ENISA

ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

ΕΓΧΕΙΡΙΔΙΟ ΧΡΗΣΤΗ

ΕΥΡΩΠΑΪΚΟ ΠΛΑΙΣΙΟ ΔΕΞΙΟΤΗΤΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (ECSF)

ΣΕΠΤΕΜΒΡΊΟΥ 2022

ΣΧΕΤΙΚΆ ΜΕ ΤΟΝ ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ENISA, είναι ο οργανισμός της Ένωσης που ασχολείται με την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο οποίος ιδρύθηκε το 2004 και ενισχύθηκε με την πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στην πολιτική της ΕΕ για τον κυβερνοχώρο, ενισχύει την αξιοπιστία των προϊόντων, των υπηρεσιών και των διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, συνεργάζεται με τα κράτη μέλη και τα όργανα της ΕΕ και βοηθά την Ευρώπη να ετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της ευαισθητοποίησης, ο Οργανισμός συνεργάζεται με τα βασικά ενδιαφερόμενα μέρη για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την ενίσχυση της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας της κοινωνίας και των πολιτών της Ευρώπης. Περισσότερες πληροφορίες σχετικά με τον ENISA και το έργο του διατίθενται στη διεύθυνση: Βλ. www.enisa.europa.eu.

ΕΠΙΚΟΙΝΩΝΊΑ

Για να επικοινωνήσετε με τους συντάκτες, χρησιμοποιήστε τη διεύθυνσηeuskills@enisa.europa.eu

ΕΥΧΑΡΙΣΤΊΕΣ

Το πλαίσιο αυτό είναι το αποτέλεσμα της γνωμοδότησης και της συμφωνίας των εμπειρογνωμόνων στην ειδική ομάδα εργασίας για το πλαίσιο δεξιοτήτων, η οποία απαρτίζεται από τους Agata BEKIER, Vladlena BENSON, Jutta BREYER *, Fabio DI FRANCO, Sara GARCIA, Αθανάσιο ΓΡΑΜΔΗΜΟΠΟΥΛΟ, Μαρκκού ΚΟΡΚΙΑΚΟΣΚΗ, Csaba KRASZNAY, Χαράλαμπος ΜΟΥΡΑΤΙΔΗΣ, Χριστίνα ΓΕΩΡΓΙΑΔΟΥ, Erwin ORYE *, Edmundas PIESARSKAS, Nineta POLEMI *, Paresh RATHOD *, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN και Jan HAJNY.

Οι Fabio DI FRANCO και Athanasios GRAMMATOPOULOS ηγήθηκαν αυτής της δραστηριότητας για τον ENISA.

ΝΟΜΙΚΉ ΑΝΑΚΟΊΝΩΣΗ

ΕΠΙΦΎΛΑΞΗ ΔΙΚΑΙΩΜΆΤΩΝ ΠΝΕΥΜΑΤΙΚΉΣ ΙΔΙΟΚΤΗΣΊΑΣ

* Εισηγητής της ειδικής ομάδας εργασίας για το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας

ISBN: 978-92-9204-583-8 — DOI: 10.2824/95989

ΠΊΝΑΚΑΣ ΠΕΡΙΕΧΟΜΈΝΩΝ

ΠΕΡΊΛΗΨΗ

Η έλλειψη εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας και η έλλειψη δεξιοτήτων αποτελούν μείζονα πηγή ανησυχίας τόσο για την οικονομική ανάπτυξη όσο και για την εθνική ασφάλεια. Εξετάζοντας το πρόβλημα, ο ENISA εντόπισε την ανάγκη της Ευρώπης για μια ολοκληρωμένη προσέγγιση για τον καθορισμό ενός συνόλου ρόλων και δεξιοτήτων στον τομέα της κυβερνοασφάλειας που θα μπορούσαν να αξιοποιηθούν για τη μείωση της έλλειψης και του χάσματος δεξιοτήτων. Ο ENISA έχει εργαστεί για την ανάπτυξη ενός τέτοιου πλαισίου και παρουσιάζει το **ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας (ECSF)**, το οποίο αποσκοπεί στην ενίσχυση της ευρωπαϊκής κουλτούρας κυβερνοασφάλειας παρέχοντας μια κοινή ευρωπαϊκή γλώσσα σε όλες τις κοινότητες, κάνοντας ένα ουσιαστικό βήμα προόδου προς το ψηφιακό μέλλον της Ευρώπης.

Το ECSF παρέχει ένα πρακτικό εργαλείο για την **υποστήριξη του προσδιορισμού και της διάρθρωσης των καθηκόντων, των ικανοτήτων, των δεξιοτήτων και των γνώσεων που συνδέονται με** τους ρόλους των Ευρωπαίων **επαγγελματιών στον τομέα της κυβερνοασφάλειας**. Κύριος σκοπός του πλαισίου είναι η **δημιουργία κοινής αντίληψης** μεταξύ ιδιωτών, εργοδοτών και παρόχων προγραμμάτων μάθησης σε όλα τα κράτη μέλη της ΕΕ, ώστε να καταστεί πολύτιμο εργαλείο για τη γεφύρωση του χάσματος μεταξύ του επαγγελματικού χώρου εργασίας στον τομέα της κυβερνοασφάλειας και των μαθησιακών περιβαλλόντων.

Το πλαίσιο περιγράφει τις σημαντικότερες απαιτήσεις ενός επαγγελματικού χώρου εργασίας στον τομέα της κυβερνοασφάλειας, καθορίζοντας ένα **σύνολο 12 τυπικών επαγγελματικών προφίλ ρόλων στον τομέα της κυβερνοασφάλειας**. Τα προφίλ αυτά παρέχουν μια κοινή αντίληψη των κύριων αποστολών, καθηκόντων και δεξιοτήτων κυβερνοασφάλειας που απαιτούνται σε ένα επαγγελματικό πλαίσιο κυβερνοασφάλειας, καθιστώντας το τέλειο σημείο αναφοράς για τις δεξιότητες και τις γνώσεις κατάρτισης προφίλ που χρειάζονται οι επαγγελματίες του τομέα της κυβερνοασφάλειας. Το πλαίσιο σχεδιάστηκε έτσι ώστε να είναι εύκολα κατανοητό και ολοκληρωμένο ώστε να παρέχει κατάλληλες εμπεριστατωμένες πληροφορίες για την κυβερνοασφάλεια, καθώς και αρκετά ευέλικτο ώστε να επιτρέπει την εξατομίκευση με βάση τις ανάγκες κάθε χρήστη. Με την ενσωμάτωση όλων των απόψεων όλων των ενδιαφερόμενων μερών, το πλαίσιο εφαρμόζεται σε όλους τους τύπους οργανισμών και στηρίζει την ανάπτυξη όλων των επαγγελμάτων στον τομέα της κυβερνοασφάλειας.

Το ECSF είναι το αποτέλεσμα των εργασιών της ad hoc ομάδας εργασίας του ENISA για το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας[1], η οποία απαρτίζεται από εμπειρογνώμονες που εκπροσωπούν διάφορες απόψεις. Το ανεπτυγμένο πλαίσιο βασίζεται σε ανάλυση των υφιστάμενων πλαισίων, των αποτελεσμάτων και των πορισμάτων της έρευνας σχετικά με τις ανάγκες της αγοράς και της συμφωνίας μεταξύ εμπειρογνωμόνων. Περιπτωσιολογικές μελέτες χρηστών και ενδεικτικά παραδείγματα, εμπνευσμένα από διάφορους χώρους εργασίας και μαθησιακά περιβάλλοντα, καταδεικνύουν την πρακτική εφαρμογή αυτού του πλαισίου και υποστηρίζουν το έργο αυτό.

Τα κύρια οφέλη από τη χρήση του ECSF ήταν τα εξής:

- διασφάλιση κοινής **ορολογίας και κοινής αντίληψης** όσον αφορά τους επαγγελματίες του τομέα της κυβερνοασφάλειας σε ολόκληρη την ΕΕ

Το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας (ECSF) αποσκοπεί στην ενίσχυση της ευρωπαϊκής κουλτούρας κυβερνοασφάλειας, παρέχοντας μια κοινή ευρωπαϊκή γλώσσα σε όλες τις κοινότητες, κάνοντας ένα ουσιαστικό βήμα προόδου προς το ψηφιακό

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

- προσδιορισμός του **κρίσιμου συνόλου δεξιοτήτων** που απαιτούνται από τη σκοπιά του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας για τη στήριξη της περαιτέρω ανάπτυξης και ενίσχυσής του·

- προώθηση της **εναρμόνισης των** προγραμμάτων **εκπαίδευσης**, **κατάρτισης** και **ανάπτυξης του εργατικού δυναμικού** στον τομέα της κυβερνοασφάλειας.

Το παρόν εγχειρίδιο χρήσης του ECSF παρέχει ολοκληρωμένη επισκόπηση του κύριου πεδίου εφαρμογής, των αρχών-πλαισίων και των ευκαιριών εφαρμογής του ECSF. Πρωταρχικός σκοπός του εγχειριδίου είναι να καταστήσει το ECSF εύκολα προσβάσιμο, κατανοητό και χρησιμοποιήσιμο από όλα τα ενδιαφερόμενα μέρη με ενεργό ρόλο ή ανάγκη για κατάλληλα καταρτισμένους επαγγελματίες στον τομέα της κυβερνοασφάλειας.

1. ΕΙΣΑΓΩΓΉ

Η έλλειψη δεξιοτήτων κυβερνοασφάλειας είναι μία από τις βασικές προκλήσεις που πρέπει να αντιμετωπιστούν για μια ασφαλή στον κυβερνοχώρο Ευρωπαϊκή Ένωση. Ειδικότερα, υπάρχει έλλειψη ειδικευμένου και ειδικευμένου προσωπικού στην αγορά εργασίας για την ανάληψη ρόλων στον τομέα της κυβερνοασφάλειας και το οποίο μπορεί να αντιμετωπίσει επαρκώς τις εξελισσόμενες κυβερνοαπειλές και τις αναδυόμενες προκλήσεις στον κυβερνοχώρο. Το χάσμα όσον αφορά τις δεξιότητες στον τομέα της κυβερνοασφάλειας έχει μια σειρά υποκείμενων κινητήριων μοχλών. Σε αυτές περιλαμβάνεται το ανεπαρκές επίπεδο κατανόησης των ικανοτήτων και των δεξιοτήτων που απαιτούνται στον τομέα της κυβερνοασφάλειας μεταξύ των διαφόρων παραγόντων της αγοράς δεξιοτήτων κυβερνοασφάλειας. Με την πάροδο των ετών, αυτό έχει καταστεί ένα καλά τεκμηριωμένο πρόβλημα2, το οποίο εξακολουθεί να επηρεάζει σημαντικά τις χώρες σε ευρωπαϊκό και διεθνές επίπεδο.

Προκειμένου να μειωθεί το υφιστάμενο και το μελλοντικό χάσμα και η έλλειψη δεξιοτήτων, απαιτούνται περισσότεροι επαγγελματίες στον τομέα της κυβερνοασφάλειας με κατάλληλα σύνολα δεξιοτήτων. Για τον σκοπό αυτό, το ευρωπαϊκό θεματολόγιο δεξιοτήτων3, το σχέδιο δράσης για την ψηφιακή εκπαίδευση4και το σύμφωνο δεξιοτήτων5 παραμένουν σημαντικά μέσα για την κινητοποίηση των ενδιαφερόμενων μερών ώστε να συνεργαστούν για την επίτευξη των στόχων της ψηφιακής δεκαετίας,6 δημιουργώντας περισσότερες και καλύτερες ευκαιρίες κατάρτισης.

Στο πλαίσιο αυτό, τον7 Δεκέμβριο του 2020 ο ENISA δρομολόγησε ad hoc ομάδα εργασίας για το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας. Συγκροτήθηκε διεπιστημονική ομάδα εμπειρογνωμόνων με στόχο την προώθηση της εναρμόνισης των εννοιών της εκπαίδευσης, της κατάρτισης και της ανάπτυξης του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας. Το ανεπτυγμένο πλαίσιο (ECSF) παρέχει ένα ανοικτό ευρωπαϊκό εργαλείο για την ανάπτυξη κοινής αντίληψης των επαγγελματικών προφίλ ρόλων στον τομέα της κυβερνοασφάλειας και κοινών αντιστοιχίσεων με τις κατάλληλες δεξιότητες και ικανότητες που απαιτούνται. Οι εργασίες αυτές παρέχουν τη βάση για τη συνένωση δυνάμεων σε ένα πρόγραμμα ανάπτυξης ικανοτήτων για το ευρωπαϊκό εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας σύμφωνα με τη συνεχιζόμενη ζήτηση της αγοράς.

1.1 ΣΤΟΧΕΥΌΜΕΝΟ ΚΟΙΝΌ

Ενώ το απώτερο πεδίο εφαρμογής του περιεχομένου του πλαισίου του ECSF είναι οι βασικοί επαγγελματίες στον τομέα της κυβερνοασφάλειας, ιδιαίτερη έμφαση δίνεται επίσης στις ομάδες-στόχους του ECSF για εμπειρογνώμονες εκτός κυβερνοασφάλειας, οι οποίοι χρειάζονται ολοκληρωμένη εικόνα του κλάδου. Η εστίαση αυτή καθιστά το πλαίσιο εύκολα κατανοητό για όλα τα ενδιαφερόμενα μέρη.

Το κοινό-στόχος για το ECSF είναι οι ηγετικές ομάδες των οργανισμών, οι ανθρώπινοι πόροι και οι λειτουργίες κυβερνοασφάλειας, οι επαγγελματίες του τομέα της κυβερνοασφάλειας, οι νεοεισερχόμενοι και οι ενθουσιασμένοι στον κυβερνοχώρο, καθώς και οι πάροχοι προγραμμάτων μάθησης κάθε είδους στο δημόσιο και ιδιωτικό πλαίσιο, οι κλαδικές ενώσεις, οι ερευνητές της αγοράς και οι υπεύθυνοι χάραξης πολιτικής.

1.2 ΔΟΜΉ ΤΟΥ ΕΓΧΕΙΡΙΔΊΟΥ

Το εγχειρίδιο χρήστη διαρθρώνεται ως εξής:

2 ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-safety education-in-the-european-Union (Ανάπτυξη δεξιοτήτων στον τομέα της κυβερνοασφάλειας στην ΕΕ)
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196
[4] https://education.ec.europa.eu/focus-topics/digital-education/action-plan
[5] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197
[6] https://digital-strategy.ec.europa.eu/en/node/157
[7] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

* ENISA

- Στο κεφάλαιο 1 παρουσιάζονται οι βασικές προκλήσεις που αναδεικνύουν την ανάγκη να δημιουργηθεί ένα πλαίσιο για τις δεξιότητες κυβερνοασφάλειας, καθώς και το κοινό-στόχος για το έργο αυτό·

- Στο κεφάλαιο 2 παρουσιάζονται οι αρχές σχεδιασμού του ECSF, καθώς και τα βασικά οφέλη για τη χρήση του·

- Το κεφάλαιο 3 εξηγεί τις διαφορετικές εφαρμογές του ECSF από διάφορες απόψεις.

Επιπλέον, το έγγραφο περιλαμβάνει δύο (2) Παραρτήματα που υποστηρίζουν το εγχειρίδιο χρήστη του ECSF και τους στόχους του:

- Το παράρτημα Α συνδέει το ECSF με άλλα πρότυπα και πλαίσια της ΕΕ.
Στόχος του παρόντος παραρτήματος είναι η σύνδεση του ECSF με τα υφιστάμενα αναγνωρισμένα ευρωπαϊκά πρότυπα και πλαίσια που σχετίζονται με το έργο αυτό.

- Στο παράρτημα Β απαριθμούνται οι περιπτώσεις χρήσης του ECSF.
Στόχος του παρόντος παραρτήματος είναι η παροχή πραγματικών σεναρίων για την ανάδειξη της πρακτικής εφαρμογής του εν λόγω πλαισίου.

Το ECSF παρέχει ένα ανοικτό ευρωπαϊκό εργαλείο για την ανάπτυξη κοινής αντίληψης των επαγγελματικών προφίλ ρόλων στον τομέα της κυβερνοασφάλειας και κοινών αντιστοιχίσεων με τις κατάλληλες δεξιότητες και ικανότητες που απαιτούνται.

Το απώτερο πεδίο εφαρμογής του πλαισίου του ECSF είναι οι βασικοί επαγγελματίες στον τομέα της κυβερνοασφάλειας, ενώ δίνεται επίσης έμφαση σε εμπειρογνώμονες εκτός-κυβερνοασφάλει

2. ΚΑΤΑΝΌΗΣΗ ΤΗΣ ECSF

Το ECSF αποτελείται από ένα αντιπροσωπευτικό σύνολο **12 προφίλ ρόλων για επαγγελματίες του τομέα της κυβερνοασφάλειας** (τα οποία παρουσιάζονται στο γράφημα 1), τα οποία συνήθως απαιτούνται και εφαρμόζονται στο πλαίσιο οργανισμών που αναπτύσσουν επαγγελματίες στον τομέα της κυβερνοασφάλειας. Κάθε προφίλ καθορίζεται από ένα κοινό υπόδειγμα που ενσωματώνει βασικά καθορισμένα κριτήρια (π.χ. τίτλος, εναλλακτικοί τίτλοι, συνοπτική περιγραφή, αποστολή, κύρια καθήκοντα, βασικές δεξιότητες, βασικές γνώσεις, ηλεκτρονικές ικανότητες). Το περιεχόμενο κάθε κριτηρίου είναι προσαρμοσμένο σε κάθε ρόλο, αλλά υπόκειται σε πιθανή προσαρμογή ώστε να καταστεί δυνατή η ευέλικτη εφαρμογή για την κάλυψη συγκεκριμένων καταστάσεων και απαιτήσεων.

Διάγραμμα 1: Τα προφίλ ρόλου του ECSF για τους επαγγελματίες

Το ECSF εισάγει ένα αντιπροσωπευτικό σύνολο 12 προφίλ ρόλων για τους επαγγελματίες του τομέα της κυβερνοασφάλειας (που συνήθως απαιτούνται και εφαρμόζονται εντός των οργανισμών) σε μορφότυπο που έχει συμφωνηθεί από την ΕΕ και

Τα 12 προφίλ ρόλων για τους επαγγελματίες του τομέα της κυβερνοασφάλειας παρέχονται σε μορφότυπο που έχει συμφωνηθεί από την ΕΕ και βασίζεται στην πρακτική και είναι αφιερωμένος στον επαγγελματικό τομέα της κυβερνοασφάλειας. Τα προφίλ είναι εύκολα κατανοητά και προσφέρουν εναλλακτικά σημεία εισόδου ανάλογα με το πλαίσιο, την προοπτική και τις ανάγκες. Μέσω αυτών των προφίλ, το ECSF μπορεί να χρησιμοποιηθεί ως κοινό εργαλείο αναφοράς και επικοινωνίας που μπορεί να εφαρμοστεί σε διάφορους οργανισμούς και χώρες για μια κοινή αμοιβαία εσωτερική και εξωτερική κατανόηση.

Η δομή κάθε προφίλ ρόλου περιγράφεται στον πίνακα 1 κατωτέρω.
Πίνακας 1: Τα στοιχεία κάθε προφίλ ρόλων ECSF

Τίτλος προφίλ	Το όνομα του προφίλ επαγγελματικού ρόλου
Εναλλακτικός (-οί) τίτλος (-οι)	Παραθέτει τυπικούς εναλλακτικούς τίτλους στο ίδιο προφίλ.
ΣΥΝΟΠΤΙΚΗ ΚΑΤΑΣΤΑΣΗ	Δηλώνει τον κύριο σκοπό του προφίλ.
Αποστολή	Περιγράφει το σκεπτικό του προφίλ.
Παραδοτέο (-α)	Κατάλογο τυπικών αποτελεσμάτων του προφίλ, ο οποίος εξηγεί επίσης τη σημασία του προφίλ από μη εξειδικευμένη άποψη.
Κύρια καθήκοντα	Κατάλογος των τυπικών καθηκόντων που εκτελούνται από τον προκαθορισμένο ρόλο.
Βασική/-ές δεξιότητα/-ες	Κατάλογο των ικανοτήτων που απαιτούνται για την εκτέλεση των καθηκόντων και των καθηκόντων του ρόλου. Οι μη τεχνικές δεξιότητες και η δεοντολογία καθίστανται σαφείς σε ορισμένες περιπτώσεις.
Βασικές γνώσεις	Κατάλογο των βασικών γνώσεων που απαιτούνται για την εκτέλεση των καθηκόντων και των καθηκόντων στο πλαίσιο του ειδικού ρόλου.
ηλεκτρονικές ικανότητες (EN16234-1 e-CF)	Σύνδεση με το EN16234-1 e-Competence Framework (e-CF) — Ένα κοινό ευρωπαϊκό πλαίσιο για τους επαγγελματίες ΤΠΕ σε όλους τους τομείς.

Όπως παρουσιάζεται στον πίνακα 1, το προφίλ για κάθε ρόλο συμπληρώνεται από ένα σύνολο περιγραφικών στοιχείων που έχουν σχεδιαστεί για να παρέχουν μια συνοπτική εικόνα του ρόλου όσον αφορά την περιγραφή, τα καθήκοντα και τις αρμοδιότητές του. Τίτλοι και τυπικοί εναλλακτικοί τίτλοι μπορούν να χρησιμοποιηθούν ως γρήγορη αναφορά για την καθοδήγηση των χρηστών του ECSF στα καταλληλότερα προφίλ ρόλων για την εφαρμογή τους.

Οι συνιστώσες των προφίλ ρόλων **μπορούν να τροποποιηθούν** ώστε να καλύπτουν καλύτερα τις ανάγκες των ενδιαφερόμενων μερών, και **τα προφίλ ρόλων** (από το ECSF και άλλα πλαίσια) **μπορούν να συνδυαστούν** για τον ίδιο λόγο. Περισσότερες πληροφορίες σχετικά με την εφαρμογή του ECSF παρέχονται στο κεφάλαιο 3.

Οι μη τεχνικές δεξιότητες (οι οποίες αποκαλούνται επίσης εγκάρσιες, μεταβιβάσιμες ή συμπεριφορικές δεξιότητες) είναι συστατικά στοιχεία που είναι απαραίτητα σε κάθε σύνολο επαγγελματικών δεξιοτήτων· ως εκ τούτου, οι δεξιότητες αυτές είναι επίσης απαραίτητες για τους επαγγελματίες στον τομέα της κυβερνοασφάλειας. Ένα ευρύ φάσμα δεξιοτήτων εμπίπτουν στις μη τεχνικές δεξιότητες, όπως οι ικανότητες επικοινωνίας, συνεργασίας με άλλους, αναφοράς, επιρροής, κριτικής σκέψης και διαχείρισης του χρόνου και του άγχους. Οι βασικές μη τεχνικές δεξιότητες ενσωματώνονται στη βασική συνιστώσα των δεξιοτήτων.

Για παράδειγμα, το προφίλ ρόλου ενός υπεύθυνου ασφάλειας πληροφοριών (CISO) περιλαμβάνει ως βασικές δεξιότητες τις ικανότητες επιρροής, καθοδήγησης, επικοινωνίας, συνεργασίας και συνεργασίας. Όλα αυτά αποτελούν βασικές δεξιότητες προκειμένου ένας CISO να εκπληρώσει τις αποστολές και τα καθήκοντά του. Με βάση τις ανάγκες ενός ενδιαφερόμενου μέρους, ενδέχεται να προστεθούν περισσότερες μη τεχνικές δεξιότητες στο προφίλ ενός CISO ή μπορεί να πραγματοποιηθεί χαρτογράφηση με πλαίσιο ήπιων δεξιοτήτων.

Η **δεοντολογία** αποτελεί επίσης σημαντικό εγκάρσιο στοιχείο που επηρεάζει όλες τις πτυχές της κυβερνοασφάλειας και, ως εκ τούτου, αποτελεί βασική συνιστώσα δεξιοτήτων εντός του ευρωπαϊκού πλαισίου δεξιοτήτων για την κυβερνοασφάλεια (ECSF). Στο πλαίσιο της κυβερνοασφάλειας, η δεοντολογία αφορά το ποιες αποφάσεις ευθυγραμμίζονται με τις αξίες μας και τι είναι ηθικά αποδεκτό τόσο για τον ιδιοκτήτη των δεδομένων όσο και για τον οργανισμό. Δεδομένου ότι οι επαγγελματίες του τομέα της κυβερνοασφάλειας θα μπορούσαν να αποκτήσουν προνομιακή πρόσβαση σε διάφορα είδη πληροφοριών, ακόμη και σε ευαίσθητες πληροφορίες, η δεοντολογική ευαισθητοποίηση αποτελεί σημαντική αξία που θα πρέπει να έχουν. Πέραν τούτου, η δεοντολογική λήψη αποφάσεων αποτελεί σημαντική δεξιότητα που θα πρέπει να διαθέτουν οι επαγγελματίες στον τομέα της κυβερνοασφάλειας καθώς

οι αποφάσεις τους επηρεάζουν άλλα άτομα. Όπως και στην περίπτωση των μη τεχνικών δεξιοτήτων, το ECSF ανέλυσε ρητά κατά πόσον η δεοντολογική πλευρά του τομέα ευθυγραμμίζεται με τις ευρωπαϊκές αξίες και τη δεοντολογία.

Το ενδιαφερόμενο μέρος μπορεί να προβεί σε λεπτομερέστερη ανάλυση των μη τεχνικών και δεοντολογικών δεξιοτήτων, δεδομένου ότι το πλαίσιο είναι ευέλικτο και προσαρμόσιμο.

2.1 ΟΙ ΑΡΧΈΣ ΣΧΕΔΙΑΣΜΟΎ ΤΟΥ ECSF

Το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας βασίζεται σε ορισμένες αρχές που έχουν σχεδιαστεί για να καλύπτουν τις ανάγκες των ενδιαφερόμενων μερών. Αυτό προσφέρει εύκολη κατανόηση, έγκριση και εφαρμογή του πλαισίου, διατηρώντας παράλληλα τη συνάφεια και τον αντίκτυπο βραχυπρόθεσμα και μακροπρόθεσμα.

