρατίας.
- Να διακρίνει τα μέτρα κυβερνοασφάλειας στις επιμέρους κατηγορίες τους.
- Να περιγραφεί τα μέτρα φυσικής ασφάλειας που ενισχύουν την κυβερνοασφάλεια των οργανισμών και των επιχειρήσεων
- Να περιγράφει τα μέτρα προστασίας των επιμέρους πολίτικων τεχνικών μέτρων που ενισχύουν την κυβερνοασφάλεια των οργανισμών και των επιχειρήσεων
- Να περιγράφει τα μέτρα προστασίας των επιμέρους πολίτικων οργανωτικών μέτρων που ενισχύουν την κυβερνοασφάλεια των οργανισμών και των επιχειρήσεων
- Να απαριθμεί τις επιμέρους πολίτικες τεχνικών μέτρων κυβερνοασφάλειας
- Να απαριθμεί τις επιμέρους πολίτικες οργανωτικών μέτρων κυβερνοασφάλειας
- Να υιοθετεί στην κουλτούρα του τις βέλτιστες πρακτικές μεθόδους μέτρων προστασίας φυσικής ασφάλειας για την ανάπτυξη κατάλληλου επιπέδου προστασίας από κυβερνοεπιθέσεις
- Να υιοθετεί στην κουλτούρα του τις βέλτιστες πρακτικές μεθόδους τεχνικών μέτρων προστασίας για την ανάπτυξη κατάλληλου επιπέδου προστασίας από κυβερνοεπιθέσεις
- Να υιοθετεί στην κουλτούρα του τις βέλτιστες πρακτικές μεθόδους οργανωτικών μέτρων προστασίας για την ανάπτυξη κατάλληλου επιπέδου προστασίας από κυβερνοεπιθέσεις
- Να επαληθεύει τα εφαρμοζόμενα μέτρα φυσικής ασφάλειας κατά την εργασία του σε οργανισμούς και επιχειρήσεις.
- Να επαληθεύει τα εφαρμοζόμενα οργανωτικά μέτρα ασφάλειας κατά την εργασία του σε οργανισμούς και επιχειρήσεις.
- Να επαληθεύει τα εφαρμοζόμενα τεχνικά μέτρα ασφάλειας κατά την εργασία του σε οργανισμούς και επιχειρήσεις
- Να εφαρμόζει τεχνικά, οργανωτικά και μέτρα φυσικής ασφάλειας κατά την εργασία του σε επιχειρήσεις και οργανισμούς
- Να αντιλαμβάνεται έγκαιρα ένα περιστατικό κυβερνοασφάλειας
- Να διαχειρίζεται με επάρκεια περιστατικά τα οποία μπορεί να πλήξουν την ακεραιότητα , την διαθεσιμότητα και την εμπιστευτικότητα των πληροφοριακών συστημάτων του οργανισμού ή της επιχείρησης στην οποία εργάζεται.
- Να συμμετέχει σε ομάδα διαχείρισης περιστατικών ασφάλεια από κυβερνοεπιθέσεις.
- Να ερμηνεύει και να γνωρίζει τις βασικές έννοιες που αναφέρονται στην Κρυπτογράφηση δεδομένων
- Να ορίζει και να διαχωρίζει την συμμετρική και ασύμμετρη κρυπτογράφηση

- Να διακρίνει πότε υφίσταται ψευδωνυμοποιήση, πότε ελαχιστοποίηση και πότε ανωνυμοποιήση
- Να προσδιορίζει και να υλοποιεί την διαδικασία της ψευδωνυμοποίησης, της ελαχιστοποίησης και της ανωνυμοποίησης
- Να γνωρίζει πως γίνεται κρυπτογράφηση τμημάτων (ή κατατμήσεων) του σκληρού δίσκου, χρησιμοποιώντας το BitLocker
- Να αποκτήσει βασική γνώση για το πως γίνεται Κρυπτογράφηση Δίσκου Δεδομένων
- Να αποκτήσει βασική γνώση για το πως γίνεται Κρυπτογράφηση επιμέρους τμημάτων του δίσκου των Windows (Windows Partition Encryption)
- Να προσδιορίζει την διαδικασία Κρυπτογράφησης αφαιρούμενου δίσκου USB
- Να αποκτήσει βασική πρακτική γνώση για την κρυπτογράφηση είτε ενός ψηφιακού αρχείου είτε ενός αρχείου word καθώς και το κλείδωμα αρχείων pdf
- Να αποκτήσει βασική πρακτική γνώση για την κρυπτογράφηση συλλογής αρχείων με το PeaZip και για την κρυπτογράφηση συμπιεσμένου (zip) αρχείου με το 7-zip
- Να προσδιορίζει και να υλοποιεί την διαδικασία της κρυπτογράφησης χώρου αποθήκευσης στο Cloud (Cloud Storage Encryption)
- Να προσδιορίζει και να υλοποιεί την διαδικασία για κρυπτογράφηση του αποθηκευτικού χώρου στο Cloud, χρησιμοποιώντας το CryptSync
- Να ερμηνεύει και να γνωρίζει τις υπηρεσίες κοινωνικής δικτύωσής
- Να ορίζει τι είναι τα κοινωνικά δίκτυα
- Να διακρίνει ποιοι εμπλέκονται και ποιες είναι οι οντότητες στις υπηρεσίες κοινωνικής δικτύωσης
- Να προσδιορίζει τις θεμελιώδεις βασικές έννοιες στην Ασφάλεια και Ιδιωτικότητα στις Υπηρεσίες Κοινωνικής Δικτύωσης
- Να αποκτήσει βασική γνώση για τους κίνδυνους Ασφάλειας και Ιδιωτικότητας στις Υπηρεσίες Κοινωνικής Δικτύωσης
- Να προσδιορίζει τους κινδύνους για την Ασφάλεια και την Ιδιωτικότητα των χρηστών στο ‘’Facebook’’
- Να αποκτήσει βασική πρακτική γνώση για τους τρόπους και τα μέτρα προστασίας της ασφάλειας και ιδιωτικότητας στο ‘’Facebook’’
- Να προσδιορίζει τους κινδύνους για την Ασφάλεια και την Ιδιωτικότητα των χρηστών στο ‘’ Twitter’’
- Να αποκτήσει βασική πρακτική γνώση για τους τρόπους και τα μέτρα προστασίας της ασφάλειας και ιδιωτικότητας στο ‘’ Twitter’’
- Να αποκτήσει βασική πρακτική γνώση για τους τρόπους και τα μέτρα προστασίας της ασφάλειας και ιδιωτικότητας κατά την χρήση υπηρεσιών κοινωνικής δικτύωσης για έναν ερευνητή ασφάλειας όπως έλεγχος και προστασία