Το ECSF βασίζεται σε αρχές που έχουν σχεδιαστεί για να καλύπτουν τις ανάγκες των ενδιαφερόμενων μερών, προσφέροντας εύκολη κατανόηση, έγκριση και εφαρμογή, διατηρώντας παράλληλα τη

Διάγραμμα 2: Οι αρχές σχεδιασμού του ECSF

2.1.1 Απλή αλλά ολοκληρωμένη

Το πλαίσιο έχει σχεδιαστεί έτσι ώστε να είναι κατάλληλα γενικό ώστε να διασφαλίζεται ότι μπορεί να γίνει εύκολα κατανοητό και να εφαρμοστεί από ένα ευρύτερο κοινό. Ταυτόχρονα, περιλαμβάνει επαρκείς λεπτομέρειες για την παροχή εις βάθος πληροφοριών σχετικά με την κυβερνοασφάλεια. Τα χαρακτηριστικά αυτά διευκολύνουν τη χρήση του πλαισίου σε ευρύ φάσμα δραστηριοτήτων και περιβαλλόντων και από ενδιαφερόμενα μέρη από διάφορα περιβάλλοντα (π.χ. οργανώσεις διαφόρων μεγεθών, τεχνική εμπειρογνωμοσύνη ποικίλης έντασης και επιχειρηματικοί τομείς με διαφορετικές βασικές δραστηριότητες).

Αυτό επιτεύχθηκε με την εφαρμογή του κατάλληλου επιπέδου λεπτομέρειας στο περιεχόμενο του ECSF, το οποίο δεν είναι υπερβολικά συγκεκριμένο ούτε υπερβολικά αφηρημένο. Προσφέροντας 12 προφίλ, το ECSF καλύπτει ευρύ φάσμα ποικίλων δραστηριοτήτων εργασίας, αλλά διατηρεί εύχρηστη μορφή.

2.1.2 Ευέλικτο και κλιμακούμενο

Υιοθετώντας μια σπονδυλωτή προσέγγιση και μια ευέλικτη δομή, το πλαίσιο επιτρέπει την επέκταση ή την ανεξάρτητη χρήση κάθε στοιχείου. Τα χαρακτηριστικά αυτά υποστηρίζουν την περαιτέρω επέκταση του ECSF και/ή τη σύνδεση με άλλα πλαίσια για την επέκταση των εφαρμογών του.

Με την εφαρμογή αυτής της ευελιξίας, τα προφίλ και οι συνιστώσες τους, όπως ορίζονται από το ECSF, μπορούν να εφαρμοστούν ανά ενότητα, επιτρέποντας την προσαρμογή καθενός σε συγκεκριμένες ανάγκες. Η ευελιξία αυτή διασφαλίζει τη συνάφεια του πλαισίου με την πάροδο των ετών και θα επιτρέψει επίσης απλές επικαιροποιήσεις του πλαισίου στο μέλλον.

2.1.3 Ανοικτή και ατελής

Το πλαίσιο αναπτύχθηκε με τη συμβολή μιας μεγάλης και ποικιλόμορφης ομάδας εργασίας επαγγελματιών εμπειρογνωμόνων στον τομέα της κυβερνοασφάλειας. Προκειμένου να αναπτύξει ένα αμερόληπτο πλαίσιο, ο ENISA συγκρότησε την ομάδα αυτή από διάφορους εμπειρογνώμονες από διάφορα υπόβαθρα. Με τη συμμετοχή εμπειρογνωμόνων με διαφορετικό υπόβαθρο, η διαδικασία ανάπτυξης του πλαισίου ακολούθησε μια προσέγγιση πολλαπλών προοπτικών που εξαλείφει κάθε μεροληψία προς συγκεκριμένους τομείς ενδιαφέροντος. Επιπλέον, ως δημοσίευση του ENISA, το πλαίσιο είναι διαθέσιμο στο κοινό, προσβάσιμο και ανοικτό.

Τα προφίλ και οι συνιστώσες του ECSF έχουν αναπτυχθεί με βάση μια πολυσυμμετοχική προοπτική, με έμφαση όχι μόνο στην άποψη της απασχόλησης στον τομέα της κυβερνοασφάλειας, αλλά και από τη σκοπιά των παρόχων προγραμμάτων μάθησης. Επιπλέον, η ειλικρίνεια του πλαισίου ενισχύθηκε με τη συμμετοχή και την επανεξέταση διαφόρων πρόσθετων ενδιαφερόμενων μερών.

2.1.4 Ευρωπαϊκή

Λόγω της απαίτησης να ελαχιστοποιηθούν τα κενά σε δεξιότητες κυβερνοασφάλειας και οι ελλείψεις εργατικού δυναμικού σε ολόκληρη την Ευρώπη, το ECSF έπρεπε να συμμορφώνεται με συγκεκριμένες ευρωπαϊκές απαιτήσεις, ώστε να καταστεί δυνατή η εύκολη υιοθέτηση και χρήση από τους ευρωπαϊκούς οργανισμούς. Η κατεύθυνση αυτή βασίστηκε στη συμμόρφωση με τα υφιστάμενα ευρωπαϊκά πρότυπα και πλαίσια.

Το ECSF συνδέεται καλά με το σημερινό ευρωπαϊκό επαγγελματικό τοπίο στον τομέα των ΤΠΕ, ώστε να διασφαλίζεται η εύκολη αφομοίωση και η ευρεία αναγνώριση. Το ECSF επωφελείται καλύτερα από τις υφιστάμενες εμπειρίες και δομές και παρέχει συνεκτικούς δεσμούς με τα σχετικά επαγγελματικά πρότυπα και πλαίσια της ΕΕ στον τομέα των ΤΠΕ. Τα προφίλ που καθορίζονται από το πλαίσιο έχουν σχεδιαστεί έτσι ώστε να είναι συμβατά και συμπληρωματικά προς τους ευρωπαϊκούς νόμους και κανονισμούς και να ενισχύουν τις προσεγγίσεις της ευρωπαϊκής δεοντολογίας, όπως προσδιορίζονται στην ευρωπαϊκή αγορά. Το ECSF λαμβάνει υπόψη τις απαιτήσεις για την προστασία των δεδομένων και της ιδιωτικής ζωής που ορίζονται από τους ευρωπαϊκούς κανονισμούς, τους κοινούς εργασιακούς ρόλους που απαιτεί η ευρωπαϊκή αγορά και τα ευρωπαϊκά πρότυπα και πλαίσια που χρησιμοποιούνται στον τομέα των ΤΠΕ.

2.2 ΟΙ ΚΎΡΙΕΣ ΠΑΡΟΧΈΣ ΠΟΥ ΠΑΡΈΧΟΝΤΑΙ ΑΠΌ ΤΟ ECSF

Το ECSF είναι ένα εύχρηστο αλλά ολοκληρωμένο εργαλείο. Βασίζεται σε πρόσφατες μελέτες αγοράς, στη συνεργασία εμπειρογνωμόνων στον τομέα της κυβερνοασφάλειας και σε ανάλυση του ευρύτερου τοπίου των πλαισίων κυβερνοασφάλειας και ΤΠΕ. Έτσι, εκφράζει τις σχετικές ανάγκες της ευρωπαϊκής αγοράς. Αποτελείται από 12 τυπικούς επαγγελματικούς ρόλους στον τομέα της κυβερνοασφάλειας, με σχετική συνοπτική δήλωση, αποστολή, παρατηρήσιμα αποτελέσματα (παραδοτέα), καθήκοντα, ικανότητες, δεξιότητες, γνώσεις και επίπεδα επάρκειας, όπως απαιτείται και εφαρμόζεται στο πλαίσιο της εργασίας στην Ευρώπη, προς κατανόηση και χρήση σε ολόκληρη την Ευρώπη.

Το ECSF παρέχει μια αδιαμφισβήτητη αναφορά για τον εντοπισμό και τη μείωση των υφιστάμενων και μελλοντικών ελλείψεων και κενών σε δεξιότητες κυβερνοασφάλειας. Είναι γενικό αλλά ταυτόχρονα επαρκώς αναλυτικό ώστε να παρέχει στην αγορά της ΕΕ σαφή ταξινόμηση των δεξιοτήτων, των ικανοτήτων και των επαγγελμάτων του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας. Επιπλέον, μπορεί να συνδέεται εύκολα με άλλες υφιστάμενες δομές και πλαίσια σε συναφείς τομείς.

Το ECSF παρέχει μια αδιαμφισβήτητη αναφορά για τον εντοπισμό και τη μείωση των υφιστάμενων και μελλοντικών

Η χρήση του ECSF ως κοινής ευρωπαϊκής γλώσσας για τους επαγγελματικούς ρόλους, τις δεξιότητες, τις γνώσεις και τις ικανότητες στον τομέα της κυβερνοασφάλειας προσφέρει πολλά οφέλη, ορισμένα από τα οποία παρατίθενται παρακάτω.

1. Η χρήση του ECSF διασφαλίζει κοινή ορολογία και κοινή κατανόηση μεταξύ της επαγγελματικής ζήτησης στον τομέα της κυβερνοασφάλειας (χώρος εργασίας, πρόσληψη) και της προσφοράς (προσόντα, κατάρτιση, αξιολόγηση και αναγνώριση) σε ολόκληρη την ΕΕ.
2. Το ECSF υποστηρίζει τον προσδιορισμό των κρίσιμων απαιτήσεων δεξιοτήτων από τη σκοπιά του εργατικού δυναμικού. Δίνει τη δυνατότητα στους παρόχους προγραμμάτων μάθησης να στηρίζουν την ανάπτυξη κρίσιμων δεξιοτήτων και στους υπεύθυνους χάραξης πολιτικής να στηρίζουν στοχευμένες πρωτοβουλίες για τον μετριασμό των ελλείψεων που εντοπίζονται στις δεξιότητες.
3. Το ECSF συμβάλλει στην κατανόηση των επαγγελματικών ρόλων κυβερνοασφάλειας και των απαιτούμενων βασικών δεξιοτήτων, καθώς και της σχετικής νομοθεσίας. Ειδικότερα, οι μη εμπειρογνώμονες και τα τμήματα ανθρώπινων πόρων είναι σε θέση να κατανοήσουν καλύτερα τις απαιτήσεις για τον σχεδιασμό πόρων στον τομέα της κυβερνοασφάλειας, τις προσλήψεις και τον σχεδιασμό σταδιοδρομίας.
4. Το ECSF προωθεί την εναρμόνιση της εκπαίδευσης, της κατάρτισης και της ανάπτυξης του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας. Επιπλέον, η χρήση μιας κοινής ευρωπαϊκής γλώσσας στις δεξιότητες και τους ρόλους κυβερνοασφάλειας σχετίζεται άμεσα με ολόκληρο τον επαγγελματικό τομέα των ΤΠΕ.

5. Το ECSF συμβάλλει στην επίτευξη μεγαλύτερης ανθεκτικότητας σε κυβερνοεπιθέσεις και στη διασφάλιση ασφαλών συστημάτων ΤΠΕ σε ολόκληρη την κοινωνία. Παρέχει μια τυποποιημένη δομή και παρέχει συμβουλές σχετικά με τον τρόπο επιβολής της ανάπτυξης ικανοτήτων στο ευρωπαϊκό εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας.

Το ECSF παρέχει πρόσθετα οφέλη με βάση το είδος των ενδιαφερόμενων μερών. Ένα παράδειγμα των κύριων ενδιαφερόμενων μερών και των βασικών συναφών βασικών οφελών παρουσιάζεται το 3.

Διάγραμμα 3: Παράδειγμα των κυριότερων δικαιούχων του ECSF που εκφράζουν την ανάγκη κοινού ορισμού του διαχειριστή κινδύνου

Λεπτομερής κατάλογος των πιθανών εφαρμογών και οφελών από τη χρήση του ECSF με βάση τα ενδιαφερόμενα μέρη παρουσιάζεται στον πίνακα 2.

Πίνακας 2: Πιθανές εφαρμογές ECSF και οφέλη για τα ενδιαφερόμενα μέρη

Ενδιαφερόμενος	Οφέλη από τη χρήση του ECSF
Οργανώσεις	● υποστηρίζει την ανάπτυξη στρατηγικής και οργανωτικής δομής για την ασφάλεια στον κυβερνοχώρο ● υποστηρίζει την ανάπτυξη του σχεδιασμού των ανθρώπινων πόρων στον τομέα της κυβερνοασφάλειας ● παρέχει στήριξη στη διαδικασία πρόσληψης, ιδίως: ○ τον προσδιορισμό των απαιτήσεων για τον ρόλο στον τομέα της κυβερνοασφάλειας ○ αξιολόγηση των υποψηφίων για θέματα κυβερνοασφάλειας ● παρέχει ανάλυση του ρόλου και της έλλειψης δεξιοτήτων στον τομέα της κυβερνοασφάλειας και συνακόλουθη πρόβλεψη ανάγκες σε ατομικό, ομαδικό ή οργανωτικό επίπεδο ● καθορίζει σχέδια ανάπτυξης και κατάρτισης σε ατομικό, ομαδικό ή οργανωτικό επίπεδο ● υποστηρίζει την αξιολόγηση των ρόλων της ασφάλειας στον κυβερνοχώρο, βοηθώντας στην ανάπτυξη εξατομικευμένων υποδείγματα για ρόλους κυβερνοασφάλειας ● παρέχει μια κοινή και εύκολα κατανοητή γλώσσα για τις προσκλήσεις υποβολής ● προσφορών στον τομέα της κυβερνοασφάλειας, προμήθειες, κενές θέσεις εργασίας και λογιστικοί έλεγχοι

Πάροχοι προγραμμάτων μάθησης	● υποστηρίζει τον σχεδιασμό προγραμμάτων μάθησης και προγραμμάτων σπουδών, τον επανασχεδιασμό και συντήρηση ● προσφέρει συνεργασία μεταξύ ιδρυμάτων και κινητικότητα σε προγράμματα μάθησης, π.χ. διευρωπαϊκά προγράμματα μάθησης από πολλαπλά ιδρύματα ● προωθεί την προσφορά προγραμμάτων μάθησης και αυξάνει την ευαισθητοποίηση ● τοποθετεί μαθησιακά αποτελέσματα σε πραγματικό εργασιακό πλαίσιο ● υποστηρίζει τις διαδικασίες αξιολόγησης και αναγνώρισης ● παρέχει επαγγελματικό προσανατολισμό στους σπουδαστές

Άτομα	● στηρίζει τα άτομα ώστε να κάνουν επιλογές επαγγελματικής σταδιοδρομίας και να τοποθετηθούν οι ίδιοι ● διευρύνει τις μαθησιακές προοπτικές, ανοίγει νέες σταδιοδρομίες και προωθεί την επαγγελματική ανάπτυξη για τη στήριξη της επανειδίκευσης και της αναβάθμισης των δεξιοτήτων ● συμβάλλει στην κατανόηση των πρακτικών απαιτήσεων στον χώρο εργασίας και των εργασιακών προσδοκιών σε περισσότερα λεπτομερώς ● προσδιορίζει τους τρόπους τυπικής και μη τυπικής μάθησης ● παρέχει στήριξη για τη δημιουργία σταδιοδρομιών
Επαγγελματικές ενώσεις	● επιτρέπει την εδραίωση των κοινοτήτων των ενδιαφερόμενων μερών για την υποστήριξη της ανταλλαγής γνώσεων, νέες εξελίξεις, βελτιώσεις και περαιτέρω εφαρμογή στα κράτη μέλη της ΕΕ ● παρέχει υποστήριξη για τη διενέργεια ανάλυσης της αγοράς και την παρουσίαση των αποτελεσμάτων σε κοινή γλώσσα ● συμβάλλει στην παροχή ολοκληρωμένης επαγγελματικής καθοδήγησης στον τομέα της κυβερνοασφάλειας
Υπεύθυνοι χάραξης πολιτικής και κυβερνητικοί φορείς	● υποστηρίζει μια κοινή αντίληψη στον τομέα της κυβερνοασφάλειας ● ενθαρρύνει τον σχεδιασμό κατά προτεραιότητα και την ανάπτυξη ικανοτήτων στον τομέα της κυβερνοασφάλειας ● επιτρέπει τη χαρτογράφηση πολλών πρωτοβουλιών κυβερνοασφάλειας με βάση τα προφίλ του ECSF ● υποστηρίζει πρωτοβουλίες πολιτικής που βασίζονται στην ανάλυση δεδομένων
Όλα	● προσφέρει μια κοινή γλώσσα για όλα τα ενδιαφερόμενα μέρη ● επιταχύνει τη συνεργασία παρέχοντας ένα κοινό σημείο εκκίνησης ● παρέχει κοινή αναφορά για τη συγκέντρωση και την παρουσίαση επαγγελματιών στον τομέα της κυβερνοασφάλειας, πληροφορίες και ανάγκες σε όλα τα επίπεδα, σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο

3. ΑΙΤΉΣΕΙΣ ΤΟΥ ECSF

Το παρόν κεφάλαιο καταδεικνύει τον τρόπο με τον οποίο το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας (ECSF) μπορεί να εφαρμοστεί με σπονδυλωτό και ευέλικτο τρόπο με βάση τις ανάγκες των διαφόρων ενδιαφερόμενων μερών.

Τα 12 προφίλ ρόλων που ορίζονται από το ECSF αποτελούν ένα ευέλικτο εργαλείο και ένα τυποποιημένο ευρωπαϊκό πρότυπο

Η ειδική χρήση και πρακτική εφαρμογή εξαρτώνται από πολλούς παράγοντες, όπως η προοπτική της αγοράς, το μέγεθος του οργανισμού, το πλαίσιο μιας συγκεκριμένης επίδοσης και ο συνολικός σκοπός.

Τα 12 προφίλ ρόλων για τους επαγγελματίες του τομέα της κυβερνοασφάλειας που ορίζονται από το ECSF αποτελούν ένα ευέλικτο εργαλείο και ένα τυποποιημένο ευρωπαϊκό πρότυπο αναφοράς για εξατομικευμένη χρήση σε ένα συγκεκριμένο πλαίσιο.

Ο ακόλουθος γενικός οδηγός πέντε βημάτων παρέχει βασικό προσανατολισμό:

Διάγραμμα 4: Αρθρωτός οδηγός πέντε βημάτων για την εφαρμογή του ECSF

1. **Ανάλυση** της κατάστασης του περιβάλλοντος στόχου.
   Συλλογή και επεξεργασία των κατάλληλων πληροφοριών που απαιτούνται σχετικά με την κατάσταση του στοχευόμενου περιβάλλοντος που σχετίζεται με την κυβερνοασφάλεια (π.χ. οργανισμός) για τη δημιουργία βάσης αναφοράς. Προσδιορίστε τα εμπλεκόμενα μέρη και τον στόχο που πρέπει να επιτευχθεί.

2. **Προσδιορισμός** συγκεκριμένων στόχων που πρέπει να επιτευχθούν.
   Να εξετάσει την κατάσταση του στοχευόμενου περιβάλλοντος και να προσδιορίσει τυχόν ειδικές απαιτήσεις σχετικά με την κυβερνοασφάλεια που πρέπει να καλυφθούν ή οποιονδήποτε στόχο που πρέπει να επιτευχθεί από το στοχευόμενο περιβάλλον. Ανάλογα με την κατάσταση, μπορεί να είναι δυνατή η χρήση του ECSF ως ταξινομίας για τον προσδιορισμό των εν λόγω στόχων.

3. **Επιλέξτε** τα κατάλληλα στοιχεία του ECSF.
   Ελέγξτε τα προφίλ του ECSF και επιλέξτε προφίλ που σχετίζονται με μια συγκεκριμένη κατάσταση. Στη συνέχεια, επιλέξτε τα στοιχεία που συμβάλλουν στην κάλυψη των αναγκών ή στην επίτευξη των απαιτούμενων στόχων του στοχευόμενου περιβάλλοντος.

4. **Προσαρμόστε** τα στοιχεία που επιλέξατε ανάλογα με τις ανάγκες σας.
   Πραγματοποίηση κατάλληλων αλλαγών σε επιλεγμένα στοιχεία για την καλύτερη προσαρμογή σε μια συγκεκριμένη κατάσταση και/ή στοχευμένο περιβάλλον. Τα προφίλ ECSF και/ή οι συνιστώσες τους

μπορούν να αναμειγνύονται, να διαιρούνται ή να εντάσσονται σε συγκεκριμένο τομεακό πλαίσιο ανάλογα με τις ανάγκες κάθε κατάστασης.

5. **Εφαρμογή** των εξατομικευμένων στοιχείων στο στοχευόμενο περιβάλλον.
   Να αναλάβει δράση χρησιμοποιώντας τα ειδικά προσαρμοσμένα στοιχεία του ECSF για την κάλυψη των σχετικών με την ασφάλεια στόχων που απαιτούνται για τη βελτίωση της κατάστασης του στοχευόμενου περιβάλλοντος και την επίτευξη του οργανωτικού στόχου.

Στον πίνακα 3 παρουσιάζονται ορισμένα ενδεικτικά παραδείγματα των αιτήσεων ECSF σύμφωνα με τα πέντε στάδια που παρουσιάστηκαν ανωτέρω.

Πίνακας 3: Η σπονδυλωτή προσέγγιση του ECSF στην πράξη

Παράδειγμα	Στάδιο	Περιγραφή
Χρήση της ασφάλειας στον κυβερνοχώρο επαγγελματίες σε οργανισμό	1. Ανάλυση	Ανάλυση της τρέχουσας κατάστασης του οργανισμού που σχετίζεται με την κυβερνοασφάλεια.
	2. Προσδιορισμός	Προσδιορισμός της έλλειψης προσωπικού για τον χειρισμό της αύξησης των ζητημάτων κυβερνοασφάλειας.
	3. Επιλογή	Επιλέξτε το κατάλληλο καθήκον από προφίλ ECSF που αποτυπώνει διαπιστωμένη έλλειψη ή έλλειψη συγκεκριμένων δεξιοτήτων.
	4. Προσαρμογή	Συνδυασμός των προφίλ του ECSF με καθήκοντα που ενδιαφέρουν τον οργανισμό και διάρθρωση νέων ρόλων με τα επικαιροποιημένα καθήκοντα, δεξιότητες και γνώσεις για την κάλυψη των μεταβαλλόμενων οργανωτικών αναγκών και τη δημιουργία τροποποιημένων ρόλων κυβερνοασφάλειας.
	5. Ισχύουν	Χρησιμοποιήστε το νέο προφίλ για να δημιουργήσετε κενές θέσεις εργασίας με στόχο τις ειδικές ανάγκες του οργανισμού.
Κυβερνοασφάλεια των δεξιοτήτων επαγγελματίες	1. Ανάλυση	Κατανόηση των επιχειρηματικών στόχων και της στρατηγικής του οργανισμού.
	2. Προσδιορισμός	Εντοπισμός τυχόν έλλειψης εμπειρογνωσίας και προσωπικού σε τομείς που σχετίζονται με την κυβερνοασφάλεια.
	3. Επιλογή	Χρησιμοποιήστε το/τα προφίλ ECSF για να προσδιορίσετε τις σχετικές δεξιότητες και γνώσεις που δεν διαθέτει ο οργανισμός.
	4. Προσαρμογή	Ανάλυση επιλεγμένων δεξιοτήτων και γνώσεων από το ECSF για τον προσδιορισμό των αναγκών κατάρτισης ενός επαγγελματία στον τομέα της κυβερνοασφάλειας για την κάλυψη των αναγκών του οργανισμού.
	5. Ισχύουν	Προσδιορισμός παρεμβάσεων κατάρτισης για την ενίσχυση των ικανοτήτων του εργατικού δυναμικού του οργανισμού.
Πραγματοποίηση δικών τους επιλογών σταδιοδρομίας	1. Ανάλυση	Επιλέξτε τη σταδιοδρομία που σας ενδιαφέρει.
	2. Προσδιορισμός	Προσδιορίστε την έλλειψη δεξιοτήτων και γνώσεων που απαιτούνται για τη μετάβαση στον τομέα της κυβερνοασφάλειας.
	3. Επιλογή	Προσδιορίστε το ή τα προφίλ του ECSF που θεωρείτε χρήσιμα από την άποψη της εξέλιξης της σταδιοδρομίας και χρησιμοποιήστε τις συνδεδεμένες δεξιότητες, γνώσεις και ικανότητες ως κατευθυντήριες γραμμές για την επανειδίκευση και την αναβάθμιση των δεξιοτήτων.

	4. Προσαρμογή	Ενίσχυση των επιλεγμένων προφίλ ECSF με τη συμπερίληψη πρόσθετων δεξιοτήτων και γνώσεων με βάση τις ατομικές ανάγκες.
	5. Ισχύουν	Προσδιορισμός προγράμματος κατάρτισης που ενσωματώνει την πλειονότητα των δεξιοτήτων και των γνώσεων που απαιτούνται για την επανειδίκευση ή την αναβάθμιση των δεξιοτήτων για το προφίλ.

3.1 ΑΠΑΣΧΌΛΗΣΗ ΕΠΑΓΓΕΛΜΑΤΊΩΝ ΣΤΟΝ ΤΟΜΈΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑΣ — ΕΦΑΡΜΟΓΉ ECSF ΩΣ ΟΡΓΑΝΙΣΜΌΣ

Το ECSF μπορεί να χρησιμοποιηθεί ως οδηγός και χάρτης πορείας που παρέχει μια κοινή αντίληψη μεταξύ των εμπλεκόμενων μερών όσον αφορά τους ρόλους

Το ECSF παρέχει ένα τυποποιημένο σύνολο αναφοράς 12 τυπικών ρόλων που εκτελούνται από επαγγελματίες του τομέα της κυβερνοασφάλειας από οργανωτική άποψη, καλύπτοντας τις ανάγκες κυβερνοασφάλειας των οργανισμών και τις διαδικασίες κυβερνοασφάλειας που πρέπει να ακολουθούνται για τη διασφάλιση των επιχειρηματικών δραστηριοτήτων, των προϊόντων, των υπηρεσιών και των αλυσίδων εφοδιασμού τους. Ως εκ τούτου, το **πλαίσιο παρέχει πολύτιμο οδηγό και χάρτη πορείας όχι μόνο για την οικοδόμηση, την επέκταση και την εκτέλεση λειτουργιών που σχετίζονται με την κυβερνοασφάλεια εντός ενός οργανισμού, αλλά και για τη διασφάλιση της εκπλήρωσης της αποστολής, του οράματος και των στόχων του που σχετίζονται με την κυβερνοασφάλεια. Ως** εκ τούτου, ένας οργανισμός μπορεί να χρησιμοποιεί το ECSF ως σημείο εκκίνησης ή οδηγό για την ταχεία και εύκολη πρόσβαση στους πρωταρχικούς ρόλους που απαιτούνται για τη διαχείριση των κινδύνων κυβερνοασφάλειας και την ανάπτυξη της προσέγγισής του για την κυβερνοασφάλεια. Ταυτόχρονα, τα προφίλ του ECSF παρέχουν μια κοινή αντίληψη μεταξύ των εμπλεκόμενων μερών όσον αφορά τους ρόλους κυβερνοασφάλειας ενός οργανισμού.

Τρία ενδεικτικά παραδείγματα, τα οποία παρουσιάζονται αργότερα στο παρόν κεφάλαιο, έχουν ως στόχο να αναδείξουν την πρακτική εφαρμογή του πλαισίου:

I. ενίσχυση των πρακτικών κυβερνοασφάλειας μιας μικρής εταιρείας·
II. διαδικασία πρόσληψης μεγάλης εταιρείας με αυξανόμενες απαιτήσεις συμμόρφωσης·
III. σχεδιασμός των πόρων κυβερνοασφάλειας σε μεγάλο οργανισμό.

Παράδειγμα Ι: *Η ενίσχυση των πρακτικών κυβερνοασφάλειας μιας μικρής εταιρείας* παρουσιάζει την εφαρμογή του ECSF για την αντιμετώπιση των αναγκών μιας μικρής εταιρείας που επιδιώκει να ενισχύσει τη δομή και την πρακτική της στον τομέα της κυβερνοασφάλειας. Δείχνει τον τρόπο με τον οποίο μια εταιρεία θα μπορούσε να χρησιμοποιήσει το ECSF για να στηρίξει την ανάπτυξη στρατηγικής κυβερνοασφάλειας, συμπεριλαμβανομένου του σχεδιασμού ανθρώπινων πόρων για την κυβερνοασφάλεια και του σχεδιασμού της προμήθειας κυβερνοασφάλειας.

Χρησιμοποιώντας το ECSF ως σημείο εκκίνησης ή ως οδηγός, η εταιρεία δεν χρειάζεται να επινοήσει ή να ερευνήσει βασικούς ρόλους που απαιτούνται για τη βελτίωση της θέσης της στον τομέα της κυβερνοασφάλειας. Οι ρόλοι μπορούν να ανατεθούν σε διαφορετικά πρόσωπα ή να συγχωνευθούν από ένα μόνο ή λίγα μόνο άτομα ανάλογα με τη στρατηγική, τις απαιτήσεις, τις ανάγκες και τον προϋπολογισμό.

Το παράδειγμα δείχνει επίσης τον τρόπο με τον οποίο το ECSF μπορεί να στηρίξει τον οργανισμό στη διαδικασία πρόσληψης, προσδιορίζοντας τους ρόλους και τις αρμοδιότητες κυβερνοασφάλειας που απαιτούνται στο πλαίσιο μιας μικρής εταιρείας. Στο παράδειγμα αυτό, παρέχεται επίσης ανάλυση του ρόλου και των ελλείψεων δεξιοτήτων στον τομέα της κυβερνοασφάλειας, καθώς και επακόλουθη πρόβλεψη των αναγκών σε οργανωτικό επίπεδο. Εκτός από τη στήριξη των διαδικασιών ανθρώπινων πόρων στις προσλήψεις, το ECSF παρέχει επίσης μια κοινή γλώσσα για την προμήθεια υπηρεσιών κυβερνοασφάλειας.

Παράδειγμα Ι: Ενίσχυση των πρακτικών κυβερνοασφάλειας μιας μικρής εταιρείας

Μια μικρή εταιρεία υπηρεσιών υπολογιστικού νέφους στέφθηκε με επιτυχία σε λίγους μόλις μήνες αφότου οι ιδρυτές, τα αδέλφια Alicia και Max, έθεσαν σε εφαρμογή την ιδέα τους για μια καινοτόμο λύση. Το Alicia ήταν το εξειδικευμένο γένος «techie», ενώ το Max ήταν ένα γένος εμπορίας. Δυστυχώς, κανένας από αυτούς δεν είχε εμπειρία στη λειτουργία ή την κατασκευή εταιρείας. Μετά από ένα έτος, η εταιρεία άρχισε να απογειώνεται και, ως εκ τούτου, μετακόμισε στο δικό της γραφείο και απασχολούσε προσωπικό για να αναπτύξει την επιχείρησή της. Κατά τη διάρκεια του ECSF μπορεί να χρησιμοποιείται ως οδηγός παρέχοντας κοινοί κατανόηση.

Στη φάση επέκτασης, κανείς δεν εξέτασε το ενδεχόμενο οργάνωσης της εταιρείας. Πολλοί ρόλοι και καθήκοντα μοιράστηκαν και οι προκλήσεις αντιμετωπίστηκαν με ad hoc τρόπο. Ευτυχώς, δεν σημειώθηκε σοβαρό περιστατικό κυβερνοασφάλειας κατά τη διάρκεια αυτής της μεταβατικής φάσης.

Τελικά, η εταιρεία απέκτησε κάποια έκθεση στα μέσα ενημέρωσης, η οποία είχε ως αποτέλεσμα να αυξηθεί το ενδιαφέρον νέων επενδυτών και πελατών για τη μικρή νεοφυή επιχείρηση. Ωστόσο, οι μεγαλύτεροι πελάτες και επενδυτές ζήτησαν εγγυήσεις και αποδεικτικά στοιχεία για επαρκή μέτρα ασφάλειας και οργανωτική δομή πριν από τη συμμετοχή τους στην εταιρεία. Οι ιδρυτές συνειδητοποίησαν ότι θα έπρεπε να διαμορφώσουν πραγματικά τα πράγματα εντός του οργανισμού τους. Γνώριζαν ότι το κλειδί για την **επιτυχία του οργανισμού ήταν οι** εργαζόμενοι και, για να μπορέσει ο οργανισμός να ακμάσει και να προσφέρει ανθεκτικές υπηρεσίες, **ήταν σημαντικό να καθοριστούν οι ρόλοι και οι αρμοδιότητές τους στον τομέα της κυβερνοασφάλειας**. Ωστόσο, το ερώτημα που πρέπει να απαντηθεί ήταν τι είδους οργάνωση ήταν αναγκαία και ποιοι ρόλοι και τι είδους αρμοδιότητες χρειάστηκε ο οργανισμός;

Οι χρηματοδότες **χρησιμοποίησαν το ECSF και προσδιόρισαν ότι η οργάνωσή τους απαιτούσε πέντε βασικούς ρόλους για** την υποστήριξη της βάσης αναφοράς τους στον τομέα της κυβερνοασφάλειας:

- στρατηγικός διαχειριστής κυβερνοασφάλειας (CISO)
- νομικός υπάλληλος στον τομέα της κυβερνοασφάλειας
- αρχιτέκτονας κυβερνοασφάλειας
- λίγοι φορείς υλοποίησης της κυβερνοασφάλειας
- αντιμετώπιση συμβάντων στον κυβερνοχώρο.

Εξετάζοντας εσωτερικά το κατά **πόσον** οι **υπάλληλοί** τους ήταν **σε θέση να καλύψουν αυτούς τους ρόλους**, διαπίστωσαν ότι ο νομικός λειτουργός τους διαχειριζόταν ήδη τη συμμόρφωση με τα νομικά και κανονιστικά πλαίσια και ότι είχε συμφέρον να **εμπλουτίσει τις ικανότητές της σε νομικά θέματα προστασίας της ιδιωτικής ζωής και ασφάλειας στον κυβερνοχώρο**. Οι ανθρώπινοι πόροι θα είναι σε θέση **να στηρίξουν την αναβάθμιση των δεξιοτήτων χρησιμοποιώντας** έναν κατάλογο βασικών **γνώσεων** και **δεξιοτήτων** που αποκτώνται **από το ECSF**.

Ο αρχιτέκτονας ΤΠΕ του οργανισμού είχε προηγούμενη πείρα στον σχεδιασμό ασφαλών δικτύων και, ως εκ τούτου, με πρόσθετη **κατάρτιση για την επικαιροποίηση και τον εμπλουτισμό** των **ικανοτήτων** της θα μπορούσε επίσης να **καλύψει τις απαιτήσεις αρχιτεκτονικής κυβερνοασφάλειας του οργανισμού**.

Οι διαχειριστές του συστήματος ακολουθούσαν πολλές βέλτιστες πρακτικές κυβερνοασφάλειας, αλλά εργάζονταν κυρίως κατά περίπτωση χωρίς στρατηγική ή δομή. Κατά συνέπεια, οι ιδρυτές **διαπίστωσαν την ανάγκη πρόσληψης στρατηγικού διαχειριστή κυβερνοασφάλειας**. Ανατέθηκε στον υπεύθυνο προσλήψεων να **συντάξει περιγραφή καθηκόντων με βάση το προφίλ CISO του ECSF** και να καταχωρίσει την κενή θέση στον ιστότοπό του.

Τέλος, διαπιστώθηκε ότι οι λειτουργίες αντιμετώπισης συμβάντων της εταιρείας απαιτούσαν τη λειτουργία 24/7 για τη διασφάλιση της συνεχούς λειτουργίας των υπηρεσιών.

Figure 5: The key roles needed as identified using the ECSF and the actions to be taken

Το παράδειγμα μου ανέδειξε πόσο χρήσιμο μπορεί να είναι το ECSF για τα ακόλουθα οφέλη:

- κατανόηση των ρόλων κυβερνοασφάλειας
- προσδιορισμός των απαιτήσεων για το εργατικό δυναμικό
- αξιολόγηση των διαδικασιών και της δομής
- επανειδίκευση και/ή αναβάθμιση των δεξιοτήτων των εργαζομένων
- υποστήριξη της διαδικασίας προσλήψεων
- ανάπτυξη ικανοτήτων κυβερνοασφάλειας
- δημιουργία ασφαλούς και αξιόπιστου οργανισμού στον κυβερνοχώρο
- οικοδόμηση ανθεκτικότητας έναντι κυβερνοεπιθέσεων.

Διάγραμμα 6: Οφέλη από τη χρήση του ECSF, όπως φαίνεται στο παράδειγμα I

Παράδειγμα II*: Η σύνταξη περιγραφής καθηκόντων* καταδεικνύει την εφαρμογή του ECSF κατά τη δημιουργία περιγραφής καθηκόντων. Δείχνει τον τρόπο με τον οποίο το ECSF μπορεί να είναι επωφελές από την άποψη των ανθρώπινων πόρων χωρίς να χρειάζεται να έχει βαθιά κατανόηση του επαγγέλματος του κυβερνοχώρου. Το παράδειγμα αυτό δείχνει πώς μπορεί να δημιουργηθεί μια κενή θέση εργασίας και πώς να αποφευχθεί η δημιουργία παραπλανητικών ή συγκεχυμένων προσδοκιών και πώς μπορεί να προσελκυσθεί προσωπικό με τα κατάλληλα προσόντα. Καταδεικνύει επίσης τον τρόπο συνδυασμού των συνιστωσών ενός προφίλ ρόλων ECSF και τον τρόπο προσαρμογής τους ανάλογα με τις ανάγκες ενός οργανισμού σε θέσεις εργασίας.
Το παράδειγμα αυτό καταδεικνύει τον τρόπο με τον οποίο ένας οργανισμός μπορεί να χρησιμοποιήσει το ECSF για τη δημιουργία περιγραφής ενός ρόλου. Ακόμη και χωρίς υπόβαθρο

ανθρώπινου δυναμικού, είναι δυνατόν να καθοριστούν τα καθήκοντα, οι δεξιότητες και οι γνώσεις που απαιτούνται για έναν υποψήφιο για πρόσληψη, γνωρίζοντας την αποστολή του ρόλου. Εκτός από την παροχή στήριξης στη διαδικασία πρόσληψης, το ECSF μπορεί επίσης να βοηθήσει την εταιρεία να καταρτίσει σχέδια κατάρτισης για το νεοπροσλαμβανόμενο προσωπικό. Αξίζει να σημειωθεί ότι το ECSF δεν παρέχει μόνο μια κοινή γλώσσα για τις δημόσιες συμβάσεις στον τομέα της κυβερνοασφάλειας, αλλά και για σκοπούς ελέγχου, ιδίως όταν εφαρμόζεται η αρχή της λογοδοσίας, και απαιτείται ουσιαστικός και σαφής διαχωρισμός καθηκόντων.

Παράδειγμα ΙΙ: Σύνταξη περιγραφής καθηκόντων

Μια μεγάλη ασφαλιστική εταιρεία επεκτείνει το χαρτοφυλάκιό της στην ασφάλεια στον κυβερνοχώρο, καθώς πολλοί πελάτες αναζητούν αυτή την υπηρεσία. Μετά από μια ελαφρά εσωτερική αναδιάρθρωση και την επικαιροποίηση του καταλόγου προσωπικού, η εταιρεία αποφασίζει να προσθέσει την κυβερνοασφάλεια στο τμήμα συμμόρφωσης. **Κατά συνέπεια, η διοίκηση του τμήματος συμμόρφωσης καταλήγει στο συμπέρασμα ότι πρέπει να προσλάβει υπεύθυνο συμμόρφωσης στον κυβερνοχώρο** για την υποστήριξη της νέας αποστολής.

Το τμήμα ανθρώπινων πόρων της εταιρείας είναι επιφορτισμένο με την **εξεύρεση και την πρόσληψη του καταλληλότερου υποψηφίου**. Δεδομένου ότι η κυβερνοασφάλεια αποτελεί νέο τομέα για τον οργανισμό, η ΥΕ πρέπει επίσης **να δημιουργήσει περιγραφή ρόλου**. Για τον καθορισμό αυτού του νέου ρόλου, οι **ανθρώπινοι πόροι πραγματοποιούν συνεντεύξεις** με **εξειδικευμένα διευθυντικά στελέχη και προσωπικό** για **τον προσδιορισμό των αναγκών** και των **βασικών καθηκόντων** για τη θέση αυτή. Οι ανάγκες αυτές προσδιορίζονται και τα βασικά καθήκοντα που επιλέγονται είναι τα εξής:

- διασφάλιση της συμμόρφωσης και παροχή νομικών συμβουλών και καθοδήγησης σχετικά με τα πρότυπα, τις νομοθετικές και κανονιστικές διατάξεις για την προστασία των δεδομένων και την προστασία των δεδομένων·
- τον εντοπισμό και την τεκμηρίωση των κενών συμμόρφωσης·
- καταρτίζει σχέδιο ελέγχου που περιγράφει τα πλαίσια, τα πρότυπα, τις διαδικασίες και τις ελεγκτικές δοκιμές·
- εκτελεί το σχέδιο ελέγχου και συλλέγει αποδεικτικά στοιχεία και μετρήσεις·
- ανάπτυξη και κοινοποίηση των αποτελεσμάτων του ελέγχου (υποβολή εκθέσεων).

Ο αρμόδιος υπάλληλος ανθρώπινων πόρων αναγνωρίζει ότι πρόκειται για πολύπλοκο ρόλο και ότι δεν υπάρχουν υποδείγματα προσλήψεων που να ανταποκρίνονται στον ρόλο αυτό. **Ως εκ τούτου, πρέπει να δημιουργηθεί και να εγκριθεί από τη διοίκηση νέα περιγραφή και υπόδειγμα ρόλου**.

Ο υπεύθυνος ανθρώπινων πόρων, **που χρησιμοποιεί τώρα το ECSF, αναλύει διαφορετικούς ρόλους εντός του πλαισίου**. Τα συγκεκριμένα καθήκοντα περιλαμβάνονται στα **βασικά καθήκοντα που προσδιορίζονται στους ρόλους του** νομικού τομέα **στον κυβερνοχώρο, του υπεύθυνου πολιτικής & Συμμόρφωσης** και του **Ελεγκτή Κυβερνοασφάλειας**.

Για την εκτέλεση των καθηκόντων αυτών, οι συγκεκριμένες **δεξιότητες και οι απαιτούμενες γνώσεις** είναι οι εξής:

- Δεξιότητες
  - να κατανοούν τις επιπτώσεις των τροποποιήσεων του νομικού πλαισίου στη στρατηγική και τις πολιτικές του οργανισμού για την κυβερνοασφάλεια και την προστασία των δεδομένων·
  - να ακολουθούν και να εφαρμόζουν τα πλαίσια, τα πρότυπα και τις μεθοδολογίες ελέγχου·
  - εφαρμογή ελεγκτικών εργαλείων και τεχνικών·
  - εργάζεστε στο πλαίσιο ομάδας και συνεργάζεστε με συναδέλφους.

- Γνώση
  - προηγμένη γνώση της εθνικής, ενωσιακής και διεθνούς ασφάλειας στον κυβερνοχώρο και των σχετικών προτύπων, νομοθεσίας, πολιτικών και κανονισμών για την προστασία της ιδιωτικής ζωής·
  - γνώση της συμμόρφωσης με την ασφάλεια των πληροφοριών και των κανονιστικών απαιτήσεων σε διεθνές, εθνικό και ενωσιακό επίπεδο·

- βασική κατανόηση της αποθήκευσης, της επεξεργασίας και της προστασίας δεδομένων εντός των συστημάτων, των υπηρεσιών και των υποδομών.

Μια **νέα περιγραφή των ρόλων**, προσαρμοσμένη στις ανάγκες των εταιρειών, μπορεί πλέον να δημιουργηθεί με **τη χαρτογράφηση και τον συνδυασμό** τμημάτων του προφίλ για τον ρόλο του **νομικού ρόλου του κυβερνοχώρου, του υπεύθυνου πολιτικής & Συμμόρφωσης** και τμημάτων του προφίλ για τον ρόλο του **ελεγκτή κυβερνοασφάλειας**. Είναι σημαντικό ότι, με τη χαρτογράφηση στο πλαίσιο, αυτός ο νέος μοναδικός **ρόλος βασίζεται στο βασικό περιεχόμενο του ECSF**. Αυτό παρέχει έναν ομοιόμορφο και δομημένο ρόλο που μπορεί να αναδειχθεί στην προέλευσή του.

Διάγραμμα 7: Προφίλ εργασίας στον τομέα της κυβερνοασφάλειας που δημιουργήθηκε με βάση τα προφίλ ρόλων του ECSF

Μετά τη χαρτογράφηση αυτή στο ECSF, η απαιτούμενη περιγραφή ρόλου είναι διαθέσιμη και μπορεί να χρησιμοποιηθεί για τη σύνταξη του ρόλου και της επακόλουθης περιγραφής καθηκόντων που πρέπει να λάβει εσωτερική έγκριση και να δημοσιεύσει στον ιστότοπο της εταιρείας για τις προσλήψεις. Περαιτέρω στοιχεία, όπως η αποστολή προφίλ, μπορούν να χρησιμοποιηθούν ως εισαγωγικό κείμενο για τη δημοσίευση της παρούσας κενής θέσης.

Το παράδειγμα ΙΙ κατέδειξε πόσο χρήσιμο μπορεί να είναι το ECSF για τα ακόλουθα οφέλη:

- κατανόηση των ρόλων κυβερνοασφάλειας
- προσδιορισμός των απαιτήσεων για το εργατικό δυναμικό
- προσδιορισμός των απαιτήσεων για τους ρόλους
- υποστήριξη της διαδικασίας προσλήψεων
- υποστήριξη της δημιουργίας εξατομικευμένου υποδείγματος κενών θέσεων
- χρήση κοινής γλώσσας για τις κενές θέσεις εργασίας.

Διάγραμμα 8: Οφέλη από τη χρήση του ECSF που παρουσιάζεται στο παράδειγμα ΙΙ

***Παράδειγμα III**: Μια μεγάλη εταιρεία με την κύρια δραστηριότητά της εκτός των ΤΠΕ πρέπει να δημιουργήσει ένα τμήμακυβερνοασφάλειας* αποδεικνύει την εφαρμογή του ECSF κατά τη δημιουργία νέου τμήματος κυβερνοασφάλειας και την προετοιμασία στρατηγικής κυβερνοασφάλειας για την εταιρεία. Προτείνει επίσης την κατηγοριοποίηση των 12 προφίλ σε τέσσερις (4) μακροτομείς για κατανόηση και επικοινωνία υψηλού επιπέδου. Δείχνει τον τρόπο με τον οποίο ένας μεγάλος οργανισμός μπορεί να χρησιμοποιήσει το ECSF για να στηρίξει την ανάπτυξη στρατηγικής κυβερνοασφάλειας, συμπεριλαμβανομένου του σχεδιασμού ανθρώπινων πόρων και της ανάπτυξης ταλέντων στον τομέα της κυβερνοασφάλειας.

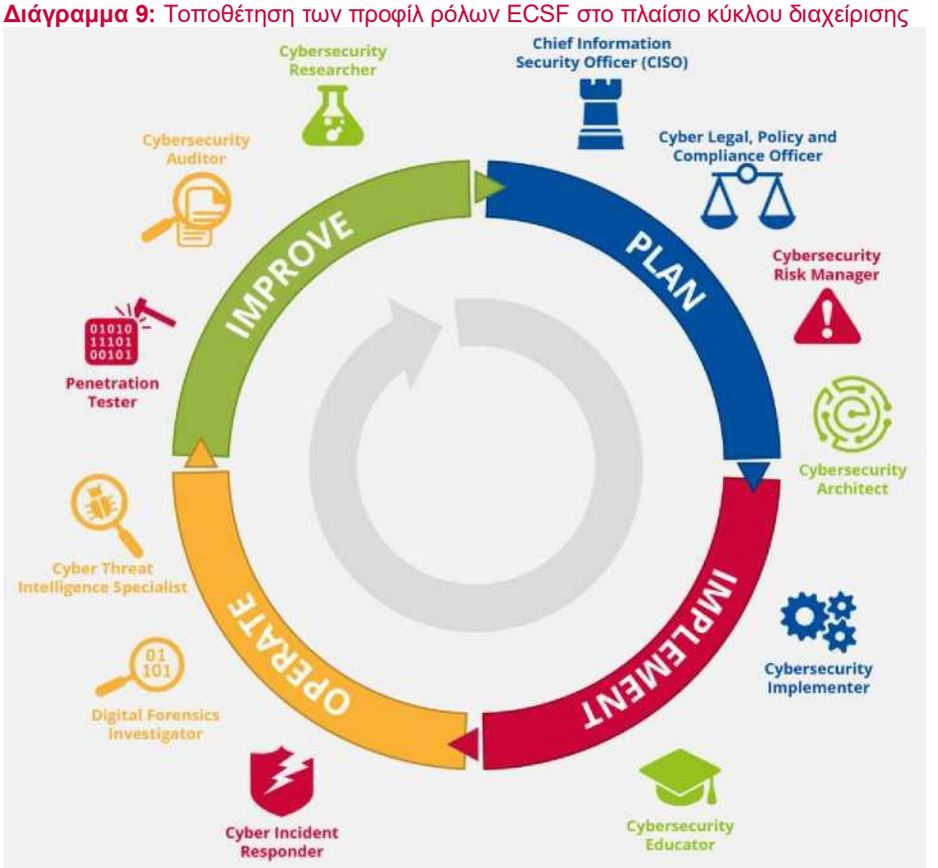
Παράδειγμα III: Μια μεγάλη εταιρεία με την κύρια δραστηριότητά της εκτός των ΤΠΕ πρέπει να δημιουργήσει ένα τμήμα κυβερνοασφάλειας

Μια μεγάλη εταιρεία με βασική δραστηριότητα που δεν σχετίζεται με τις ΤΠΕ ή τις υπηρεσίες κυβερνοασφάλειας συνειδητοποίησε την ανάγκη προστασίας των πολύτιμων περιουσιακών στοιχείων της από απειλές κατά της κυβερνοασφάλειας. Πράγματι, η εγκριθείσα επιχειρηματική στρατηγική ενσωμάτωσε ένα μαζικό σχέδιο για την ψηφιοποιήσει των επιχειρηματικών διαδικασιών και η εξάρτηση από τις ΤΠΕ αυξήθηκε σημαντικά για τις κρίσιμες επιχειρηματικές δραστηριότητες.

Δεδομένου ότι η εταιρεία δεν διέθετε εσωτερική εμπειρογνωσία για τον χειρισμό κινδύνων κυβερνοασφάλειας, το διοικητικό συμβούλιο αποφάσισε να προσλάβει υπεύθυνο πληροφοριών ασφάλειας (CISO) για τον **καθορισμό της συνολικής στρατηγικής κυβερνοασφάλειας** σύμφωνα με τους επιχειρηματικούς στόχους της εταιρείας. Αυτό θα απαιτούσε επίσης **τη σύσταση τμήματος** για **την αντιμετώπιση των κινδύνων κυβερνοασφάλειας**.

Ο CISO, ο οποίος ορίσθηκε πρόσφατα, **χρησιμοποίησε το ECSF ως κατευθυντήρια γραμμή** και **ως σταθερό σημείο αναφοράς** για **τους ρόλους κυβερνοασφάλειας που απαιτούνται** για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας. Το χρησιμοποίησε ως **ευέλικτο εργαλείο** για να βοηθήσει στη **δομή ενός τμήματος κυβερνοασφάλειας**. Αναγνωρίζει επίσης ότι, για την παροχή σαφούς σχηματικού σχήματος, θα ήταν χρήσιμο να τοποθετηθούν **οι ρόλοι του ECSF στο πλαίσιο ενός κύκλου διαχείρισης**, σε τέσσερις (4) μακροτομείς: σχέδιο, β) Εφαρμογή, γ) Λειτουργία και δ) Βελτίωση.

Διάγραμμα 9: Τοποθέτηση των προφίλ ρόλων ECSF στο πλαίσιο κύκλου διαχείρισης



Στον μακροτομέα του σχεδίου καθορίστηκαν προτεραιότητες και στόχοι, αναπτύχθηκαν στρατηγικές, πολιτικές και σχέδια δράσης, καθορίστηκαν αρχιτεκτονικές, διατέθηκαν πόροι. Σε αυτόν τον μακροοικονομικό τομέα, ο CISO, ο υπεύθυνος πολιτικής και συμμόρφωσης, ο διαχειριστής κινδύνου και τα προφίλ αρχιτέκτονα τοποθετήθηκαν με φυσικό τρόπο.

Η εφαρμογή μέτρων κυβερνοασφάλειας (Implementation menter) και η κατάρτιση και η ευαισθητοποίηση (εκπαιδευτής) ανατέθηκαν στον μακροοικονομικό τομέα υλοποίησης.

Οι καθημερινές επιχειρήσεις ήταν η πλέον «απτή» περιοχή. Η αντιμετώπιση περιστατικών (συμπεριλαμβανομένων των ομάδων SOC), οι εγκληματολογικές δραστηριότητες αποτελούν καθημερινές δραστηριότητες ειδικών στον τομέα της κυβερνοασφάλειας. Το προφίλ πληροφοριών σχετικά με απειλές θεωρήθηκε επίσης ως επιχειρησιακός τομέας, καθώς οι εν λόγω επαγγελματίες ασχολούνται με επιχειρησιακά δεδομένα χρησιμοποιώντας πολλαπλές πηγές.