περιεχομένου/ευαισθητοποίηση, πραγματοποίηση συχνών ελέγχων και χρήση ασφαλών ιστοσελίδων κοινωνικής δικτύωσης

- Να ερμηνεύει και να γνωρίζει τις υπηρεσίες που προσφέρονται για λειτουργικά συστήματα κινητών συσκευών
- Να ορίζει τι είναι το λειτουργικό σύστημα κινητής συσκευής
- Να προσδιορίζει τις θεμελιώδεις βασικές έννοιες στην Ασφάλεια και Ιδιωτικότητα κατά τη χρήση κινητών συσκευών
- Να αποκτήσει βασική γνώση για τους κίνδυνους Ασφάλειας και Ιδιωτικότητας κατά τη χρήση κινητών συσκευών
- Να προσδιορίζει τους κινδύνους για την Ασφάλεια και την Ιδιωτικότητα των χρηστών στο λειτουργικό σύστημα ‘’Android’’
- Να αποκτήσει βασική πρακτική γνώση για τους τρόπους και τα μέτρα προστασίας της ασφάλειας και ιδιωτικότητας στο λειτουργικό σύστημα ‘’Android’’
- Να προσδιορίζει τους κινδύνους για την Ασφάλεια και την Ιδιωτικότητα των χρηστών στο λειτουργικό σύστημα ‘’iOS’’
- Να αποκτήσει βασική πρακτική γνώση για τους τρόπους και τα μέτρα προστασίας της ασφάλειας και ιδιωτικότητας στο στο λειτουργικό σύστημα ‘’iOS’’
- Να αποκτήσει βασική πρακτική γνώση για τους τρόπους και τα μέτρα προστασίας της ασφάλειας και ιδιωτικότητας κατά την χρήση κινητών συσκευών για έναν χρήστη, όπως έλεγχος και προστασία περιεχομένου/ευαισθητοποίηση, πραγματοποίηση συχνών ελέγχων και χρήση ασφαλών πρακτικών
- Να ενημερωθεί σχετικά με τις ευπάθειες των ασύρματων δικτύων
- Να κατηγοριοποιεί πιθανές επιθέσεις σε ασύρματα δίκτυα
- Να αντιμετωπίζει πιθανές επιθέσεις σε ασύρματα δίκτυα
- Να διακρίνει τις ασύρματες επικοινωνίες μικρής εμβέλειας
- Να έχει επίγνωση των δυνατών επιθέσεων σε κάθε μία από τις ασύρματες επικοινωνίες μικρής εμβέλειας
- Να επεξηγεί και να κατηγοριοποιεί τις επιθέσεις DNS και να γνωρίζει τους τρόπους αντιμετώπισης τους
- Να διακρίνει παραγόντων απειλών (threat actors), διανύσματα επιθέσεων (vectors) και ερευνητικές πηγές (intelligence resources)
- Να επιμορφωθεί σχετικά με τους τύπους απειλών
- Να ενημερωθεί σχετικά με τα διανύσματα επιθέσεων
- Να αναλύσει τις ερευνητικές πηγές και να τις διακρίνει σε περαιτέρω κατηγορίες
- Να αναλύει και να κατηγοριοποιεί τις ευπάθειες
- Να αντιλαμβάνεται τους κινδύνων τρίτων στον τομέα της ασφάλειας και των επιπτώσεων που πιθανόν αντιμετωπίσει ένας οργανισμός

- Να επιμορφωθεί σχετικά με τεχνικές αξιολόγησης ασφάλειας
- Να επιμορφωθεί σχετικά με κατάλληλη μεθοδολογία ελέγχου

Η συνολική διάρκεια του Προγράμματος Κατάρτισης είναι **80 ώρες**.
Ώρες δια ζώσης Κατάρτισης: 12
Ώρες Σύγχρονης εξ αποστάσεως: 48
Ώρες Ασύγχρονης: 20

Ο απαιτούμενος χρόνος ολοκλήρωσης του κάθε τμήματος κατάρτισης είναι **1 μήνας**.

Date Created
Μάρτιος 2022
Meta Fields