Ο δοκιμαστής διείσδυσης (δοκιμές για τρέχουσες και αναδυόμενες απειλές), ο ερευνητής (εισαγωγή νέων τεχνολογιών και λύσεων) και ο ελεγκτής (εντοπισμός κενών) υποστηρίζουν το στάδιο της βελτίωσης.

Ωστόσο, δεδομένου ότι το ECSF είναι ένα ευέλικτο εργαλείο για εξατομικευμένη χρήση σε ένα συγκεκριμένο πλαίσιο, ο CISO **εφάρμοσε τον οδηγό 5 βημάτων για την προσαρμογή των προφίλ ρόλων στις ειδικές ανάγκες και τους στόχους** της. Η ανάλυση των προφίλ του ECSF την βοήθησε να **καθορίσει τα σχέδια πόρων** που απαιτούνται για την επίτευξη του εταιρικού στόχου.

Στη μακροπεριοχή του Σχεδίου, αποφάσισε:

- να είναι επιφορτισμένη με καθήκοντα πολιτικής και συμμόρφωσης για τον εξορθολογισμό της οργανωτικής δομής· να προσλάβει αρχιτέκτονα κυβερνοασφάλειας, ο οποίος θα

συμβάλει στον καθορισμό της συνολικής στρατηγικής αρχιτεκτονικής για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας και τη διασφάλιση ασφαλών λύσεων εκ σχεδιασμού για τη στήριξη του ψηφιακού μετασχηματισμού·

- να προσλάβει διαχειριστή κινδύνων κυβερνοασφάλειας, ο οποίος θα συμβάλει στην αξιολόγηση της στάσης των εταιρειών όσον αφορά τους κινδύνους κυβερνοασφάλειας και θα συμβάλει στον καθορισμό σχεδίων δράσης για τη διαχείριση των εντοπισθέντων κινδύνων.

Στον μακροτομέα της υλοποίησης, **αξιοποίησε τις συνιστώσες δεξιοτήτων και γνώσεων του ECSF** για να **κατανοήσει ποια αναβάθμιση των δεξιοτήτων θα απαιτούνταν** για τη μόχλευση των διαθέσιμων εσωτερικών πόρων ή, εναλλακτικά, για να αποφασίσει να προσλάβει εξωτερικά. Η πολυεθνική εταιρεία διέθετε υφιστάμενη ομάδα εκπαιδευτών σε διαφορετικό τομέα. Ωστόσο, δεν υπήρχε ειδική ομάδα για τον σχεδιασμό και τη διεξαγωγή μαθημάτων ευαισθητοποίησης ή κατάρτισης στον τομέα της κυβερνοασφάλειας. Το CISO **διερεύνησε κατά πόσον ορισμένοι από τους εκπαιδευτές διέθεταν τις δεξιότητες και τις γνώσεις που απαριθμούνται στο ECSF** και το ενδιαφέρον **να συμμετάσχουν στη νέα ομάδα** της.
Στην επιχειρησιακή μακροπεριοχή, το CISO εξέτασε τον τρόπο διαχείρισης των καθημερινών επιχειρήσεων κυβερνοασφάλειας και αποφάσισε να **δημιουργήσει παγκόσμια επιχειρησιακά κέντρα ασφάλειας με φορείς αντιμετώπισης συμβάντων** που εργάζονται σε διάφορες ηπείρους για την παροχή στήριξης 24/7. Επιπλέον, **χρησιμοποιήθηκε ειδικός σε θέματα πληροφοριών σχετικά** με τις απειλές για την παροχή επιχειρησιακών γνώσεων με σκοπό την καθοδήγηση της θήρας απειλών και τον μετριασμό του κινδύνου. Η CISO κατέληξε στο συμπέρασμα ότι **δεν υπήρχε ανάγκη πρόσληψης ψηφιακού εγκληματολογικού ερευνητή**, αλλά **μάλλον εξειδικευμένης εταιρείας παροχής συμβουλών** για τυχόν **εγκληματολογικές ανάγκες**.

Στην ευρύτερη μακροπεριοχή, η CISO αποφάσισε να προσλάβει **εξωτερικό πάροχο υπηρεσιών για δοκιμές διείσδυσης** με στόχο τη δοκιμή της ανθεκτικότητας των εταιρικών υποδομών και εφαρμογών. Ο CISO αξιολόγησε επίσης την ικανότητα της ομάδας εσωτερικού ελέγχου και αποφάσισε να **προσλάβει ελεγκτή κυβερνοασφάλειας για** τον έλεγχο των πολιτικών που σχετίζονται με την ασφάλεια. Η CISO δεν θεώρησε αναγκαίο να προσλάβει ερευνητή στον τομέα της κυβερνοασφάλειας, δεδομένου ότι η έρευνα στον τομέα της κυβερνοασφάλειας δεν ενέπιπτε στο πεδίο του οργανισμού της.

Συνοψίζοντας, το παράδειγμα ΙΙΙ υπογράμμισε πόσο χρήσιμο μπορεί να είναι το ECSF για τα ακόλουθα οφέλη:

κατανόηση των ρόλων κυβερνοασφάλειας
συνδρομή στη δημιουργία οργανωτικής δομής που θα προσδιορίζει τις απαιτήσεις για τους ρόλους κυβερνοασφάλειας
παροχή βοήθειας στον σχεδιασμό των ανθρώπινων πόρων
αναβάθμιση των δεξιοτήτων των εργαζομένων
υποστήριξη της αξιολόγησης των υποψηφίων
χρήση κοινής ορολογίας για τη συνεργασία.

Διάγραμμα 10: Οφέλη από τη χρήση του ECSF που καταδεικνύονται από το παράδειγμα ΙΙΙ


organisation structure supporting
upskilling employees
cybersecurity roles understanding
human resource planning
common terminology for collaboration
role requirements identification
assessment of candidates

3.2 ΑΠΌΚΤΗΣΗ ΔΕΞΙΟΤΉΤΩΝ ΑΠΌ ΕΠΑΓΓΕΛΜΑΤΊΕΣ ΣΤΟΝ ΤΟΜΈΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑΣ — ΕΦΑΡΜΟΓΉ ΤΟΥ ECSF ΩΣ ΠΆΡΟΧΟΣ ΜΆΘΗΣΗΣ

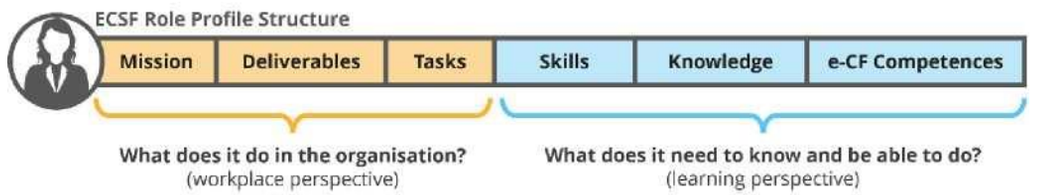
Το ECSF προσφέρει μια κοινή γλώσσα και λεξιλόγιο για την ανάπτυξη επαγγελματικών δεξιοτήτων κυβερνοασφάλειας στους παρόχους προγραμμάτων μάθησης και ιδρυμάτων μάθησης κάθε είδους, όπως η τριτοβάθμια εκπαίδευση, η επαγγελματική εκπαίδευση και κατάρτιση (ΕΕΚ) ή οποιοδήποτε άλλο εκπαιδευτικό πρόγραμμα ή κατάρτιση που σχετίζεται με την κυβερνοασφάλεια. Τα καθορισμένα προφίλ ρόλων παρέχουν μια προσέγγιση με γνώμονα τον χώρο εργασίας στον τομέα της κυβερνοασφάλειας, η οποία είναι ενσωματωμένη σε ευρωπαϊκό επίπεδο, για τη σύνδεση των υφιστάμενων απαιτήσεων για την επαγγελματική πρακτική με τα προγράμματα σπουδών και τα προγράμματα μάθησης που σχετίζονται με την κυβερνοασφάλεια.

Το ECSF καθορίζει τις τυπικές απαιτήσεις ενός προφίλ από δύο θεμελιώδεις απόψεις.

- Τι κάνει αυτός ο ρόλος στον οργανισμό;
  Εξετάζει την προοπτική του χώρου εργασίας (ενότητες προφίλ σχετικά με την αποστολή, τα παραδοτέα και τα καθήκοντα)

- Τι πρέπει να γνωρίζει και να είναι σε θέση να αναλάβει αυτός ο ρόλος;
  Εξέταση της μαθησιακής προοπτικής (ενότητες προφίλ σχετικά με τις δεξιότητες, τις γνώσεις και τις ικανότητες e-CF)

Διάγραμμα 11: Τα τμήματα προφίλ ρόλων του ECSF που συνδέονται με τον χώρο εργασίας



Το ECSF τοποθετεί τα μαθησιακά αποτελέσματα σε πραγματικό εργασιακό πλαίσιο. Ειδικότερα, οι περιγραφές στα προφίλ ρόλων του ECSF επιτρέπουν στους παρόχους προγραμμάτων μάθησης να επανεξετάζουν τα προγράμματα σπουδών τους με δομημένο και συστηματικό τρόπο, μεταξύ άλλων από την άποψη των επαγγελματιών.

Το ECSF προσφέρει κοινή γλώσσα και λεξιλόγιο για την ανάπτυξη επαγγελματικών δεξιοτήτων κυβερνοασφάλειας στους παρόχους προγραμμάτων μάθησης και ιδρυμάτων μάθησης κάθε

Όπως φαίνεται στο παράρτημα Β.2, το ECSF μπορεί να συμβάλει σε διάφορες δραστηριότητες που αναλαμβάνονται σε ακαδημαϊκά ιδρύματα.

- Το ECSF μπορεί να χρησιμεύσει για την ανάπτυξη ή την επικαιροποίηση του μαθησιακού αποτελέσματος των μαθημάτων και την ευθυγράμμισή του με τις ανάγκες της αγοράς εργασίας. Οι δεξιότητες, οι γνώσεις και οι ικανότητες στο πλαίσιο ενός προφίλ ρόλου μπορούν να χρησιμοποιηθούν για την καθοδήγηση της φάσης σχεδιασμού των προγραμμάτων σπουδών και την υποστήριξη του καθορισμού των επιθυμητών μαθησιακών αποτελεσμάτων. Για παράδειγμα, κατά την ανάλυση των εκπαιδευτικών αναγκών μιας συγκεκριμένης εργασίας στον τομέα της κυβερνοασφάλειας, ένα ευθυγραμμισμένο προφίλ ECSF παρέχει ένα σταθερό σημείο εκκίνησης για την κατανόηση των σχετικών εκπαιδευτικών απαιτήσεων.

- Το ECSF θα μπορούσε να χρησιμεύσει ως εργαλείο συνεργασίας για τη δημιουργία κοινών ακαδημαϊκών προγραμμάτων και για την κινητικότητα των σπουδαστών.

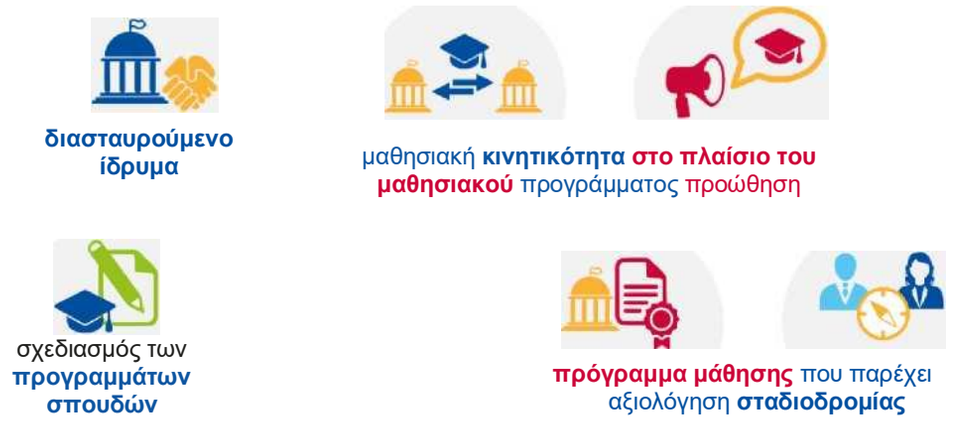
- Το ECSF θα μπορούσε να χρησιμεύσει ως βάση για τον καθορισμό ενός πλαισίου για ένα πρόγραμμα σπουδών κυβερνοασφάλειας, το οποίο θα βοηθήσει τα πανεπιστήμια να χαρτογραφήσουν το κύριο επίκεντρο του προγράμματός τους για την ασφάλεια στον

κυβερνοχώρο και να το κοινοποιήσουν στους σπουδαστές.

Όπως φαίνεται στο παράρτημα Β.1, το ECSF αντιμετωπίζει ορισμένες από τις προκλήσεις που εντοπίστηκαν στο ευρωπαϊκό τοπίο επαγγελματικών προσόντων στον τομέα της κυβερνοασφάλειας. Ειδικότερα:

- το ECSF υποστηρίζει μια διατομεακή και διακλαδική συμφωνημένη ορολογία σχετικά με τις δεξιότητες κυβερνοασφάλειας·
- το ECSF θα μπορούσε να στηρίξει την ανάπτυξη μιας ολοκληρωμένης πλατφόρμας δεξιοτήτων για την παροχή επικαιροποιημένων πληροφοριών σχετικά με την αγορά εργασίας, τις ικανότητες, τα μαθήματα κατάρτισης, τα συστήματα πιστοποίησης και έναν χάρτη πορείας σταδιοδρομίας.

Διάγραμμα 12: Οφέλη από τη χρήση του ECSF ως παρόχου

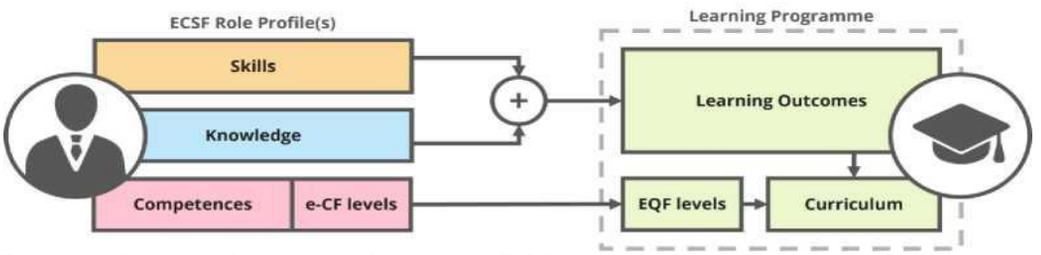


Το ECSF μπορεί να χρησιμοποιηθεί ως εργαλείο επικοινωνίας μεταξύ

Στο πλαίσιο της ανάπτυξης επαγγελματικών προσόντων και σχεδιασμού προγραμμάτων σπουδών στον τομέα της κυβερνοασφάλειας, τα προφίλ ρόλων του ECSF χρησιμεύουν ως εργαλείο επικοινωνίας μεταξύ εργοδοτών και εκπαιδευτών για τη βελτίωση της διαδικασίας διαβούλευσης και των συνεργατικών αποτελεσμάτων. Ο εργοδότης μπορεί γρήγορα να καθορίσει τις απαιτούμενες δραστηριότητες ή καθήκοντα και να εργαστεί αναδρομικά για να προσδιορίσει τις ικανότητες, τις δεξιότητες και τις γνώσεις που θα πρέπει να συμπεριλάβουν στα προγράμματα σπουδών οι εκπαιδευτές γνώσεων. Η προσέγγιση αυτή επιταχύνει σημαντικά τον σχεδιασμό των προγραμμάτων σπουδών που συμφωνούνται μεταξύ εργοδοτών, κυβερνήσεων και εκπαιδευτικών.

Στο γράφημα 13 παρουσιάζεται ο τρόπος με τον οποίο τα τμήματα των προφίλ ρόλων του ECSF

Διάγραμμα 13: Προφίλ ECSF που καθοδηγούν την επαγγελματική



Που αφορούν τις ικανότητες, τις γνώσεις και τις δεξιότητες μπορούν να χρησιμοποιηθούν για τον καθορισμό των μαθησιακών αποτελεσμάτων, τον προσδιορισμό των κατάλληλων επιπέδων μαθησιακών προγραμμάτων και τη δημιουργία προγραμμάτων σπουδών για επαγγέλματα κυβερνοασφάλειας. Δεδομένου ότι οι γνώσεις και οι δεξιότητες, όπως όλα τα περιεχόμενα των περιγραφών ρόλων, παρέχονται ως καθοδηγητικά παραδείγματα ευέλικτης προσαρμογής στο πλαίσιο, μπορούν επίσης να χρησιμοποιηθούν και άλλες πηγές**8**.

Σύνδεση των επιπέδων μάθησης (ΕΠΕΠ) και των επιπέδων επάρκειας στον χώρο εργασίας (e-CF)

Το ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων (ΕΠΕΠ) είναι ένα κοινό ευρωπαϊκό πλαίσιο αναφοράς για τα επαγγελματικά προσόντα. Σκοπός του ΕΠΕΠ είναι η σύγκριση προσόντων και μαθησιακών αποτελεσμάτων που προκύπτουν σε διάφορες χώρες και εθνικά

Τα τμήματα8 δεξιοτήτων, γνώσεων και ικανοτήτων του ECSF δεν είναι ούτε εξαντλητικά ούτε περιοριστικά, επιτρέποντας στον χρήστη να τα εμπλουτίσει συμπεριλαμβάνοντας επίσης εξωτερικούς πόρους, π.χ. τον φορέα γνώσης για την κυβερνοασφάλεια (CyBOK) https://www.cybok.org/.τηνταξινόμηση του JRC https://joint-research-centre.ec.europa.eu/publications/unified-conceptual- frameworkworkks-skills-and-Compeces_en

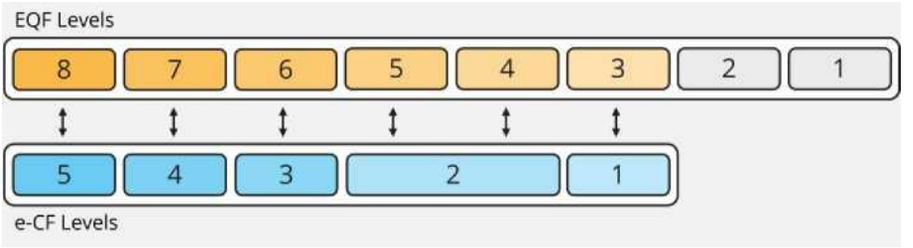
εκπαιδευτικά συστήματα. Το ΕΠΕΠ βασίζεται στα εξής:
Σύσταση σχετικά με το ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων για τη διά βίου μάθηση που εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στις 23 Απριλίου 20089.

Το ΕΠΕΠ ορίζει οκτώ (8) επίπεδα μορφωτικού επιπέδου με περιγραφικούς δείκτες που διαφοροποιούν κάθε επίπεδο. Το κριτήριο για κάθε επίπεδο βασίζεται στην αξιολόγηση της γνώσης, των δεξιοτήτων, της ευθύνης και της αυτονομίας.

Το **ευρωπαϊκό πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)**, πρότυπο EN 16234-1, που χρησιμοποιείται από το ECSF, είναι ένα κοινό ευρωπαϊκό πλαίσιο για τις επαγγελματικές ικανότητες, τις γνώσεις και τις δεξιότητες στον τομέα των ΤΠΕ10. Αφορά τις ικανότητες που απαιτούνται και εφαρμόζονται στον χώρο εργασίας. Η διάσταση 3 του e-CF καθορίζει τα επίπεδα ικανοτήτων που προκύπτουν από την επάρκεια στον χώρο εργασίας. Υπάρχουν πέντε (5) καθορισμένα επίπεδα ικανοτήτων e-1 έως e-5 σε σχέση με τα επίπεδα μάθησης 8 έως 3 του ΕΠΕΠ (τα επίπεδα 1 και 2 του ΕΠΕΠ δεν είναι συναφή στο πλαίσιο αυτό).

Η σχέση μεταξύ των επιπέδων e-CF e-1 και e-5 με τα επίπεδα 3-8 του ΕΠΕΠ απεικονίζεται κατωτέρω:

Διάγραμμα 14: Σχέση μεταξύ των επιπέδων ΕΠΕΠ και e-CF



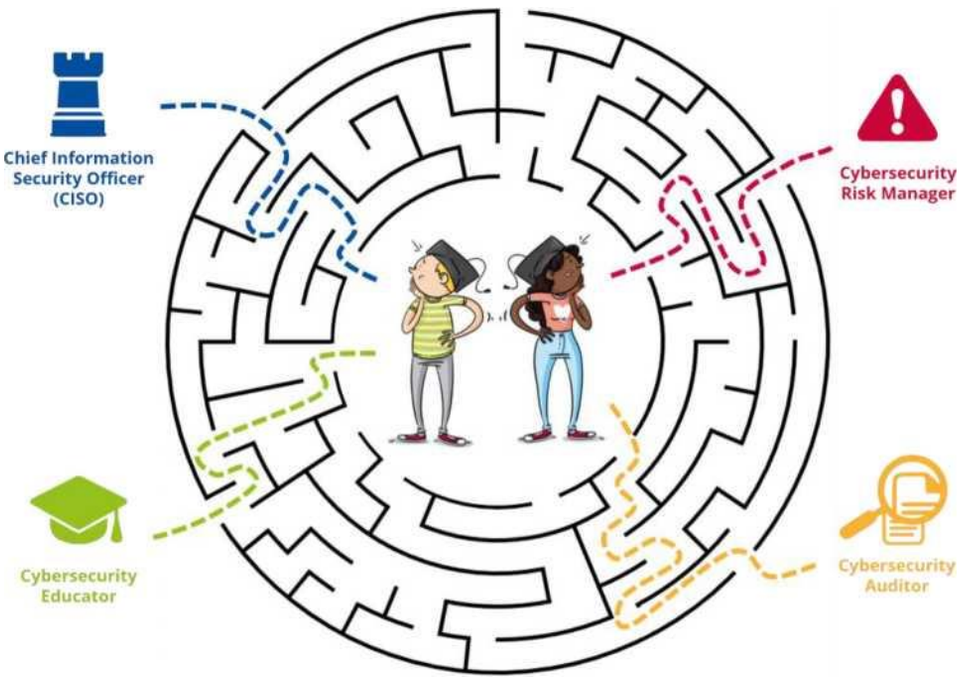
Λόγω αυτής της συστηματικά ανεπτυγμένης σχέσης, είναι δυνατόν να συσχετιστούν τα επίπεδα επάρκειας του e-CF με τα επίπεδα μάθησης του ΕΠΕΠ. Η σχέση, λόγω της διαφορετικής φύσης κάθε πλαισίου, δεν είναι πλήρως ισοδύναμη. Ωστόσο, μπορεί να εφαρμοστεί για την αύξηση της διαφάνειας και την **παροχή κοινής γλώσσας μεταξύ των απαιτήσεων για τις επαγγελματικές ικανότητες στον χώρο εργασίας και των σχετικών προσόντων από εκπαιδευτικά ιδρύματα**11. Ως εκ τούτου, τα επίπεδα ικανοτήτων e-CF που ενσωματώνονται στα προφίλ ρόλων του ECSF μπορούν, συνεπώς, να χρησιμοποιηθούν ως γενικός οδηγός για τα απαιτούμενα επίπεδα εκπαίδευσης.

9Ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων για τη διά βίου μάθηση
10EN16234-1: 2019: πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF) — ένα κοινό ευρωπαϊκό πλαίσιο για τους επαγγελματίες ΤΠΕ σε όλους τους τομείς
11Για περαιτέρω πρακτικές οδηγίες, βλ.: CEN/TS 17699: 2022 Κατευθυντήριες γραμμές για την ανάπτυξη επαγγελματικών προγραμμάτων σπουδών ΤΠΕ σύμφωνα με το πρότυπο EN16234-1 (e-CF)

3.3 ΕΠΙΛΟΓΉ ΣΤΑΔΙΟΔΡΟΜΊΑΣ — ΕΦΑΡΜΟΓΉ ΤΟΥ ECSF ΩΣ ΜΕΜΟΝΩΜΈΝΟΥ ΕΠΑΓΓΕΛΜΑΤΊΑ

Η κοινή γλώσσα που ορίζεται από το ECSF μπορεί να χρησιμοποιηθεί για την αποσαφήνιση τυχόν σύγχυσης μεταξύ των επαγγελματικών ρόλων στον τομέα της κυβερνοασφάλειας και των εκπαιδευτικών προγραμμάτων κυβερνοασφάλειας. Παρέχοντας κοινή γλώσσα και σαφή περιγραφή των επαγγελματικών ρόλων στον τομέα της κυβερνοασφάλειας, των καθηκόντων που αναμένεται να εκτελέσουν, καθώς και των δεξιοτήτων, των ικανοτήτων και των γνώσεων που απαιτούνται, το ECSF μπορεί να οικοδομήσει μια κοινή αντίληψη και να παράσχει τη σαφήνεια που απαιτείται για την προσέλκυση νέων ατόμων στον τομέα της κυβερνοασφάλειας ή για την

Διάγραμμα 15: Χρήση του ECSF για τον καθορισμό της



παροχή βοήθειας κατά τον σχεδιασμό της σταδιοδρομίας τους.

Το ECSF μπορεί να οικοδομήσει μια κοινή αντίληψη και να παράσχει τη σαφήνεια που απαιτείται για να προσελκύσει νέα άτομα στον τομέα της κυβερνοασφάλειας ή να τα

Οι επαγγελματίες που εργάζονται ήδη σε θέσεις σχετικές με την κυβερνοασφάλεια μπορούν να χρησιμοποιούν το ECSF ως οδηγό για την πρόοδο στον τομέα τους. Με τη χαρτογράφηση των δεξιοτήτων και των γνώσεων τους στα προφίλ ρόλων του ECSF που παρουσιάζουν ενδιαφέρον, τα άτομα μπορούν να εντοπίσουν τυχόν ελλείπουσες δεξιότητες ή γνώσεις που χρειάζονται για να αναπτύξουν, να μάθουν ή να μάθουν, ώστε να είναι έτοιμα να καλύψουν μελλοντικές εργασιακές απαιτήσεις ή πιθανές μεταβάσεις μεταξύ ρόλων κυβερνοασφάλειας κατά την εξέλιξη της επαγγελματικής τους σταδιοδρομίας. Αυτό συμβάλλει στον διάλογο μεταξύ εργαζομένων και εργοδοτών κατά τον σχεδιασμό της συνεχούς εκπαίδευσης στον τομέα της κυβερνοασφάλειας. Όπως επισημαίνει το ECSF τόσο στην τυπική όσο και στη μη τυπική μαθησιακή πορεία, βοηθά επίσης τους νεοεισερχόμενους που δεν γνωρίζουν πού να ξεκινήσουν. Η προσθήκη σε προηγούμενες γνώσεις και ικανότητες είναι συχνά ευκολότερη από την πλήρη επανεκκίνηση. Το παράρτημα Β.6 πραγματεύεται το θέμα αυτό και παρέχει βαθύτερες πληροφορίες και παραδείγματα όσον αφορά τη «λήψη ατομικών αποφάσεων σταδιοδρομίας» με τη χρήση του ECSF.

Χρησιμοποιώντας το ECSF ως βάση αναφοράς, ένα άτομο μπορεί να προσδιορίσει τις απαιτούμενες ικανότητες και δεξιότητες για τη μετάβαση από τον έναν ρόλο στον άλλο ή για τον προσδιορισμό των τρεχουσών αναγκών κατάρτισης.

Η κοινή γλώσσα που ορίζεται από το ECSF μπορεί να είναι χρήσιμη για τα άτομα που αναζητούν

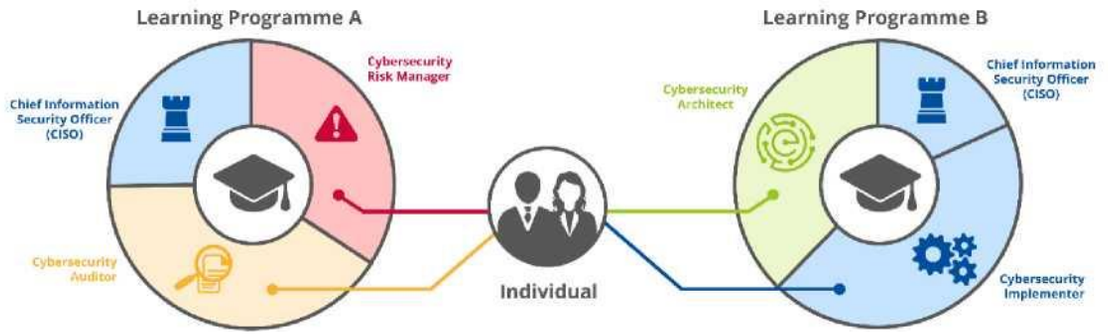
εργασία στον τομέα της κυβερνοασφάλειας. Το ECSF μπορεί να βοηθήσει στο φιλτράρισμα των θέσεων εργασίας και στην κατανόηση της περιγραφής των θέσεων εργασίας, ενώ μπορεί επίσης να διευκολύνει τη συνολική κινητικότητα της εργασίας στο πλαίσιο της κυβερνοασφάλειας μέσω της χαρτογράφησης των δεξιοτήτων, των γνώσεων και των ικανοτήτων του ατόμου στο ECSF.

Η κυβερνοασφάλεια αποτελεί καλή ευκαιρία σταδιοδρομίας ακόμη και για άτομα που επί του παρόντος ειδικεύονται σε άλλους τομείς και, ως εκ τούτου, η επανειδίκευση και η μετάβασή τους στον τομέα της κυβερνοασφάλειας είναι ένας καλός τρόπος για την κάλυψη των αναγκών της αγοράς σε εργατικό δυναμικό και τη μείωση των ελλείψεων εργατικού δυναμικού στον εν λόγω τομέα. Δεδομένου ότι η κυβερνοασφάλεια είναι επιστημονικό θέμα, μια τέτοια αλλαγή σταδιοδρομίας θα μπορούσε να είναι ταχύτερη για άτομα με υπόβαθρο που προσεγγίζει μία από τις κύριες πτυχές του τομέα**12**:

- **τεχνικά** — σχετικά με την τεχνολογία, συγκεκριμένες τεχνολογικές προσεγγίσεις και λύσεις που μπορούν να χρησιμοποιηθούν για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και της τρομοκρατίας στον κυβερνοχώρο·
- **ανθρώπινοι** — που σχετίζονται με ανθρώπινους παράγοντες, πτυχές συμπεριφοράς, ζητήματα προστασίας της ιδιωτικής ζωής, καθώς και ευαισθητοποίηση και γνώση της κοινωνίας όσον αφορά το έγκλημα στον κυβερνοχώρο και τις τρομοκρατικές απειλές·
- **οργανωτικά** — σχετικά με τις διεργασίες, τις διαδικασίες και τις πολιτικές εντός των οργανισμών, καθώς και τη συνεργασία (δημόσιου-ιδιωτικού και δημόσιου τομέα) μεταξύ οργανισμών·
- **κανονιστικές** — σχετικές με τις νομοθετικές διατάξεις, την τυποποίηση και την εγκληματολογική έρευνα.

Με τη σαφή κατανόηση των κύριων προφίλ των ρόλων κυβερνοασφάλειας στον τομέα και μιας κοινής γλώσσας κυβερνοασφάλειας σε ευρύτερο φάσμα τομέων, όπως προβλέπεται από το ECSF, τα άτομα που επιδιώκουν να αλλάξουν σταδιοδρομία προς την κυβερνοασφάλεια μπορούν να χρησιμοποιήσουν το ECSF ως σημείο εκκίνησης για τον προσδιορισμό συγκεκριμένων δεξιοτήτων και γνώσεων που χρειάζονται για τη μετάβαση.

Διάγραμμα 16: Χρήση του ECSF για την ανάλυση και τη σύγκριση προγραμμάτων



12https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity

Είτε το άτομο εργάζεται ήδη στον τομέα της κυβερνοασφάλειας (επιδιώκοντας να διευρύνει τις γνώσεις του), απασχολείται επί του παρόντος σε άλλον τομέα (επιδιώκοντας να αλλάξει σταδιοδρομία) είτε αναζητά ακαδημαϊκή εκπαίδευση (επιδιώκοντας να εργαστεί στον τομέα της κυβερνοασφάλειας στο μέλλον), το ECSF μπορεί να βοηθήσει στην κατανόηση των κύριων προφίλ των ρόλων κυβερνοασφάλειας (παρέχοντας περιγραφή και ανάλυσή τους σε καθήκοντα, δεξιότητες, γνώσεις και ικανότητες), καθώς και στην ανάλυση και τη σύγκριση των διαθέσιμων προγραμμάτων μάθησης (χαρτογράφηση των μαθησιακών αποτελεσμάτων με τις απαιτούμενες δεξιότητες και γνώσεις των προφίλ προτίμησης στον τομέα της κυβερνοασφάλειας).

Το ECSF δημιουργεί κοινή ορολογία και κοινή κατανόηση των προφίλ ρόλων των επαγγελματιών στον τομέα της κυβερνοασφάλειας και, ως εκ τούτου, μπορεί να εξαλείψει τη σύγχυση στην ορολογία και κάθε έλλειψη

3.4 ΟΙΚΟΔΌΜΗΣΗ ΚΟΙΝΟΤΉΤΩΝ ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑΣ — ΕΦΑΡΜΟΓΉ ΤΟΥ ECSF ΩΣ ΕΠΑΓΓΕΛΜΑΤΙΚΉ ΈΝΩΣΗ

Το ECSF δημιουργεί κοινή ορολογία και κοινή κατανόηση των προφίλ ρόλων των επαγγελματιών στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, μπορεί να χρησιμοποιηθεί από επαγγελματικές ενώσεις ως πρότυπο για να διασφαλιστεί ότι το έργο τους μπορεί να χρησιμοποιηθεί και να εφαρμοστεί σε ολόκληρη την ΕΕ, εξαλείφοντας τη σύγχυση στην ορολογία και κάθε έλλειψη κατανόησης.

Οι επαγγελματικές οργανώσεις μπορούν να χρησιμοποιούν το πλαίσιο για να διενεργούν αναλύσεις αγοράς χρησιμοποιώντας τα προφίλ ρόλων του ECSF και να παρουσιάζουν τα αποτελέσματα σε κοινή γλώσσα. Για παράδειγμα, το ECSF αναμένεται να συμβάλει στην ανάδειξη των προφίλ που λείπουν στην αγορά, των θέσεων εργασίας στον τομέα της κυβερνοασφάλειας που

έχουν υψηλή ζήτηση και οι νομοθετικές πτυχές ορισμένων επαγγελματικών προφίλ εργασίας. Επιπλέον, χρησιμοποιώντας το ECSF ως κοινή ορολογία, οι επαγγελματικές ενώσεις μπορούν να εργαστούν για την επαγγελματική καθοδήγηση στον τομέα της κυβερνοασφάλειας, όπως παρουσιάζεται στο παράρτημα Β.5.

Η χρήση του ECSF επιτρέπει επίσης την εδραίωση μιας κοινότητας ενδιαφερόμενων μερών για την υποστήριξη νέων εξελίξεων, βελτιώσεων και περαιτέρω εφαρμογής στα κράτη μέλη της ΕΕ. Ένα τέτοιο πλαίσιο συνεργασίας καθιστά δυνατή την ανθρώπινη αλληλεπίδραση, η οποία αποφέρει οφέλη όπως η ανταλλαγή γνώσεων, ο εντοπισμός τάσεων σε κλίμακα ΕΕ, οι δραστηριότητες μάθησης από ομότιμους, η εφαρμογή διεπιστημονικών προσεγγίσεων και η ενδυνάμωση για την προσαρμογή και την προσαρμογή του ECSF σε συγκεκριμένες απαιτήσεις.

Συνολικά, το ECSF μπορεί να χρησιμοποιηθεί από επαγγελματικές ενώσεις κυβερνοασφάλειας ως εργαλείο για να βασίσουν τις δραστηριότητές τους στη διασφάλιση της δυνατότητας εφαρμογής τους σε ολόκληρη την ΕΕ, με στόχο την επίτευξη μεγαλύτερης θωράκισης έναντι κυβερνοεπιθέσεων σε ολόκληρη την ΕΕ ως κοινωνία.

Δεδομένης της διαρθρωμένης προσέγγισης σε ένα πολύ ποικιλόμορφο περιβάλλον αγοράς, τα προφίλ ρόλων του ECSF παρέχουν ένα πολύτιμο εργαλείο για τη στήριξη των υπευθύνων χάραξης πολιτικής, των επιθεωρητών της αγοράς και άλλων ενδιαφερόμενων

3.5 ΣΤΡΑΤΗΓΙΚΉ ΕΝΔΥΝΆΜΩΣΗ ΤΟΥ ΤΟΜΈΑ — ΕΦΑΡΜΟΓΉ ΤΟΥ ECSF ΩΣ ΦΟΡΈΑΣ ΧΆΡΑΞΗΣ ΠΟΛΙΤΙΚΉΣ

Με το ECSF, μια κρίσιμη επαγγελματική κοινότητα εξασφαλίζει σαφή προβολή, καθώς η χρήση του πλαισίου δημιουργεί κοινή κατανόηση του τι κάνουν οι ειδικοί στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, το ECSF παρέχει ένα εργαλείο για την ανάλυση και την ανταλλαγή κρίσιμων συλλογών δεδομένων και στατιστικών που σχετίζονται με το εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας με κοινή και κατανοητή ορολογία σε επίπεδο ΕΕ. Τα δεδομένα αυτά είναι σημαντικά για τους υπεύθυνους χάραξης πολιτικής, καθώς αποκτούν καλύτερη γνώση της κατάστασης του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας σε ολόκληρη την ΕΕ, δίνοντάς τους έτσι τη δυνατότητα να κατανοούν και να εκτιμούν τις μελλοντικές ανάγκες των ειδικών στον τομέα της κυβερνοασφάλειας σε ποσότητα και ποιότητα. Η εν λόγω στρατηγική συμβολή συμβάλλει στην επικαιροποίηση και τη διατήρηση του ίδιου του ECSF, ώστε η σημασία του στο μέλλον να εξακολουθήσει να ισχύει. Επιπλέον, με τον καθορισμό κοινής ορολογίας, το ECSF επιτρέπει τη διασυνοριακή συνεργασία μεταξύ των υπευθύνων χάραξης πολιτικής μέσω της ανταλλαγής δεδομένων και πληροφοριών.

Δεδομένης της διαρθρωμένης προσέγγισης σε ένα πολύ ποικιλόμορφο περιβάλλον αγοράς, τα προφίλ ρόλων του ECSF παρέχουν ένα πολύτιμο εργαλείο για τη στήριξη των υπευθύνων χάραξης πολιτικής, των επιθεωρητών της αγοράς και άλλων ενδιαφερόμενων μερών με την επιρροή και τον ρόλο να ενδυναμώσουν τον τομέα με στρατηγικό τρόπο. Τα προφίλ ECSF μπορούν να είναι χρήσιμα για μελέτες δεδομένων σχετικά με την προσφορά και τη ζήτηση που διεξάγονται σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο. Τα προφίλ παρέχουν έναν κοινό, συμφωνημένο ορισμό για τη διευκόλυνση της συλλογής αξιόπιστων και συγκρίσιμων δεδομένων στην αγορά εργασίας στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένης της προσφοράς και της ζήτησης για διάφορους τύπους επαγγελματιών στον τομέα της κυβερνοασφάλειας και των σχετικών απαιτήσεων για συγκεκριμένες δεξιότητες.

Οι διαδικασίες χάραξης πολιτικής για την κυβερνοασφάλεια μπορούν να επωφεληθούν από τη συλλογή δεδομένων κατά τον χρόνο λήψης των αποφάσεων, π.χ. διατάξεις χρηματοδότησης, επενδυτικές προτεραιότητες και περίοδοι παρέμβασης. Εκτός από τις βασικές δραστηριότητες κάθε προφίλ, οι δραστηριότητες που διεξάγονται από αυτά μπορούν να συμβάλουν στη δημιουργία και τη συλλογή σχετικών συνόλων δεδομένων που μπορούν να στηρίξουν τις αποφάσεις πολιτικής. Στο παράρτημα Β.3 παρουσιάζεται ο τρόπος με τον οποίο οι αποσπασματικές πληροφορίες αποτελούν πρόκληση κατά τη λήψη αποφάσεων και οι δράσεις που αναλαμβάνει η INCIBE για την αντιμετώπιση της πρόκλησης αυτής με την υποστήριξη του ECSF. Με την ενσωμάτωση του ECSF ως ομοιογενούς πλαισίου για τον καθορισμό των προφίλ κυβερνοασφάλειας, τα κράτη μέλη της ΕΕ λαμβάνουν πολύτιμη στήριξη για την επίτευξη των στόχων τους για αύξηση των ταλέντων στον τομέα της κυβερνοασφάλειας και ευθυγράμμιση με τις υπόλοιπες χώρες σε ευρωπαϊκό επίπεδο.

4. ΌΡΟΙ ΚΑΙ ΟΡΙΣΜΟΊ

Όρος	Ορισμός	Πηγή
κυβερνοασφάλεια	Κάθε δραστηριότητα που είναι αναγκαία για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων προσώπων που επηρεάζονται από κυβερνοαπειλές.	Εντολή του ENISA (κανονισμός (ΕΕ) 2019/881)
κυβερνοαπειλή	Κάθε πιθανή περίσταση, συμβάν ή ενέργεια που θα μπορούσε να βλάψει, να διαταράξει ή να επηρεάσει αρνητικά με άλλον τρόπο τα συστήματα δικτύου και πληροφοριών, τους χρήστες των εν λόγω συστημάτων και άλλα πρόσωπα.	Εντολή του ENISA (κανονισμός (ΕΕ) 2019/881)
Τεχνολογία πληροφοριών και επικοινωνιών	Το αρκτικόλεξο ΤΠΕ σημαίνει τεχνολογία πληροφοριών και επικοινωνιών. Χρησιμοποιείται σε πολλά διαφορετικά πλαίσια και, από τεχνική άποψη, οι ΤΠΕ σχετίζονται με ψηφιακούς υπολογιστές και συστήματα διαδικτύου (επικοινωνίας), συμπεριλαμβανομένου του λογισμικού, του υλισμικού και των δικτύων. Από οικονομική και πολιτική άποψη, οι ΤΠΕ αφορούν έναν διατομεακό τομέα επιχειρήσεων, συμπεριλαμβανομένων των κατασκευαστών, των προμηθευτών προϊόντων ή των παρόχων υπηρεσιών που σχετίζονται με τον τομέα των ΤΠΕ.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
αρμοδιότητα	Η αποδεδειγμένη ικανότητα εφαρμογής γνώσεων, δεξιοτήτων και συμπεριφορών για την επίτευξη παρατηρήσιμων αποτελεσμάτων. Παραδείγματα είναι το Β.1. Ανάπτυξη εφαρμογών και Ε.3. Διαχείριση κινδύνων.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
δεξιότητα	Ικανότητα εκτέλεσης διαχειριστικών ή τεχνικών δραστηριοτήτων και καθηκόντων σε γνωστικό ή πρακτικό επίπεδο· να γνωρίζετε πώς να το κάνετε.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
μη τεχνικές δεξιότητες	Διαδραστικές δεξιότητες που χρησιμοποιούνται για την επιτυχή αντιμετώπιση καταστάσεων στον χώρο εργασίας· μπορεί να αναφέρεται στην ποιότητα της εργασίας, στην κοινωνική αλληλεπίδραση ή στο συναίσθημα. (αποκαλούνται επίσης εγκάρσιες, μεταβιβάσιμες ή συμπεριφορικές δεξιότητες)	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
γνώσεις	Σύνολο πραγματικών περιστατικών που πρέπει να εφαρμοστούν σε έναν τομέα εργασίας ή σπουδών· να γνωρίζετε τι πρέπει να κάνετε.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
στάση	Αναπαράσταση του ανθρώπινου στοιχείου μιας ηλεκτρονικής ικανότητας· εξετάζει τον τρόπο με τον οποίο ένα άτομο ενσωματώνει τις γνώσεις και τις δεξιότητες και τις εφαρμόζει κατάλληλα στο συγκεκριμένο πλαίσιο.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
μαθησιακό αποτέλεσμα	Δήλωση σχετικά με το τι γνωρίζει, κατανοεί και μπορεί να κάνει ένα άτομο μετά την ολοκλήρωση μιας μαθησιακής διαδικασίας	Ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων (ΕΠΕΠ)
προφίλ ρόλου	Περίγραμμα ή γενικό έγγραφο που καταδεικνύει τη σχέση μεταξύ συγκεκριμένων δραστηριοτήτων ή καθηκόντων στο πλαίσιο ενός ρόλου και των ατομικών δεξιοτήτων, ικανοτήτων και γνώσεων που απαιτούνται για την εκτέλεσή τους. Σε αντίθεση με μια συγκεκριμένη θέση εργασίας, ένας ρόλος απορρέει από μια Δημιουργική Ηγεσία,	Δημιουργική ηγεσία — Διαχείριση ταλέντων Προφίλ ΤΠΕ CWA

	οι οργανωτικές ανάγκες πρέπει να κάνουν κάτι. Οι απασχολούμενοι υπάλληλοι μπορούν να πληρούν τις οργανωτικές απαιτήσεις εκτελώντας το σύνολο ή μέρος των καθηκόντων που απαιτούνται για τη διασφάλιση του ρόλου τους.	
περιγραφή θέσης εργασίας	Ειδική και λεπτομερής περιγραφή του τι κάνει ο εργαζόμενος προκειμένου να βεβαιωθεί ότι ο κάτοχος της θέσης δεν έχει αμφιβολίες σχετικά με τα καθήκοντα, τις υποχρεώσεις, τις ευθύνες του και συχνά εκείνους στους οποίους αναφέρεται. Συνήθως περιέχει ακριβείς πληροφορίες σχετικά με τις ικανότητες, τις δεξιότητες και τις γνώσεις που απαιτούνται, καθώς και πρακτικές πληροφορίες σχετικά με την υγεία και την ασφάλεια και τις αμοιβές.	Προφίλ ΤΠΕ CWA
επίπεδο επάρκειας	Σαφής ένδειξη του βαθμού γνώσης που επιτρέπει στον επαγγελματία να πληροί τις απαιτήσεις κατά την άσκηση μιας ικανότητας. Το πρότυπο EN 16234-1 (e-CF) περιλαμβάνει τα επίπεδα επάρκειας e-1 έως e-5. Το e-CF χαρακτηρίζει τα επίπεδα επάρκειας συνδυάζοντας τα επίπεδα επιρροής εντός μιας κοινότητας, την πολυπλοκότητα του πλαισίου και την αυτονομία.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)
επίπεδο μάθησης	Υποδεικνύει την κατάταξη και μπορεί να εκπροσωπείται από επίσημο τίτλο. Τα επίπεδα μάθησης προέρχονται γενικά από ένα εκπαιδευτικό σύστημα ή υποδεικνύουν κατάταξη σε μια ταξινόμηση διανοητικής ή μαθησιακής συμπεριφοράς (όπως η μνήμη, η εφαρμογή, η διερμηνεία) και έχουν σχέση με τα επίπεδα επάρκειας, αλλά πρέπει να διακρίνονται από αυτά.	EN16234-1: 2019 πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF)

5. ΠΑΡΑΠΟΜΠΈΣ

Εντολή ENISA, κανονισμός (ΕΕ) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

Ευρωπαϊκά προφίλ επαγγελματικού ρόλου ΤΠΕ, CWA 16458
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0:::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=1799176DA0D15C74D91B71423CAD4A9A3

EN 16234-1: 2019 Πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF), Ένα κοινό ευρωπαϊκό πλαίσιο για τους επαγγελματίες ΤΠΕ σε όλους τους τομείς

CEN/TS 17699: 2022 Κατευθυντήριες γραμμές για την ανάπτυξη επαγγελματικών προγραμμάτων στον τομέα των ΤΠΕ, σύμφωνα με το πρότυπο EN 16234-1 (e-CF)

CEN/TS 17834: 2022 Ευρωπαϊκό πλαίσιο επαγγελματικής δεοντολογίας για το επάγγελμα των ΤΠΕ (Δεοντολογία ΤΠΕ της ΕΕ)

Ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων (ΕΠΕΠ)

ESCO Η ευρωπαϊκή πολυγλωσσική ταξινόμηση δεξιοτήτων, ικανοτήτων και επαγγελμάτων, http://www.ec.europa.eu/esco

Κωδικός Δεοντολογίας IFIP

Κύκλος ζωής απόκρισης σε συμβάντα NIST

Η Εθνική Πρωτοβουλία για την Εκπαίδευση στην Κυβερνοασφάλεια (NICE) του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας
οι ΗΠΑ

Εθνικές στρατηγικές κυβερνοασφάλειας (NCSS), https://www.enisa.europa.eu/topics/national-cyber-security-στρατηγικές/εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο — κατευθυντήριες γραμμές — εργαλεία

The Cybersecurity Body of Knowledge (CyBOK) του Εθνικού Προγράμματος Κυβερνοασφάλειας του Ηνωμένου Βασιλείου και του Πανεπιστημίου του Μπρίστολ, https://www.cybok.org

JRC, Taxonomy and glossary for Cybersecurity by European Commission (Ταξινομία και γλωσσάριο για την κυβερνοασφάλεια από την Ευρωπαϊκή Επιτροπή),
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Το ευρωπαϊκό θεματολόγιο δεξιοτήτων, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196

Σχέδιο δράσης για την ψηφιακή εκπαίδευση, https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education- σχέδιο δράσης

Σύμφωνο για τις δεξιότητες, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

Επικεφαλής της ψηφιακής δεκαετίας, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

ENISA, εγκληματολογική ανάλυση, ανάλυση ιστοεξυπηρετητή, Εγχειρίδιο, Έγγραφο για εκπαιδευτικούς, 2016, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe3_forensic_analysis_iii-Handbook

Συμβούλιο της Ευρώπης, Ηλεκτρονικά αποδεικτικά στοιχεία σε αστικές και διοικητικές διαδικασίες, κατευθυντήριες γραμμές και επεξηγήσεις
υπόμνημα, 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

Α ΠΑΡΆΡΤΗΜΑ: ΣΎΝΔΕΣΗ ΤΟΥ ECSF ΜΕ ΆΛΛΑ ΠΡΌΤΥΠΑ ΤΗΣ ΕΕ ΚΑΙ ΠΛΑΊΣΙΑ

Το ECSF είναι ένα πλαίσιο για τη στήριξη του επαγγελματικού τομέα της κυβερνοασφάλειας στην ΕΕ. Η σύνδεση των υφιστάμενων αναγνωρισμένων ευρωπαϊκών δομών που σχετίζονται με τον επαγγελματικό τομέα της κυβερνοασφάλειας της ΕΕ ήταν ζωτικής σημασίας αρχή σχεδιασμού του ECSF (βλ. ενότητα 2.1)

Στις παραγράφους που ακολουθούν παρέχεται σύντομη επισκόπηση των βασικών προτύπων και πλαισίων με τα οποία συνδέεται το ECSF.

Α.1 EN16234-1 E-CF ΈΝΑ ΚΟΙΝΌ ΕΥΡΩΠΑΪΚΌ ΠΛΑΊΣΙΟ ΑΝΑΦΟΡΆΣ ΓΙΑ ΤΟΥΣ ΕΠΑΓΓΕΛΜΑΤΊΕΣ ΤΠΕ ΣΕ ΌΛΟΥΣ ΤΟΥΣ ΤΟΜΕΊΣ

Το ευρωπαϊκό πρότυπο (EN) 16234-1 για το ευρωπαϊκό πλαίσιο ηλεκτρονικών ικανοτήτων (e-CF) παρέχει αναφορά σε 41 ικανότητες, όπως εφαρμόζονται στον χώρο εργασίας των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ), χρησιμοποιώντας μια τυποποιημένη ευρωπαϊκή γλώσσα για τις ικανότητες, τις δεξιότητες, τις γνώσεις και τα επίπεδα επάρκειας που μπορούν να γίνουν κατανοητά σε ολόκληρη την Ευρώπη. Πρωταρχικός στόχος αυτού του προτύπου είναι να παράσχει μια κοινή ευρωπαϊκή γλώσσα για τα επίπεδα ικανοτήτων, δεξιοτήτων, γνώσεων και επάρκειας που σχετίζονται με τον χώρο εργασίας ΤΠΕ, όπως απαιτείται και εφαρμόζεται από οργανισμούς και επαγγελματίες. Με τον τρόπο αυτό, όλα τα ενδιαφερόμενα μέρη του τομέα, συμπεριλαμβανομένων του δημόσιου και του ιδιωτικού τομέα και των ιδιωτών, έχουν πρόσβαση σε κοινή αναφορά.

Το πρότυπο θεσπίστηκε ως εργαλείο για την υποστήριξη της αμοιβαίας κατανόησης και την παροχή διαφάνειας στη γλώσσα μέσω της διάρθρωσης των ικανοτήτων που απαιτούνται και αναπτύσσονται από επαγγελματίες ΤΠΕ. Το πρότυπο αυτό διαρθρώνεται σε πολλαπλές διαστάσεις. Οι διαστάσεις αντικατοπτρίζουν τομείς σχεδιασμού των επιχειρήσεων και των ανθρώπινων πόρων και ενσωματώνουν κατευθυντήριες γραμμές για την επάρκεια των θέσεων εργασίας και της εργασίας. Επιπλέον, το πρότυπο αυτό προσθέτει μια εγκάρσια συνιστώσα που παρέχει βασικούς γενικούς περιγραφικούς δείκτες ΤΠΕ για την επιτυχή εφαρμογή των ικανοτήτων e-CF στο πλαίσιο ενός χώρου εργασίας.

Πίνακας 4: EN16234-1 (e-CF) επισκόπηση. Πηγή: CEN 2019

Διάσταση 1 5 περιοχές e-CF	**Διάσταση 2** 41 εντοπισθείσες ηλεκτρονικές ικανότητες	**Διάσταση 3** 5 επίπεδα επάρκειας ηλεκτρονικής ικανότητας				
		e-1	e-2	e-3	e-4	e-5
Α. Σχέδιο	A.1. Ευθυγράμμιση των συστημάτων πληροφοριών και της επιχειρηματικής στρατηγικής					
	A.2. Διαχείριση επιπέδου εξυπηρέτησης					
	A.3. Ανάπτυξη επιχειρηματικού σχεδίου					
	A.4. Σχεδιασμός προϊόντων/υπηρεσιών					
	A.5. Σχεδιασμός αρχιτεκτονικής					
	A.6. Σχεδιασμός της αίτησης					
	A.7. Παρακολούθηση των τεχνολογικών τάσεων					
	A.8. Διαχείριση της βιωσιμότητας					

* ENISA

	Α.9. Καινοτομία					
	Α.10. Εμπειρία χρήστη					
Β. Build	Β.1 Ανάπτυξη εφαρμογής					
	Β.2 Συνιστώσα Ένταξη					
	Β.3 Δοκιμές					
	Β.4 Εγκατάσταση λύσεων					
	Β.5 Παραγωγή τεκμηρίωσης					
	Β.6 Μηχανική συστημάτων ΤΠΕ					
Γ. Κυρία	Γ.1. Υποστήριξη χρήστη					
	Γ.2. Στήριξη για την αλλαγή					
	Γ.3. Παροχή υπηρεσίας					
	Γ.4. Διαχείριση προβλημάτων					
	Γ.5. Διαχείριση συστημάτων					
Ε. Εφαρμοστέο	Δ.1. Ανάπτυξη στρατηγικής για την ασφάλεια των					
	Δ.2. Ανάπτυξη στρατηγικής για την ποιότητα των ΤΠΕ					
	Δ.3. Παροχή εκπαίδευσης και κατάρτισης					
	Δ.4. Αγορές					
	Δ.5. Εξέλιξη πωλήσεων					
	Δ.6. Ψηφιακή εμπορία					
	Δ.7. Επιστήμη και ανάλυση δεδομένων					
	Δ.8. Διαχείριση συμβάσεων					
	Δ.9. Ανάπτυξη προσωπικού					
	Δ.10. Διαχείριση πληροφοριών και γνώσης					
	Δ.11. Προσδιορισμός αναγκών					
Ε. Διαχείριση	Ε.1. Πρόβλεψη ανάπτυξης					
	Ε.2. Διαχείριση έργων και χαρτοφυλακίων					
	Ε.3. Διαχείριση κινδύνων					
	Ε.4. Διαχείριση σχέσεων					
	Ε.5. Βελτίωση της διαδικασίας					
	Ε.6. Διαχείριση ποιότητας ΤΠΕ					
	Ε.7. Διαχείριση επιχειρηματικών αλλαγών					
	Ε.8. Διαχείριση της ασφάλειας των πληροφοριών					
	Ε.9. Διακυβέρνηση των συστημάτων πληροφοριών					

Το e-CF παρέχει συνεκτικούς δεσμούς στο πλαίσιο των επαγγελματικών προσόντων ΤΠΕ και άλλων πλαισίων που αφορούν τον τομέα (ιδίως, ΕΠΕΠ, DigComp, ευρωπαϊκά προφίλ επαγγελματικού ρόλου ΤΠΕ, δεξιότητες συμπεριφοράς, ESCO, EQANIE, SFIA, Ιδρυτικός Φορέας Γνώσεων για το επάγγελμα των ΤΠΕ, ISO και άλλα πρότυπα του κλάδου ΤΠΕ).

Για κάθε ρόλο κυβερνοασφάλειας, επιλέχθηκε ένα σύνολο εφαρμοστέων ικανοτήτων e-CF σε επίπεδο εφαρμογής ως ενσωματωμένο στοιχείο της περιγραφής προφίλ για τον ρόλο του επαγγελματία στον τομέα της κυβερνοασφάλειας.

Α.2 ΕΥΡΩΠΑΪΚΆ ΠΡΟΦΊΛ ΕΠΑΓΓΕΛΜΑΤΙΚΏΝ ΡΌΛΩΝ ΤΠΕ

Τα ευρωπαϊκά προφίλ επαγγελματικού ρόλου ΤΠΕ CWA 16458 παρέχουν ένα γενικό σύνολο τυπικών ρόλων που επιτελούν οι επαγγελματίες ΤΠΕ σε οποιονδήποτε οργανισμό, καλύπτοντας ολόκληρη την επιχειρηματική διαδικασία ΤΠΕ. Τριάντα προφίλ συνολικά παρέχουν ένα ισχυρό σημείο εκκίνησης και έμπνευση για τη δημιουργία πιο συγκεκριμένων και ευέλικτων προφίλ με βάση οργανωτικούς ρόλους, ατομικές περιγραφές θέσεων εργασίας ή ειδικότητες επιμέρους τομέων από διάφορα πλαίσια. Με την εφαρμογή των ικανοτήτων e-CF στην κατασκευή προφίλ ΤΠΕ, τα ευρωπαϊκά προφίλ επαγγελματικού ρόλου ΤΠΕ παρέχουν επίσης ένα εργαλείο και σημείο εισόδου για την εφαρμογή e-CF σε άτομα και οργανισμούς που επιθυμούν να συνεργαστούν με το e-CF.

Τα ευρωπαϊκά προφίλ επαγγελματικού ρόλου ΤΠΕ περιγράφονται με τη χρήση συνεκτικού μορφότυπου που περιλαμβάνει τα ακόλουθα στοιχεία: συνοπτική δήλωση, δήλωση αποστολής, παραδοτέα, κύρια καθήκοντα, ηλεκτρονικές ικανότητες και τομείς βασικών δεικτών επιδόσεων (ΒΔΕ)13.

Με την υιοθέτηση των καταλληλότερων στοιχείων του συστήματος περιγραφής προφίλ ΤΠΕ που έχει συμφωνηθεί σε ευρωπαϊκό επίπεδο και βασίζεται στην πρακτική, τα προφίλ του ECSF καθίστανται συγκρίσιμα και παρέχουν μια μοναδική, εύκολα προσβάσιμη και ολοκληρωμένη επισκόπηση των απαιτήσεων για τους Ευρωπαίους επαγγελματίες στον τομέα της κυβερνοασφάλειας.

Αυτά τα λεπτομερή προφίλ υψηλού περιεχομένου έχουν χαλαρά συνδέσμους προς τους γενικούς ρόλους που ενσωματώνονται στο σύνολο των ευρωπαϊκών επαγγελματικών προφίλ ΤΠΕ. Από την άποψη των χρηστών του ECSF, μπορεί να εδραιωθεί εμπιστοσύνη στη βιωσιμότητα της δομής μέσω της σύνδεσής της με τα ευρωπαϊκά προφίλ ΤΠΕ, αλλά με εστιασμένη εφαρμογή για την κοινότητα κυβερνοασφάλειας.

Α.3 ΕΥΡΩΠΑΪΚΌ ΠΛΑΊΣΙΟ ΕΠΑΓΓΕΛΜΑΤΙΚΏΝ ΠΡΟΣΌΝΤΩΝ

Η ΕΕ δημιούργησε το **ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων (ΕΠΕΠ)** που λειτουργεί ως μηχανισμός μετατροπής για την ευκολότερη κατανόηση και συγκρισιμότητα των επαγγελματικών προσόντων που προβλέπονται στις διάφορες χώρες. Το ΕΠΕΠ επιδιώκει να στηρίξει τη διασυνοριακή κινητικότητα των εκπαιδευομένων και των εργαζομένων και να προωθήσει τη διά βίου μάθηση και την επαγγελματική ανάπτυξη σε ολόκληρη την Ευρώπη.

Το ΕΠΕΠ είναι ένα πλαίσιο 8 επιπέδων που βασίζεται στα μαθησιακά αποτελέσματα14 για όλα τα είδη επαγγελματικών προσόντων. Χρησιμεύει ως εργαλείο μετάφρασης μεταξύ των διαφόρων πλαισίων εθνικών προσόντων. Συμβάλλει στη βελτίωση της διαφάνειας, της συγκρισιμότητας και της φορητότητας των επαγγελματικών προσόντων και καθιστά δυνατή τη σύγκριση προσόντων από διαφορετικές χώρες και ιδρύματα.

Το ΕΠΕΠ καλύπτει όλα τα είδη και όλα τα επίπεδα επαγγελματικών προσόντων και η χρήση των μαθησιακών αποτελεσμάτων καθιστά σαφές τι γνωρίζει, κατανοεί και μπορεί να κάνει ένα άτομο. Το επίπεδο αυξάνεται ανάλογα με το επίπεδο μάθησης, με το επίπεδο 1 το χαμηλότερο και το 8 το υψηλότερο επίπεδο. Το σημαντικότερο είναι ότι το ΕΠΕΠ συνδέεται στενά με τα εθνικά πλαίσια επαγγελματικών προσόντων και15, ως εκ τούτου, παρέχει έναν ολοκληρωμένο χάρτη όλων των τύπων και επιπέδων επαγγελματικών προσόντων στην Ευρώπη, τα οποία είναι όλο και πιο προσβάσιμα μέσω βάσεων δεδομένων επαγγελματικών προσόντων. Το ΕΠΕΠ συστάθηκε το 2008 και αργότερα αναθεωρήθηκε το 201716.

Τα προφίλ του ECSF περιλαμβάνουν αρμοδιότητες e-CF και αναθέσεις επιπέδου e-CF, οι οποίες παρέχουν συνεπή

13CWA 16458 Ευρωπαϊκά προφίλ επαγγελματικού ρόλου ΤΠΕ
14https://europa.eu/europass/en/description-eight-eqf-levels
15https://europa.eu/europass/en/national-qualifications-frameworks-nqfs
16https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615 (01) & from = EL

σύνδεση με τα επίπεδα του ΕΠΕΠ (βλ. ενότητα 3.2). Αυτή η σχέση προσανατολισμού αποτελεί γέφυρα για την κατανόηση μεταξύ της παροχής προγραμμάτων μάθησης και των απαιτήσεων στον χώρο εργασίας.

Α.4 ESCO — ΕΥΡΩΠΑΪΚΉ ΤΑΞΙΝΌΜΗΣΗ ΔΕΞΙΟΤΉΤΩΝ, ΙΚΑΝΟΤΉΤΩΝ ΚΑΙ ΕΠΑΓΓΕΛΜΆΤΩΝ

Το ESCO είναι η πολύγλωσση ταξινόμηση των ευρωπαϊκών δεξιοτήτων, ικανοτήτων, προσόντων και επαγγελμάτων. Βασικός σκοπός του ESCO είναι να παρέχει ένα λεξικό, το οποίο θα περιγράφει, θα εντοπίζει και θα ταξινομεί τα επαγγελματικά επαγγέλματα και τις δεξιότητες που σχετίζονται με την αγορά εργασίας, την εκπαίδευση και την κατάρτιση της ΕΕ και θα παρουσιάζει συστηματικά τις σχέσεις μεταξύ των εν λόγω επαγγελμάτων και δεξιοτήτων. Το ESCO τελεί υπό τη διαχείριση της Ευρωπαϊκής Επιτροπής, η οποία είναι αρμόδια για την επικαιροποίηση της ταξινόμησης. Ο πόρος ESCO στηρίζει δύο από τις βασικές στρατηγικές της ΕΕ στον τομέα αυτό, τη στρατηγική «Ευρώπη 2020» και το θεματολόγιο δεξιοτήτων για την Ευρώπη17.

Στόχος του ESCO είναι να περιγράψει όλα τα επαγγέλματα στην ευρωπαϊκή αγορά εργασίας, συμπεριλαμβανομένης της κυβερνοασφάλειας. Ως εκ τούτου, είναι χρήσιμο να καθιερωθεί μια προσανατολισμένη χαρτογράφηση μεταξύ των προφίλ ρόλων του ECSF και ορισμένων από τα προφίλ ESCO.

Στον πίνακα 5 παρατίθενται διάφορα επαγγέλματα ESCO που σχετίζονται με την κυβερνοασφάλεια, μαζί με ενδεικτική χαρτογράφηση των προφίλ ρόλων του ECSF. Δεδομένου ότι η μεταξύ τους σχέση δεν είναι πάντα μία προς μία, ορίστηκαν οι ακόλουθες σχέσεις για να εξηγηθούν οι αντίστοιχες συνδέσεις:

- **is** — Αυτό το ESCO Occupation μπορεί να χαρτογραφηθεί στο αντίστοιχο προφίλ ρόλων ECSF, καθώς αμφότερα περιγράφουν τον ρόλο στον τομέα της κυβερνοασφάλειας.
- **μπορεί να περιλαμβάνει** — Αυτή η ESCO Occupation μπορεί να περιλαμβάνει, με βάση το πλαίσιο, το προφίλ ρόλων ECSF που παρατίθεται στον κατάλογο. (Πρόκειται για ενδεικτική χαρτογράφηση.)
- **μπορεί να συμπεριληφθεί** — Ορισμένες πτυχές αυτού του επαγγέλματος ESCO μπορούν να περιγράψουν μέρη του προφίλ ρόλων ECSF που παρατίθενται. (Πρόκειται για ενδεικτική χαρτογράφηση.)

Πίνακας 5: Τα προφίλ ESCO και οι σχέσεις προφίλ ECSF

Κωδικός	ESCO Επαγγελματική	Σχέση	Προφίλ ρόλου ECSF
2149.2.8	Ερευνητής μηχανικός	μπορεί να περιλαμβάνει	Ερευνητής κυβερνοασφάλειας
2310.1	Καθηγητής τριτοβάθμιας εκπαίδευσης	μπορεί να περιλαμβάνει	Εκπαιδευτής κυβερνοασφάλειας
2356	Εκπαιδευτικοί τεχνολογιών πληροφόρησης	μπορεί να περιλαμβάνει	Εκπαιδευτής κυβερνοασφάλειας
2511.18	Ελεγκτής ΤΠ	μπορεί να περιλαμβάνει	Ελεγκτής κυβερνοασφάλειας
2519.2	Διαχειριστής ελεγκτή ΤΠΕ	μπορεί να περιλαμβάνει	Ελεγκτής κυβερνοασφάλειας
2529.1	Προϊστάμενος ασφάλειας ΤΠΕ	είναι	Προϊστάμενος ασφάλειας πληροφοριών (CISO)
2529.2	Εμπειρογνώμονας ψηφιακής	είναι	Ερευνητής ψηφιακών εγκληματολογικών
2529.3	Μηχανικός ασφάλειας ενσωματωμένου συστήματος	μπορεί να συμπεριληφθεί	Υπεύθυνος για την κυβερνοασφάλεια
2529.4	Ηθικός χάκερ	είναι	Εστέρας διείσδυσης
2529.6	Διαχειριστής ασφάλειας ΤΠΕ	μπορεί να συμπεριληφθεί	Υπεύθυνος για την κυβερνοασφάλεια
2529.7	Μηχανικός ασφάλειας ΤΠΕ//sm//sf//n	μπορεί να συμπεριληφθεί	Αρχιτέκτονας κυβερνοασφάλειας
2529.7	Μηχανικός ασφάλειας ΤΠΕ//sm//sf//n	μπορεί να συμπεριληφθεί	Υπεύθυνος για την κυβερνοασφάλεια

17https://ec.europa.eu/social/main.jsp?catId=1326&langId=en

2619.4	Υπεύθυνος προστασίας δεδομένων	είναι	Νομικό ζήτημα στον κυβερνοχώρο, Πολιτική & Υπεύθυνος Συμμόρφωσης

Σημαντική σημείωση: Η σχέση μεταξύ του επαγγέλματος ESCO και του προφίλ ρόλων ECSF δεν αντιπροσωπεύει ισοδυναμία· προσφέρει μια καταλληλότερη προσέγγιση την οποία οι αναγνώστες ενδέχεται να επιθυμούν να διερευνήσουν.

Β ΠΑΡΆΡΤΗΜΑ: ΠΕΡΙΠΤΏΣΕΙΣ ΧΡΉΣΗΣ

Μια περίπτωση χρήσης δείχνει γιατί και πώς ένας οργανισμός χρησιμοποιεί το ECSF, δίνοντας έμφαση στην ποικιλία των προσεγγίσεων και των οφελών. Το παρόν παράρτημα αποτελεί συλλογή υποθέσεων που δημοσιοποιήθηκαν στις 20 Ιουλίου 2022.

Οι ακόλουθες περιπτώσεις χρήσης αποτελούν απλώς ενδεικτικά παραδείγματα. Οι πληροφορίες και τα περιεχόμενα που περιλαμβάνονται σε αυτές τις περιπτώσεις δεν θα πρέπει να θεωρούνται ως προσυπογραφή ή δήλωση επικύρωσης από τον ENISA. Η χρήση αυτών των παραδειγμάτων θα πρέπει να θεωρείται μάλλον πηγή έμπνευσης παρά ως βασικές γραμμές ή ως αναφορές συγκριτικής αξιολόγησης.

8.1 ΠΕΡΊΠΤΩΣΗ ΧΡΉΣΗΣ ΑΠΌ ΤΟ ΈΡΓΟ CONCORDIA H2020

Το παρόν τμήμα περιλαμβάνει μέρη από την περίπτωση χρήσης που συντάχθηκαν από το έργο CONCORDIA H202018.

Προς μια ολοκληρωμένη πλατφόρμα για δεξιότητες στον κυβερνοχώρο, βασισμένη στο ευρωπαϊκό πλαίσιο δεξιοτήτων για την κυβερνοασφάλεια

Δυσνόητη γενική εικόνα της κατάρτισης

Η ανάγκη να προστατευθεί ο ίδιος από απειλές κατά των πληροφοριών και των επιχειρήσεων, να διατηρηθεί η θέση ενός οργανισμού στον τομέα της κυβερνοασφάλειας και να αυξηθεί η ανθεκτικότητα έναντι των εν λόγω απειλών, εξακολουθούν να γίνονται επειγόντως αισθητές από όλα τα ενδιαφερόμενα μέρη. Βασική συνιστώσα για την κάλυψη αυτών των αναγκών είναι η ύπαρξη επαγγελματιών του κυβερνοχώρου — ικανών. Και οι ικανότητες όσον αφορά την κυβερνοασφάλεια δεν απαιτούνται μόνο για τους ειδικούς επαγγελματίες (εξωτερικούς ή εσωτερικούς) αλλά και για όλα τα μέλη του προσωπικού ενός οργανισμού, ακόμη και αν δεν συμμετέχουν άμεσα σε διαδικασίες και δραστηριότητες κυβερνοασφάλειας.
Όσον αφορά τους επαγγελματίες στον τομέα της κυβερνοασφάλειας, διάφορες δημοσιεύσεις εξακολουθούν να αναφέρουν έλλειψη δεξιοτήτων στον τομέα της κυβερνοασφάλειας, επισημαίνοντας ότι οι 3 κορυφαίες ικανότητες που λείπουν ή δεν καλύπτονται επαρκώς από τους υφιστάμενους επαγγελματίες ποικίλλουν από το ένα έτος στο άλλο19. Από την άλλη πλευρά, σημαντικός αριθμός μαθημάτων και προγραμμάτων κατάρτισης σχετικά με την κυβερνοασφάλεια προσφέρονται από διάφορους ευρωπαϊκούς και διεθνείς οργανισμούς. Μια απλή αναζήτηση στο διαδίκτυο θα αποκαλύψει πολλά μαθήματα που σχετίζονται με τον τομέα της κυβερνοασφάλειας, χωρίς να παρέχεται σαφής εικόνα των προσφερόμενων ικανοτήτων ή του τρόπου με τον οποίο θα μπορούσαν να σχετίζονται με συγκεκριμένο ρόλο. Για να προστεθεί αυτή η σύγχυση, υπάρχουν μαθήματα κατάρτισης που φαίνεται να αφορούν έναν συγκεκριμένο ρόλο (π.χ. CISO), έχουν παρόμοιους τίτλους αλλά έχουν διαφορετικό πρόγραμμα σπουδών.

Ως εκ τούτου, σε αρκετές περιπτώσεις, οι παρεχόμενες πληροφορίες προκαλούν σύγχυση στον εκπαιδευόμενο σχετικά με το τι και πώς θα πρέπει να αντιλαμβάνονται τις έννοιες της κυβερνοασφάλειας, καθώς και σχετικά με τον τρόπο χρήσης τους για την κάλυψη των επαγγελματικών αναγκών του. Επιπλέον, τα μαθήματα για επαγγελματίες προωθούνται σε διάφορες πλατφόρμες και είναι δύσκολο να συγκριθούν σε σχέση με τις ικανότητες που καλύπτονται και το προφίλ ρόλων που εξετάζονται. Αυτό καθιστά δύσκολο για ένα άτομο να διαμορφώσει μια σαφή σταδιοδρομία και να εντοπίσει ευκαιρίες ανάπτυξης.
Ο χάρτης μαθημάτων CONCORDIA για επαγγελματίες του τομέα της κυβερνοασφάλειας

18https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-european- πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας/
19https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new- isaca-research -retention-tities-in-years

Σε μια προσπάθεια να αντιμετωπίσουμε αυτές τις προκλήσεις, καταρτίσαμε τον χάρτη μαθημάτων και κατάρτισης της CONCORDIA για τους επαγγελματίες του τομέα της κυβερνοασφάλειας20. Ο χάρτης εμφανίζει δομημένες πληροφορίες σχετικά με την υφιστάμενη ευρωπαϊκή προσφορά για σύντομα μαθήματα/προγράμματα κατάρτισης και παρέχει διάφορα φίλτρα που διευκολύνουν την αντιστοίχιση της συγκεκριμένης ανάγκης για ανάπτυξη δεξιοτήτων με την προσφορά. [...]

Μπορείτε να επιλέξετε να ταξινομήσετε τα μαθήματα με βάση το υπό εξέταση επίπεδο κυβερνοασφάλειας (Device-, Network-, Software/System, Data/Application-, User-Centric) ή τη συνάφεια με έναν κλάδο της βιομηχανίας (π.χ. τηλεπικοινωνίες, οικονομία, ηλεκτρονική κινητικότητα στον τομέα των μεταφορών, ηλεκτρονική υγεία ή άμυνα), αλλά και με βάση τη μορφή (διά ζώσης, διαδικτυακά, μεικτή) και το χρονοδιάγραμμα του μαθήματος/κατάρτισης.

Λείπει ένα βασικό συστατικό — Η λύση ενεργοποιείται από το ECSF

Αν και προσφέρουμε στον χάρτη CONCORDIA μια μεγάλη πληθώρα φίλτρων που θα βοηθήσουν τους χρήστες να εντοπίσουν ευκολότερα τα μαθήματα που ενδιαφέρουν, η βάση δεδομένων δεν διαθέτει ένα βασικό συστατικό — τους συνδέσμους προς τα προφίλ ρόλων που αφορούν καθένα από τα μαθήματα μέσω των γνώσεων και των δεξιοτήτων που καλύπτονται. Το ευρωπαϊκό πλαίσιο ικανοτήτων για τους επαγγελματίες ΤΠΕ που είναι διαθέσιμο κατά τον χρόνο κατάρτισης του χάρτη καθορίζει 30 προφίλ ρόλων και 40 συναφείς ικανότητες, αλλά είναι δύσκολο να συνδεθούν με τις ιδιαιτερότητες του τομέα της κυβερνοασφάλειας.

Πρόκειται για πρόκληση του εκπαιδευτικού οικοσυστήματος κυβερνοασφάλειας που επισημάναμε ήδη πριν από δύο χρόνια και αποτυπώνεται στον χάρτη πορείας της CONCORDIA για την εκπαίδευση21 υπό τον τίτλο C5: Ετερογένεια της ορολογίας που σχετίζεται με τις ικανότητες. Αυτή η έλλειψη διατομεακής και διακλαδικής συμφωνημένης ορολογίας σχετικά με τις δεξιότητες κυβερνοασφάλειας που απαιτούνται για έναν συγκεκριμένο ρόλο καθιστά δύσκολη για τις εταιρείες την κάλυψη ανοικτών θέσεων. Δυσκολεύονται να αντιστοιχίσουν τα κριτήρια πρόσληψης με τις σπουδές και τα προσόντα που απαριθμούνται στα βιογραφικά σημειώματα των προσφευγόντων λόγω της χρήσης μη τυποποιημένης ορολογίας. Τα άτομα, με τη σειρά τους, δεν μπορούν να προσδιορίσουν εύκολα τις δεξιότητες που πρέπει να διαθέτουν ή να αναπτύξουν για να ανταποκριθούν στη ζήτηση της αγοράς. Τέλος, οι πάροχοι μαθημάτων δυσκολεύονται να σχεδιάσουν προγράμματα σπουδών που ανταποκρίνονται στις ανάγκες της αγοράς.
Στο πλαίσιο του χάρτη πορείας της CONCORDIA, δεσμευθήκαμε για μια ενιαία πλατφόρμα που θα φιλοξενεί όλα τα υφιστάμενα προγράμματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο (πανεπιστημιακά και διδακτορικά προγράμματα, σύντομα μαθήματα και προγράμματα κατάρτισης για επαγγελματίες). [...]

Η πλατφόρμα θα πρέπει να εξετάσει το ενδεχόμενο συλλογής του περιεχομένου χρησιμοποιώντας κατηγορίες που βασίζονται σε τυποποιημένη ορολογία (συμπεριλαμβανομένου του ειδικού πλαισίου δεξιοτήτων). Οι κατηγορίες θα χρησιμοποιηθούν περαιτέρω ως φίλτρα για διαφορετικές έρευνες στη βάση δεδομένων των μαθημάτων. Τα 12 προφίλ ρόλων που ορίζονται στην τρέχουσα έκδοση του ευρωπαϊκού πλαισίου δεξιοτήτων στον τομέα της κυβερνοασφάλειας (ECSF) φαίνεται να αποτελούν φυσική λύση.

Το όφελος για τα ενδιαφερόμενα μέρη

Η υιοθέτηση ενός τυποποιημένου λεξιλογίου, όπως αυτό που προτείνεται από το ESCF, συμπεριλαμβανομένων προφίλ ρόλων στον τομέα της κυβερνοασφάλειας, θα βοηθήσει τις εταιρείες να εντοπίσουν τα κατάλληλα ταλέντα για τις θέσεις εργασίας, καθώς και τους παρόχους εκπαίδευσης να διαμορφώσουν καλύτερα το πρόγραμμα σπουδών τους ώστε να ανταποκρίνονται στις ανάγκες του εργατικού δυναμικού στον κυβερνοχώρο. Με την εφαρμογή της ίδιας ορολογίας και τη χρήση ενός πανευρωπαϊκού πλαισίου δεξιοτήτων για τις περιγραφές θέσεων εργασίας, την περιγραφή των μαθημάτων και το προφίλ ρόλων θα βοηθούσαν τα άτομα να επιλέξουν τις κατάλληλες εκπαιδευτικές ενότητες για να υποστηρίξουν την επαγγελματική τους πορεία και να φιλτράρουν καλύτερα τις θέσεις εργασίας σύμφωνα με τις ικανότητες και το επίπεδο εμπειρογνωσίας τους. Τέλος, οι υπεύθυνοι χάραξης πολιτικής θα είναι σε θέση να συλλέγουν πιο δομημένα δεδομένα σε εθνικό/περιφερειακό επίπεδο για τη στήριξη της μελλοντικής ανάπτυξης πολιτικής και να έχουν στέρεη βάση κατά τον συντονισμό με τις εξωτερικές χώρες για την αντιμετώπιση των προκλήσεων στον τομέα της ασφάλειας στον κυβερνοχώρο σε παγκόσμια κλίμακα.

20 https://www.concordia-h2020.eu/map-courses-cyber-professionals/
21 https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

Προς μια ολοκληρωμένη πλατφόρμα για τις δεξιότητες

Με βάση τη βάση δεδομένων CONCORDIA με μαθήματα και προγράμματα κατάρτισης για επαγγελματίες στον τομέα της κυβερνοασφάλειας, το έργο REWIRE22 επιχειρεί να λάβει περαιτέρω μέτρα για την ενσωμάτωση του σχετικού περιεχομένου που σχετίζεται με τις δεξιότητες κυβερνοασφάλειας. Η πλατφόρμα REWIRE Cyber ABILITY — που βρίσκεται επί του παρόντος στο στάδιο του σχεδιασμού — θα παρέχει επικαιροποιημένες πληροφορίες σχετικά με την αγορά εργασίας, τις ικανότητες, τα μαθήματα κατάρτισης, τα συστήματα πιστοποίησης και έναν χάρτη πορείας σταδιοδρομίας.

8.2 ΠΕΡΊΠΤΩΣΗ ΧΡΉΣΗΣ ΑΠΌ ΤΟ ΈΡΓΟ SPARTA H2020

Το παρόν τμήμα περιλαμβάνει μέρη από την περίπτωση χρήσης που συντάχθηκαν από το έργο SPARTA H202023.

Βελτίωση της τριτοβάθμιας εκπαίδευσης με τη χρήση του ECSF και του SPARTA προγραμματιστή προγραμμάτων σπουδών

Εισαγωγή

Αυτή η περίπτωση χρήσης παρέχει συστάσεις σχετικά με τον τρόπο με τον οποίο το ECSF μπορεί να χρησιμοποιηθεί για τη διαμόρφωση εκπαιδευτικών προγραμμάτων που συνδέονται με την κυβερνοασφάλεια. Καθώς το ECSF εκφράζει τη δομή των προφίλ υψηλού επιπέδου από την άποψη των επαγγελματιών, συμπεριλαμβανομένων των κύριων καθηκόντων, των σχετικών γνώσεων και δεξιοτήτων, αυτό μπορεί να παράσχει πιο εστιασμένη προσέγγιση για την ανάπτυξη εξειδικευμένων και ολοκληρωμένων προγραμμάτων σπουδών, προσαρμοσμένων σε συγκεκριμένα προφίλ, αντί να καλύπτει την κυβερνοασφάλεια εν γένει.

Πρόκληση

Τα εκπαιδευτικά ιδρύματα συνθέτουν τα προγράμματα σπουδών τους λαμβάνοντας υπόψη την πλήρη πορεία — ξεκινώντας από τα βασικά μαθήματα που απαιτούνται για να μάθει ο σπουδαστής ως βάση για το επόμενο σύνολο μαθημάτων παρακολούθησης, τα οποία συχνά αφορούν ειδικά την κυβερνοασφάλεια. Ωστόσο, η επιλογή των μαθημάτων που θα συμπεριληφθούν στα προγράμματα σπουδών κυβερνοασφάλειας εναπόκειται στο ίδρυμα. Κάθε εκπαιδευτικό ίδρυμα έχει το δικό του ειδικό περιβάλλον (το οποίο καθορίζεται, π.χ., από τις υποδομές, τον εξοπλισμό, την εμπειρογνωμοσύνη των εκπαιδευτικών, τη σύνθεση των υφιστάμενων προγραμμάτων κ.λπ.) και δεν υπάρχει καθολικός τρόπος διαμόρφωσης του προγράμματος σπουδών.

Οι πάροχοι εκπαίδευσης διαφέρουν ως προς τον συγκεκριμένο υποτομέα της κυβερνοασφάλειας στον οποίο θα ήθελαν να εστιάσουν. Ορισμένοι πάροχοι είναι πολύ τεχνικοί και εστιάζουν, π.χ., στην επιστήμη των υπολογιστών, κάποιοι είναι περισσότερο προσανατολισμένοι στην κοινωνία, εστιάζοντας σε νομικές και κοινωνικές πτυχές. Ως εκ τούτου, η διαλειτουργικότητα μεταξύ των προγραμμάτων σπουδών που προκύπτουν και μιας κοινής γλώσσας αποτελεί επί του παρόντος σημαντική πρόκληση.
Ορισμένα ακαδημαϊκά προγράμματα δεν αναπτύσσουν δεξιότητες και ικανότητες που να προετοιμάζουν τους σπουδαστές για συγκεκριμένους εργασιακούς ρόλους που είναι διαθέσιμοι στην αγορά εργασίας. Αυτό αποτελεί πρόκληση για τους σπουδαστές που δεν κατανοούν ποιες είναι οι επαγγελματικές δυνατότητες στο τέλος των σπουδών τους.

Η λύση ενεργοποιήθηκε από ECSF

Το ECSF μπορεί να συμβάλει στις ακόλουθες δραστηριότητες για την αντιμετώπιση των ανωτέρω προκλήσεων:

- Αξιολόγηση: Η περιγραφή των προφίλ επιτρέπει στα ιδρύματα να επανεξετάζουν τα προγράμματα σπουδών τους με δομημένο και συστηματικό τρόπο, κατανοώντας την άποψη των επαγγελματιών. Αυτό επιτρέπει την κατανόηση του προφίλ του ιδρύματος που απευθύνεται κυρίως στους αποφοίτους τους.

22 https://rewireproject.eu/

23 https://sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula% 20Designer.pdf

Βελτίωση: Μπορεί να γίνει με βάση τη διαδικασία αξιολόγησης. Αυτό είναι ιδιαίτερα σημαντικό λαμβανομένου υπόψη του συνόλου των γνώσεων/δεξιοτήτων που αποδίδονται σε συγκεκριμένο προφίλ.
Εστίαση: Η εκπαίδευση που παρέχεται από τα πανεπιστήμια μπορεί να διαφέρει ως προς τον τρόπο με τον οποίο καλύπτουν τις βασικές ικανότητες. Ορισμένα ενδέχεται να επικεντρώνονται περισσότερο σε ειδικά τεχνολογικά μαθήματα, άλλα στη νομοθεσία, άλλα στην εγκληματολογία κ.λπ. Με τη συνεργασία ενός ECSF, μπορούν να χαρτογραφήσουν τις βασικές τους ικανότητες σε διάφορους τομείς μαθημάτων, οι οποίοι είναι σημαντικοί για καθορισμένα προφίλ. Αυτό δίνει τη δυνατότητα στο θεσμικό όργανο να αναπτύξει πιο αποτελεσματικά στοχευμένα προγράμματα στο εσωτερικό του γύρω από τις κύριες αρμοδιότητες.
Συνεργασία: Το ECSF παρέχει στους παρόχους εκπαίδευσης την κοινή γλώσσα και το κοινό λεξιλόγιο για την περιγραφή των μαθημάτων τους, τη δημιουργία κοινών προγραμμάτων και τη διευκόλυνση της κινητικότητας των σπουδαστών.

Κατά την εφαρμογή του ECSF στην εκπαίδευση στον τομέα της κυβερνοασφάλειας, συνιστάται η ακόλουθη προσέγγιση:

Τα μαθήματα στα προγράμματα σπουδών μπορούν να ταξινομηθούν ως υπαγόμενα είτε στις κατηγορίες «Θεμελιώδη» είτε σε κατηγορίες ασφάλειας στον κυβερνοχώρο. Τα βασικά μαθήματα είναι εκείνα που ενδέχεται να μην συνδέονται άμεσα με το ECSF, αλλά χρησιμεύουν ως προϋπόθεση για μεταγενέστερες σπουδές. Για παράδειγμα, η θεμελιώδης κρυπτολογία αποτελεί προϋπόθεση για την κρυπτοανάλυση ή την προηγμένη κρυπτολογία· Η θεωρία του αριθμού είναι απαραίτητη για τα περισσότερα ενδιάμεσα και προηγμένα μαθήματα πληροφορικής.
Μόλις προσδιοριστούν τα βασικά μαθήματα, μπορούν να προταθούν τα μαθήματα κυβερνοασφάλειας για την αντιμετώπιση των απαιτήσεων σχετικά με τους εργασιακούς ρόλους στους οποίους στοχεύουν οι σπουδαστές. Η σύνδεση επιτυγχάνεται με βάση το περιεχόμενο των επιμέρους μαθημάτων, το οποίο μπορεί να συνδεθεί με τα προφίλ και, τέλος, με τους εργασιακούς ρόλους. Τα συγκεκριμένα μέτρα, [...], είναι τα εξής:

A. Για έναν συγκεκριμένο ρόλο εργασίας 1, οι πάροχοι εκπαίδευσης βρίσκουν τα σχετικά προφίλ (προφίλ 1 και προφίλ 12 στο παράδειγμά μας). Η χαρτογράφηση αυτή, η οποία επισημαίνεται με καστανά βέλη, θα πρέπει να
B. προσδιορίζεται από τους διαφημιστές/εργοδότες των θέσεων εργασίας.
Οι πάροχοι εκπαίδευσης προσδιορίζουν τις απαραίτητες γνώσεις και δεξιότητες για επιλεγμένα προφίλ. Οι απαιτήσεις αυτές καθορίζονται από το
Γ. ECSF, με γαλάζια βέλη.
Οι πάροχοι εκπαίδευσης σχεδιάζουν νέα ή επαναχρησιμοποιούν υφιστάμενα μαθήματα (στο παράδειγμά μας μαθήματα 1, 2, 3, 4) που αφορούν τις γνώσεις και τις δεξιότητες που προσδιορίζονται στο ανωτέρω βήμα. Αυτή η
Δ. χαρτογράφηση μεταξύ των μαθημάτων και του περιεχομένου τους πρέπει να πραγματοποιείται από τους διαχειριστές των μαθημάτων.
Διαθέτοντας όλα τα απαραίτητα μαθήματα (και όλες τις προϋποθέσεις για αυτά, γενικά μαθήματα που δεν σχετίζονται με την κυβερνοασφάλεια, άλλα μαθήματα για τη διεύρυνση του πεδίου των σπουδαστών κ.λπ.), ο πυρήνας του προγράμματος σπουδών είναι έτοιμος.

- Φυσικά, το ECSF μπορεί να εφαρμοστεί και με ακριβώς αντίθετο τρόπο: πρώτη σύνθεση του προγράμματος σπουδών από επιμέρους μαθήματα, ανάλυση των γνώσεων και των δεξιοτήτων που παρέχονται, χρήση του ECSF για τον εντοπισμό προφίλ και, τέλος, εξεύρεση των εργασιακών ρόλων που υποστηρίζονται από το πρόγραμμα σπουδών. Η χαρτογράφηση αυτή αποκαλύπτει ποιες ακριβείς γνώσεις και δεξιότητες υπάρχουν ήδη στα προγράμματα σπουδών ή, από την άλλη πλευρά, τι λείπει και θα πρέπει να τονιστεί ή να προστεθεί στα μαθήματα. Με τον τρόπο αυτό, το ECSF συμβάλλει στη διάρθρωση των προγραμμάτων σπουδών ώστε να ανταποκρίνονται καλύτερα στα αναμενόμενα προφίλ και τους ρόλους εργασίας.

Αποτέλεσμα/προστιθέμενη αξία ανά SPARTA

Το έργο Sparta χρησιμοποίησε ένα πλαίσιο δεξιοτήτων κυβερνοασφάλειας για τη δημιουργία ενός ελεύθερου εργαλείου με την ονομασία «Designer» των προγραμμάτων σπουδών κυβερνοασφάλειας. Πρόκειται για μια απλή διαδικτυακή εφαρμογή που βοηθά τους παρόχους εκπαίδευσης να δημιουργήσουν νέα προγράμματα σπουδών για την κυβερνοασφάλεια και/ή να αναλύσουν υφιστάμενα προγράμματα σπουδών ανάλογα με το περιεχόμενό τους και τον τρόπο με τον οποίο αντικατοπτρίζει τις απαιτήσεις για θέσεις εργασίας στον τομέα της

κυβερνοασφάλειας.

Το εργαλείο [...] επιτρέπει στους διαχειριστές προγραμμάτων σπουδών να καταρτίζουν το πρόγραμμα σπουδών τους παρακάμπτοντας και εγκαταλείποντας μαθήματα από το αριστερό τμήμα στο μεσαίο τμήμα. Μαθήματα, από τα οποία

οι διοικητικοί υπάλληλοι αναπτύσσουν τα προγράμματα μελέτης, μπορεί να είναι είτε προκαθορισμένα είτε εξατομικευμένα. Κατά τη σύνθεση του προγράμματος μελέτης, τα στατιστικά στοιχεία σχετικά με το περιεχόμενό του εμφανίζονται στη δεξιά ενότητα. Εκτός από άλλα δεδομένα, παρέχονται πληροφορίες σχετικά με τις ικανότητες και τους εργασιακούς ρόλους που υποστηρίζονται από το πρόγραμμα. Με τη χρήση του εργαλείου, είναι εύκολο να μάθετε ποιο περιεχόμενο λείπει από το πρόγραμμα σπουδών και ποιοι συγκεκριμένοι ρόλοι εργασίας είναι οι πλέον κατάλληλοι για τους αποφοίτους του προγράμματος. Στην περίπτωση αυτή, το πλαίσιο δεξιοτήτων κυβερνοασφάλειας αποτελεί τον πυρήνα των εφαρμογών που επιτρέπει τη σύνδεση των δεξιοτήτων και των γνώσεων με τους εργασιακούς ρόλους. [...]

8.3 ΠΕΡΊΠΤΩΣΗ ΧΡΉΣΗΣ ΑΠΌ ΤΟ INCIBE

Το παρόν τμήμα περιλαμβάνει μέρη από την περίπτωση χρήσης που έχει συντάξει το INCIBE24.

Περίπτωση χρήσης από το INCIBE

Εισαγωγή

Η αποτελεσματικότητα της προστασίας μιας χώρας εξαρτάται σε μεγάλο βαθμό από τις ικανότητες των πολιτών της, και οι εκτιμήσεις στο πλαίσιο αυτό είναι ότι, έως το 2022, η Ισπανία θα μπορούσε να αποκτήσει εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας περίπου 122,284 εργαζομένους με έλλειμμα ταλέντων που εκτιμάται σε 24,119. Κατά συνέπεια, μία από τις κορυφαίες προτεραιότητες της διοίκησης σήμερα είναι να ανταποκριθεί στην πρόκληση του εντοπισμού, της προσέλκυσης, της ανάπτυξης και της διατήρησης ταλέντων στους διάφορους τομείς της κυβερνοασφάλειας.

Απόδειξη αυτής της δέσμευσης αποτελεί η ανάπτυξη της εθνικής στρατηγικής κυβερνοασφάλειας της ισπανικής κυβέρνησης του 201925, η οποία τονίζει την ανάγκη όχι μόνο να υπάρχει αμυντική και προστατευτική θέση για τις επιχειρήσεις και τους πολίτες, αλλά και να υποστηριχθεί η τόνωση της βιομηχανίας κυβερνοχώρου, αναγνωρίζοντας τον καίριο ρόλο που διαδραματίζει η κυβερνοασφάλεια στο τρέχον περιβάλλον μετασχηματισμού και αβεβαιότητας και την ευκαιρία που προσφέρει για την αύξηση της ανταγωνιστικότητας της Ισπανίας. Σε ευθυγράμμιση με τον στόχο 4 της στρατηγικής, η γραμμή δράσης 5 τονίζει τη σημασία της τόνωσης της ισπανικής βιομηχανίας κυβερνοασφάλειας, πέραν της δημιουργίας και της διατήρησης ταλέντων για την ενίσχυση της ψηφιακής αυτονομίας.

Από την άλλη πλευρά, το σχέδιο «Ψηφιακή Ισπανία 2025»26 επιδιώκει να ενισχύσει τους μοχλούς που θα διευκολύνουν την επιστροφή στην πορεία της οικονομικής ανάπτυξης, και ένας από τους στρατηγικούς άξονες του είναι η ενίσχυση της ικανότητας κυβερνοασφάλειας της Ισπανίας για τον μετριασμό των κινδύνων και την αύξηση της εμπιστοσύνης στην πορεία προς μια ψηφιακή και βιώσιμη οικονομία.

Στον στρατηγικό της άξονα 4, ο οποίος είναι μονογραφικά αφιερωμένος στην κυβερνοασφάλεια, ενσωματώνει τα μέτρα που απαρτίζουν τους τρεις κύριους άξονες δράσης του INCIBE για τα επόμενα έτη: αύξηση των ικανοτήτων των πολιτών και των επιχειρήσεων στον τομέα της

24 http://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills
25 https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
26 https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

κυβερνοασφάλειας· ενίσχυση του ισπανικού οικοσυστήματος κυβερνοασφάλειας γύρω από τη βιομηχανία της, της έρευνας και ανάπτυξης Κ και των ταλέντων στον τομέα της κυβερνοασφάλειας· και εδραίωση της Ισπανίας ως διεθνούς κόμβου στον τομέα. Η Ισπανία Digital 2025 αναγνωρίζει ήδη τον καίριο ρόλο των ταλέντων στον τομέα της κυβερνοασφάλειας ως κινητήριας δύναμης για τον τομέα.

Οι εν λόγω εθνικές πρωτοβουλίες δημιουργούν ένα κατάλληλο σενάριο που ευνοεί την έρευνα, την καινοτομία και περιλαμβάνει τους σημαντικότερους παράγοντες της αλυσίδας αξίας, όπως εκπαιδευτικά ιδρύματα και οργανισμούς, ώστε να βλέπουν το όφελος της διαχείρισης των γνώσεων, των ικανοτήτων και των τεχνολογικών εμπειριών που ανταποκρίνονται στις μεγάλες προκλήσεις που αντιμετωπίζει η χώρα όσον αφορά την κυβερνοασφάλεια.

Από την πλευρά του, το ισπανικό Εθνικό Ινστιτούτο Κυβερνοασφάλειας (INCIBE), μια εταιρεία που υπάγεται στο Υπουργείο Οικονομικών Υποθέσεων και Ψηφιακού Μετασχηματισμού, μέσω του Υπουργού Ψηφιοποίησης και Τεχνητής Νοημοσύνης· και η οντότητα αναφοράς για την ανάπτυξη της κυβερνοασφάλειας και της ψηφιακής εμπιστοσύνης των πολιτών και των εταιρειών, καθώς και του ισπανικού ακαδημαϊκού και ερευνητικού δικτύου (RedIRIS), έχει ως αποστολή τη βελτίωση της κυβερνοασφάλειας και της ψηφιακής εμπιστοσύνης των πολιτών, των ανηλίκων και των ιδιωτικών εταιρειών στην Ισπανία.

Επιπλέον, η αποστολή της περιλαμβάνει την προστασία και την άμυνα των εν λόγω ομάδων, την προώθηση της ισπανικής βιομηχανίας και της E & D & I στον τομέα της κυβερνοασφάλειας, καθώς και τον εντοπισμό, την παραγωγή και την προσέλκυση ταλέντων στον τομέα της κυβερνοασφάλειας.

Ως εκ τούτου, τα ταλέντα στον τομέα της κυβερνοασφάλειας αποτελούν ακρογωνιαίο λίθο των δράσεων του INCIBE. Χωρίς ταλέντα, είναι αδύνατη η ανάπτυξη μιας ισχυρής βιομηχανίας ή των λύσεων υψηλής προστιθέμενης αξίας που απαιτούνται για τη συμμετοχή σε μια άκρως ανταγωνιστική αγορά, όπως η κυβερνοασφάλεια.

Ωστόσο, οι πληροφορίες που ήταν διαθέσιμες μέχρι στιγμής σχετικά με την κατάσταση των ταλέντων στον τομέα της κυβερνοασφάλειας στην Ισπανία ήταν ποικίλες και κατακερματισμένες, προερχόμενες από διαφορετικές πηγές, γεγονός που εμπόδισε τη βαθιά κατανόηση του περιβάλλοντος που απαιτείται για τη διοχέτευση των δράσεων. [...]

Αυτός είναι ο λόγος για τον οποίο, με στόχο να προσφέρει ένα σαφές όραμα για τα ταλέντα στον τομέα της κυβερνοασφάλειας στην Ισπανία, το INCIBE δημοσιεύει τον Μάρτιο του 2022 τα αποτελέσματα μιας ανάλυσης και διάγνωσης των ταλέντων στον τομέα της κυβερνοασφάλειας σε εθνικό επίπεδο, η διαδικασία των οποίων έχει διεξαχθεί μέσω αυστηρών αναλυτικών εγκαταστάσεων, συνολικής εργασιακής προσέγγισης και συμμετοχικών και συμμετοχικών διαδικασιών χωρίς αποκλεισμούς που έχουν λάβει υπόψη τους κύριους παράγοντες του οικοσυστήματος κυβερνοασφάλειας. [...]

Πρόκληση

Οι συστάσεις που προκύπτουν από το εν λόγω έργο ανάλυσης αποτελούν την αφετηρία για τη διασφάλιση ενός ισχυρού και κερδοφόρου κλάδου κυβερνοασφάλειας, ο οποίος χαρακτηρίζεται από το να θέτει τα ταλέντα των ανθρώπων στο επίκεντρο των πρωτοβουλιών. Υπό την έννοια αυτή, ολόκληρη η αξιακή αλυσίδα κυβερνοασφάλειας μπορεί να δει την παρούσα μελέτη ως ευκαιρία για περαιτέρω σύνδεση και καλύτερη κατανόηση των ταλέντων στον τομέα της κυβερνοασφάλειας στην Ισπανία.

Ως εκ τούτου, είναι αναγκαίο να διαρθρωθούν και να εφαρμοστούν αποτελεσματικές πρακτικές που επηρεάζουν τη διαχείριση αυτού του συγκεκριμένου τύπου ταλέντων στους οργανισμούς. Η σημασία της κυβερνοασφάλειας για την επιβίωση των οργανισμών απαιτεί την αντιμετώπιση του προβλήματος του εντοπισμού αυτού του είδους ειδικών ταλέντων στον τομέα της κυβερνοασφάλειας, της εξέλιξης της διαδικασίας πρόσληψης και επιβίβασης, καθώς και της έγκρισης δράσεων που συμβάλλουν στη βελτίωση της διαχείρισης και στον μετριασμό της

διαρροής ταλέντων.

Για τον λόγο αυτό, η προώθηση εθνικών πολιτικών, συντονισμένων από τη διοίκηση, οι οποίες επικεντρώνονται στην ενίσχυση και την προώθηση πρωτοβουλιών για να καταστεί η κυβερνοασφάλεια στρατηγική προτεραιότητα στους οργανισμούς, καθώς και η διάρθρωση και διάρθρωση ενός προγράμματος κατάρτισης για την απόδοση της κυβερνοασφάλειας ως επαγγελματικής δραστηριότητας αποτελούν προτεραιότητες στις οποίες θα καθορίσουν τόσο οι οργανισμοί όσο και οι εταιρείες πρόσληψης στις δράσεις τους για τον εντοπισμό, την προσέλκυση, την πρόσληψη και τη διαχείριση ταλέντων στον τομέα της κυβερνοασφάλειας.

Με τον τρόπο αυτό, διατυπώνεται μια σειρά συστάσεων που θα μπορούσαν να εφαρμόσουν αυτού του είδους οι υπάλληλοι (δημόσια διοίκηση, εταιρείες πρόσληψης και άλλοι οργανισμοί) για την αύξηση των ταλέντων στον τομέα της κυβερνοασφάλειας στην Ισπανία και οι οποίες θέτουν το σημείο εκκίνησης για την επίλυση των μελλοντικών προκλήσεων στο πλαίσιο αυτό. [...]

Η λύση ενεργοποιήθηκε από ECSF

Υπάρχουν διάφοροι παράγοντες (πολιτικοί, οικονομικοί, κοινωνικοί, τεχνολογικοί, νομικοί κ.λπ.) που μπορούν να επηρεάσουν τον κλάδο της κυβερνοασφάλειας και, κατά συνέπεια, την έλλειψη ταλέντων, τα κενά και εν γένει την αναντιστοιχία μεταξύ προσφοράς και ζήτησης.

Ένας από αυτούς τους σχετικούς παράγοντες στην Ευρωπαϊκή Ένωση είναι η έλλειψη τυποποίησης του ορισμού των ρόλων και των δεξιοτήτων κυβερνοασφάλειας που συνδέονται με τους ρόλους αυτούς.

Παροχή βάσης για συνεχή επικοινωνία μεταξύ των διαφόρων ενδιαφερόμενων μερών (κυβέρνηση, βιομηχανία, ακαδημαϊκή κοινότητα, υπεύθυνοι χάραξης πολιτικής και πολίτες). Αυτό το είδος εργαλείου χρησιμεύει ως βάση για ένα πιο ικανό και πλήρες εργατικό δυναμικό που κατανοεί την ίδια γλώσσα με άλλους επαγγελματίες στην Ευρώπη. [...]

Αποτέλεσμα/προστιθέμενη αξία

Ως εκ τούτου, στο πλαίσιο που παρουσιάστηκε, έχουν δρομολογηθεί δύο πρωτοβουλίες σε εθνικό επίπεδο, οι οποίες θα αποδώσουν αξία στο ECSF που αναπτύχθηκε από τον ENISA και οι οποίες θα είναι πολύ χρήσιμες. [...]
Και οι δύο πρωτοβουλίες, συντονισμένες μεταξύ τους, θα ενσωματώσουν το ECSF ως ομοιογενές πλαίσιο για τον καθορισμό των προφίλ κυβερνοασφάλειας, το οποίο θα επιτρέψει στην Ισπανία να επιτύχει τους στόχους της όσον αφορά τα ταλέντα και να ευθυγραμμιστεί με τις υπόλοιπες χώρες σε ευρωπαϊκό επίπεδο. [...]

8.4 ΥΠΌΘΕΣΗ ΧΡΉΣΗΣ ΑΠΌ ΤΗΝ ΕΥΡΩΠΑΪΚΉ ΑΣΦΆΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΏΡΟ ΟΡΓΑΝΙΣΜΌΣ (ECSO)

Η παρούσα ενότητα περιλαμβάνει μέρη από την περίπτωση χρήσης που συνέταξε ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο (ECSO)27.

Προς μια εναρμονισμένη εκπαιδευτική προσέγγιση με το ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας (ECSF)

Έχοντας εργαστεί για την εκπαίδευση, την κατάρτιση και τις δεξιότητες στην WG5 από το 2016, η ECSO έχει δει από πρώτο χέρι τις προκλήσεις που θέτει ο κατακερματισμός και οι διάσπαρτες προσεγγίσεις που υπάρχουν σήμερα στον τομέα της κυβερνοασφάλειας. Σε αυτό το ιστολόγιο, η ECSO εξετάζει τις υφιστάμενες ευρωπαϊκές προσεγγίσεις για την εκπαίδευση

27https://www.ecs-org.eu/newsroom/consolidated-educational-and-recruiting-scheme-the-glue-to-fix-todays-scattered-προσέγγιση

και την αναβάθμιση των δεξιοτήτων και επικεντρώνεται στο ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας (ECSF) του ENISA.

Η εκπαίδευση δεν αποτελεί μόνο εθνικό προνόμιο. Συνδέεται επίσης εγγενώς με τη συνεργασία μεταξύ εθνικών φορέων, της ευρύτερης κοινότητας κυβερνοασφάλειας και των ευρωπαϊκών φορέων. Στο πλαίσιο αυτό, η συνεργασία είναι καίριας σημασίας κατά την εξεύρεση πανευρωπαϊκών προσεγγίσεων για την εναρμόνιση των εκπαιδευτικών προγραμμάτων στον τομέα της κυβερνοασφάλειας και την αντιμετώπιση των δεξιοτήτων ή, πιο συγκεκριμένα, του χάσματος εργατικού δυναμικού. Υπάρχει μεγάλη ευκαιρία να αξιοποιηθεί το συνεργατικό πνεύμα της ευρωπαϊκής κοινότητας κυβερνοασφάλειας για την παροχή πρακτικών λύσεων και πρωτοβουλιών που μπορούν να έχουν αντίκτυπο «επιτόπου», και το ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας (ECSF) του ENISA μπορεί να διαδραματίσει σημαντικό ρόλο στο πλαίσιο αυτό.

Εκπαίδευση στον τομέα της κυβερνοασφάλειας: η προοπτική των ECSO

Από τη σκοπιά του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στον Κυβερνοχώρο (ECSO), ως αντιπροσωπευτικού οργάνου του ευρωπαϊκού οικοσυστήματος και κοινότητας δημόσιου και ιδιωτικού τομέα στον τομέα της κυβερνοασφάλειας), το δυναμικό

η αξία του ECSF δεν είναι αμελητέα όσον αφορά τη σύνδεση των υφιστάμενων προσπαθειών, την παροχή θεμελιωδών στοιχείων για ένα ευρωπαϊκό εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας και τη δημιουργία κοινού πλαισίου και ταξινόμησης για την εφαρμογή προφίλ και δεξιοτήτων. Οι επαγγελματίες του τομέα της κυβερνοασφάλειας, οι πάροχοι εκπαίδευσης και κατάρτισης, οι υπεύθυνοι χάραξης πολιτικής και οι επαγγελματίες προσλήψεων θα αποκομίσουν οφέλη από την ευρύτερη εφαρμογή του ECSF.

Η πρόκληση

Είναι προφανές ότι υπάρχει αυξανόμενη ανάγκη για ειδικευμένο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας. Διάφορες μελέτες σε ολόκληρο τον κόσμο από τη βιομηχανία και την ακαδημαϊκή κοινότητα επιβεβαιώνουν ότι η ζήτηση εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας είναι πολύ υψηλή και ότι είναι δύσκολο να προσληφθούν ικανοί επαγγελματίες. Στην έκδοση του 2021 της ετήσιας μελέτης για το εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας που δημοσιεύτηκε από το μέλος του ECSO (ISC) ²28 αναφέρεται ότι η έλλειψη επαγγελματιών στον τομέα της κυβερνοασφάλειας ανέρχεται σε 2.72 εκατομμύρια παγκοσμίως, αριθμός ο οποίος, αν και μειώθηκε από 3.12 εκατομμύρια το προηγούμενο έτος, εξακολουθεί να είναι σημαντικός. Μολονότι οι μελέτες αυτές παρέχουν μια βάση για την αξιολόγηση της παγκόσμιας κατάστασης, η πραγματικότητα είναι ότι είναι πολύ δύσκολο να ποσοτικοποιηθεί η έκταση της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας στην Ευρώπη. Γνωρίζουμε ότι η ζήτηση για εμπειρογνώμονες θα αυξηθεί αναπόφευκτα λόγω της ανάπτυξης της αγοράς κυβερνοασφάλειας και του κανονιστικού τοπίου, αφήνοντας ένα επείγον κενό για την κάλυψη περισσότερων (και διαφόρων ειδών) εμπειρογνωμόνων. [...]

Ωστόσο, δεν πρόκειται μόνο για αριθμητικό ζήτημα. Μέσω πρόσφατης μελέτης του ECSO σχετικά με τις πρακτικές και τις τάσεις πρόσληψης ανθρώπινων πόρων, ο ECSO παρατήρησε επίσης αύξηση του χρόνου που απαιτείται, κατά μέσο όρο, για να καλύψουν οι οργανισμοί τις θέσεις τους στον τομέα της κυβερνοασφάλειας. Πολλοί οργανισμοί αναφέρουν ότι μπορεί να χρειαστούν έως και έξι μήνες για τη διαδικασία πρόσληψης, η οποία είναι βραδύτερη από ό, τι για τους τομείς γνώσης, ενώ άλλοι δηλώνουν ότι δυσκολεύονται να καλύψουν πλήρως τις θέσεις τους στον τομέα της κυβερνοασφάλειας. Αυτό δείχνει σαφώς ότι υπάρχει αναντιστοιχία μεταξύ προσφοράς και ζήτησης (δηλαδή χάσμα μεταξύ ακαδημαϊκών και βιομηχανικών απαιτήσεων) και παράγοντες ώθησης/έλξης (δηλ. καταλληλότητα και αξιολόγηση των υποψηφίων, προσέλκυση θέσεων εργασίας και οφέλη). Ωστόσο, το κύριο ζήτημα για τους εργοδότες παραμένει η γενική

28https://www.isc2.org/Research/Workforce-Study

έλλειψη, σε παγκόσμιο επίπεδο, ειδικών στον τομέα της κυβερνοασφάλειας, ενώ η ζήτηση αυξάνεται συνεχώς. Αρκετοί οργανισμοί τονίζουν επίσης την πολυπλοκότητα της πρόσληψης εμπειρογνωμόνων για έναν τομέα που δεν κατέχουν. Από την έρευνα του ECSO προέκυψε επίσης ότι, ως αυξανόμενη τάση, αρκετοί υποψήφιοι, παρά την έλλειψη σημαντικών δεξιοτήτων κυβερνοασφάλειας, εξακολουθούν να εμπλουτίζουν το βιογραφικό τους σημείωμα με έννοιες και λέξεις-κλειδιά κυβερνοασφάλειας.

Οι προκλήσεις αυτές αναδεικνύουν σαφώς την ανάγκη για μια κοινή γλώσσα για τη στήριξη των προσπαθειών πρόσληψης και τη σημασία της εξέτασης του πολυτομεακού χαρακτήρα της κυβερνοασφάλειας που είναι τόσο μοναδικός στον τομέα έναντι των πιο παραδοσιακών επαγγελμάτων ΤΠ/ΤΠΕ. Ενώ τα υφιστάμενα πλαίσια, όπως η NICE, το CyBoK και το ECF, παρέχουν χρήσιμες κατευθυντήριες γραμμές για την ανάπτυξη δεξιοτήτων, απουσιάζει ένα ευρωπαϊκό πλαίσιο που παρέχει γενική ταξινόμηση προφίλ και διαδρομές σταδιοδρομίας εγγενείς στην κυβερνοασφάλεια. Ως εκ τούτου, η απελευθέρωση του ECSF είναι πολύ επίκαιρη και θεμελιώδης για τη στήριξη της ευρωπαϊκής κοινότητας κυβερνοασφάλειας στην προσέλκυση, την απόκτηση δεξιοτήτων και την επανειδίκευση εμπειρογνωμόνων.

Υπάρχει λύση

Ο ECSO θα εφαρμόσει το ECSF με διάφορους τρόπους για να ενισχύσει την υιοθέτησή του και να αξιοποιήσει τις δυνατότητές του για εναρμόνιση της εκπαίδευσης και των δεξιοτήτων στον τομέα της κυβερνοασφάλειας σε ολόκληρη την Ευρώπη.

Η ECSO:

- Χαρτογραφήστε το ελάχιστο πρόγραμμα αναφοράς στο ECSF, δίνοντας στους σχεδιαστές και τους επαγγελματίες του κύκλου μαθημάτων μια πρώτη ματιά σχετικά με τον καλύτερο τρόπο καθορισμού των προγραμμάτων σπουδών τους για ειδικές σταδιοδρομίες. Αυτό θα συμβάλει ώστε τα πανεπιστημιακά μαθήματα να αντικατοπτρίζουν επαρκώς την πραγματικότητα των αναγκών της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας, επιτρέποντας παράλληλα τη συνεχή επικαιροποίηση του προγράμματος σπουδών.

- Χρησιμοποιήστε το ECSF και το σχετικό εγχειρίδιο χρήσης για την υποστήριξη των ανθρώπινων πόρων/προσλήψεων κατά τη σύνταξη των προκηρύξεων θέσεων εργασίας και την οργάνωση διαδικασιών αξιολόγησης/αξιολόγησης πρακτικών δεξιοτήτων. Θα διενεργήσουμε επίσης έρευνα παρακολούθησης των ανθρώπινων πόρων χρησιμοποιώντας τα προφίλ εργασίας του ECSF για να κατανοήσουμε τους ρόλους που χρειάζονται περισσότερο οι οργανισμοί και να αναπτύξουμε σταδιακά μια ποσοτική κατανόηση της ευρωπαϊκής αγοράς εργασίας στον τομέα της κυβερνοασφάλειας.

- Χρήση του ECSF ως βασική ταξινομία για δύο ειδικές πλατφόρμες που προβλέπονται από το Ίδρυμα Women4Cyber και τον ECSO [...]

Αποτέλεσμα και προστιθέμενη αξία

Η προστιθέμενη αξία του ECSF για την ευρωπαϊκή κοινότητα κυβερνοασφάλειας είναι πρώτα να υπάρχει ένα κοινό πλαίσιο και ταξινόμηση βάσει των οποίων να λειτουργεί. Αυτό θα οδηγήσει σε καλύτερη κατανόηση των αναγκών σε δεξιότητες και της πρακτικής πραγματικότητας των διαφόρων προφίλ εργασίας, γεγονός που θα ενισχύσει το εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας, όχι μόνο μέσω αποτελεσματικότερων μέτρων πρόσληψης και διατήρησης, αλλά και μέσω της διευκόλυνσης της εισόδου ή επανένταξης περισσότερων γυναικών και άλλων υποεκπροσωπούμενων ομάδων (δηλαδή των νευροποικιλόμορφων) στον τομέα. Το ECSF, επισημαίνοντας τις τεχνικές και μη τεχνικές πτυχές των διαφόρων προφίλ, θα συμβάλει στην εξάλειψη της εσφαλμένης αντίληψης ότι η κυβερνοασφάλεια αποτελεί μόνο τεχνικό θέμα, όταν

αφορά τόσο ανθρώπους όσο και διαδικασίες. Στο πλαίσιο αυτό, η έμφαση στη σημασία των μη τεχνικών (μεταβιβάσιμων) δεξιοτήτων στον τομέα θα συμβάλει σημαντικά στην προσέλκυση περισσότερων γυναικών στο επάγγελμα του κυβερνοχώρου. Το ECSF θα μειώσει επίσης τον κατακερματισμό των προσεγγίσεων με τη θέσπιση κατευθυντήριων γραμμών από την κορυφή προς τη βάση για τον τρόπο κατηγοριοποίησης του πολύπλευρου χαρακτήρα του επαγγέλματος του κυβερνοχώρου. Τα προφίλ που προτείνονται από το ECSF είναι αρκετά ευρέα ώστε να μπορούν να στηρίξουν τους πολυάριθμους ρόλους που πρέπει να προσφέρει το επάγγελμα, ενώ είναι κατακερματισμένα κατά τρόπο που το καθιστά κατανοητό και εφαρμόσιμο τόσο για τους επαγγελματίες του κλάδου, τους εμπειρογνώμονες του κλάδου, τους υπεύθυνους χάραξης πολιτικής, τους ειδικούς προσλήψεων όσο και τα άτομα που αναζητούν εργασία.

Στην ECSO, είμαστε πεπεισμένοι ότι το ECSF θα προσφέρει σημαντική αξία στο έργο μας και θα στηρίξει την ευρύτερη κοινότητα με ένα συγκεκριμένο εργαλείο για την εναρμόνιση των προσπαθειών και τη γεφύρωση του χάσματος μεταξύ ζήτησης και προσφοράς εμπειρογνωμόνων.

B.5 ΠΕΡΊΠΤΩΣΗ ΧΡΉΣΗΣ ΑΠΌ ΤΟ ISC2

Το παρόν τμήμα περιλαμβάνει μέρη από την περίπτωση χρήσης που έχει συνταχθεί από το (ISC) ²29.

Χρήση του (ISC) ² CISSP CBK για τη στήριξη του ευρωπαϊκού πλαισίου δεξιοτήτων στον τομέα της κυβερνοασφάλειας/των επαγγελματικών κοινοτήτων κυβερνοασφάλειας

Εισαγωγή

Το (ISC) ² CISSP CBK — μερικές φορές ονομάζεται απλώς «σώμα γνώσεων» — αναφέρεται σε μια συλλογή που έχει αναπτυχθεί από ομότιμους σχετικά με το τι πρέπει να προσδιορίσει και να διαθέτει ένας ικανός επαγγελματίας στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων γνώσεων, δεξιοτήτων, ικανοτήτων, τεχνικών και πρακτικών για να επιτύχει. Η (ISC) ² CBK είναι μια συλλογή θεμάτων σχετικών με τους επαγγελματίες του τομέα της κυβερνοασφάλειας σε ολόκληρο τον κόσμο. Θεσπίζει ένα κοινό πλαίσιο όρων και αρχών για την ασφάλεια των πληροφοριών, το οποίο επιτρέπει στους επαγγελματίες της κυβερνοασφάλειας και των ΤΠ/ΤΠΕ παγκοσμίως να συζητούν, να συζητούν και να επιλύουν θέματα που αφορούν το επάγγελμα με κοινή αντίληψη, ταξινόμηση και λεξικό. (ISC) ² συστάθηκε, εν μέρει, για τη συγκέντρωση, την τυποποίηση και τη διατήρηση της (ISC) ² CBK για τους επαγγελματίες του τομέα της κυβερνοασφάλειας παγκοσμίως. Η (ISC) 2 CBK παρουσιάζει έναν ανανεωμένο πόρο για τους σημερινούς και επίδοξους επαγγελματίες του τομέα της κυβερνοασφάλειας που πρέπει να υιοθετήσουν εντός του πλαισίου του ECSF.

29https://www.isc2.org/-/media/9644E0ED44954F7CAF895D45620213EA.ashx

* ENISA

Πρόκληση

Όπως περιγράφει ο ENISA στην πρόσφατα δημοσιευθείσα έκθεσή του με τίτλο «Αντιμετώπιση των ελλείψεων και των ελλείψεων δεξιοτήτων της ΕΕ στον τομέα της κυβερνοασφάλειας μέσω της τριτοβάθμιας εκπαίδευσης», οι παγκόσμιες ελλείψεις δεξιοτήτων στον τομέα της κυβερνοασφάλειας και η έλλειψη επαρκούς και ειδικευμένου εργατικού δυναμικού αποτελούν ανησυχίες που έχουν σημαντικό αντίκτυπο στην ικανότητα των κρατών μελών της ΕΕ να προστατεύουν το κοινό από τις αυξανόμενες απειλές που απορρέουν από τη διαρκώς αυξανόμενη χρήση της τεχνολογίας στην κοινωνία. Παρά το έργο που έχει επιτελεσθεί, οι κυβερνοεπιθέσεις και η απειλή κυβερνοεπιθέσεων εξακολουθούν να αποτελούν σημαντικό κίνδυνο για τη δημόσια ασφάλεια. Οι ευρωπαϊκοί οργανισμοί δυσκολεύονται να στελεχώσουν επαρκώς τις ομάδες κυβερνοασφάλειας. Οι αποτρέψιμες συνέπειες — λανθασμένα συστήματα, εσπευσμένες εφαρμογές, ελλιπής αντιμετώπιση περιστατικών, καθυστερημένη προετοιμασία, ανεπαρκής διαχείριση κινδύνου- καθιστούν πολλούς ευρωπαϊκούς οργανισμούς ελκυστικούς στόχους για τους παράγοντες απειλών σε ολόκληρο τον κόσμο.

Λύση που δόθηκε από το ECSF (πώς αντιμετωπίστηκαν οι προκλήσεις)

Για την αντιμετώπιση των προκλήσεων που παρουσιάζει το χάσμα δεξιοτήτων και η έλλειψη εργατικού δυναμικού, (ISC) ² προτείνει μια λύση που θα επικεντρώνεται στην παροχή βοήθειας στους επαγγελματίες του τομέα της κυβερνοασφάλειας ώστε να εντοπίζουν και να χαρτογραφούν τις γνώσεις, τις δεξιότητες, τις ικανότητες, τις τεχνικές και τις πρακτικές που απαιτούνται για τα προφίλ που προσδιορίζονται στο ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας (ECSF). Το (ISC) 2 χαρτογραφεί το CISSP CBK σε διάφορους τομείς δεξιοτήτων και γνώσεων στα ακόλουθα προφίλ ECSF:

- 2.1 προϊστάμενος ασφάλειας πληροφοριών (CISO)
- 2.2 Αντιδρών σε κυβερνοπεριστατικό
- 2.3 Νομοθεσία για τον κυβερνοχώρο, πολιτική & Συμμόρφωση Υπάλληλος
- 2.4 Ειδικός σε θέματα πληροφοριών κυβερνοαπειλών
- 2.5 Αρχιτέκτονας κυβερνοασφάλειας
- 2.6 Ελεγκτής κυβερνοασφάλειας

Χρησιμοποιώντας τις έννοιες που καλύπτονται από το CBK, οι επαγγελματίες που εργάζονται επί του παρόντος στα προαναφερόμενα προφίλ ή εκείνοι που επιθυμούν να εργαστούν σε αυτά τα προφίλ μπορούν να χρησιμοποιήσουν τις βασικές δεξιότητες και τους τομείς γνώσεων από τα προφίλ ECSF σε συνδυασμό με την (ISC) 2 CBK για να καθορίσουν τον τρόπο με τον οποίο το CBK πληροί τις γνώσεις και τις δεξιότητες που απαιτούνται για τη θέση και πού ενδέχεται να χρειαστεί να συμπληρώσουν την εκπαίδευση/κατάρτισή τους από άλλες πηγές. Αυτό θα επιτρέψει στους υποψηφίους να χαράξουν μια εκπαιδευτική/εκπαιδευτική πορεία για την επίτευξη των στόχων τους.

Ο ακόλουθος πίνακας παρέχει ένα παράδειγμα του τρόπου με τον οποίο το (ISC) 2 CISSP CBK μπορεί να χρησιμοποιηθεί από έναν τρέχοντα ή επίδοξο CISO για τον προσδιορισμό των βασικών δεξιοτήτων και των τομέων γνώσεων από το προφίλ ECSF CISO που έχει ή πρέπει να αναπτύξει. [...]

Αποτέλεσμα/Προστιθέμενη τιμή

Το επιδιωκόμενο όφελος από τη χαρτογράφηση (ISC) ² του CISSP CBK στο ECSF είναι ότι θα δημιουργήσει επαγγελματικό προσανατολισμό και επαγγελματικές εκπαιδευτικές διαδρομές για να βοηθήσει τους σημερινούς και επίδοξους επαγγελματίες του τομέα της κυβερνοασφάλειας να εντοπίσουν και να αποκτήσουν τις απαιτούμενες επαγγελματικές γνώσεις, δεξιότητες και ικανότητες προκειμένου να αποκτήσουν ταχύτερα και να συμπληρώσουν ανοικτά προφίλ,

όπως προσδιορίζονται στο ECSF, μετριάζοντας έτσι τις παγκόσμιες ελλείψεις δεξιοτήτων στον τομέα της κυβερνοασφάλειας και μειώνοντας το χάσμα ειδικευμένου εργατικού δυναμικού.

Β.6 ΠΕΡΊΠΤΩΣΗ ΧΡΉΣΗΣ ΑΠΌ ISACA

Το παρόν τμήμα περιλαμβάνει μέρη από την περίπτωση χρήσης που έχει συντάξει η ISACA30.

Ατομική λήψη αποφάσεων σταδιοδρομίας: Επαγγελματικό διαπιστευτήριο — Ευρωπαϊκό πλαίσιο δεξιοτήτων στον τομέα της κυβερνοασφάλειας

Εισαγωγή

Η Sabine εργαζόταν ως αναλυτής SOC λίγα χρόνια μετά την απόκτηση του πανεπιστημιακού της πτυχίου και ενδιαφέρθηκε να μάθει πώς να προωθήσει καλύτερα τη σταδιοδρομία της. Μίλησε με τον μέντορα της, ο οποίος την ενημέρωσε ότι η ISACA ήταν ένα εξαιρετικό εφαλτήριο για τη σταδιοδρομία του και την ενθάρρυνε να εξετάσει την ιδιότητα του μέλους και την ενδεχόμενη πιστοποίηση. Πρέπει να συνειδητοποιήσουμε ότι η μετάβαση στην κυβερνοασφάλεια παρέχει τη δυνατότητα συνεργασίας με όλους, από τους ανθρώπους και την ψυχολογία μέσω της νομικής, πολιτικής και διακυβέρνησης, έως το χαμηλότερο (ή το υψηλότερο) τεχνικό επίπεδο. Η πρόκληση είναι να βρεθεί ένα σημείο εκκίνησης και στη συνέχεια να προσδιοριστούν οι συγκεκριμένες ικανότητες που μπορεί να μάθει και στη συνέχεια να αποκτήσει κάποιος για να διευρύνει ή ακόμη και να μεταβεί μεταξύ των ρόλων στον τομέα της ασφάλειας στον κυβερνοχώρο. Το ESCF προσδιορίζει διάφορους ρόλους με τις αρμοδιότητές τους που απαιτούνται για να εργαστούν στο πλαίσιο αυτού του συγκεκριμένου ρόλου. Παρατηρούν ότι οι αρμοδιότητες αυτές δεν είναι όλες απαραίτητες για έναν συγκεκριμένο ρόλο, αλλά το απολύτως ελάχιστο. Με τη χρήση αυτού του Sabine μπορεί να προσδιοριστεί το κενό ικανοτήτων εάν κάποιος επιθυμεί να αλλάξει έναν ρόλο ή να μεταβεί σε άλλον τομέα στο πλαίσιο της κυβερνοασφάλειας.

Πρόκληση

Ως νέος επαγγελματίας σε τομέα υψηλής ζήτησης και ως γυναίκα στον τομέα της κυβερνοασφάλειας, ο Sabine αναζητούσε βοήθεια σε λίγους διαφορετικούς τομείς:

- Επαγγελματικός προσανατολισμός και πόροι — συμπεριλαμβανομένων των διαπιστευτηρίων — για την προώθηση της σταδιοδρομίας της
- Ένα δίκτυο ομότιμων και ηγετών του κλάδου για να την βοηθήσει να αντιμετωπίσει τις επαγγελματικές προκλήσεις
- Βοήθεια για την ανάπτυξη ήπιων δεξιοτήτων που θα την βοηθήσουν να γίνει η πρωτοπορία της στο μέλλον
- Πληροφορίες σχετικά με την αντιμετώπιση των προκλήσεων και τη μόχλευση ευκαιριών ως γυναίκας στον τομέα της κυβερνοασφάλειας
- Πληροφορίες που την βοηθούν να κάνει καλά την τρέχουσα δουλειά της και την βοηθά να προετοιμαστεί για σε ανώτερους ρόλους

Κάθε άτομο μπορεί να χρησιμοποιήσει το ESCF για να δει τους ρόλους που απαιτούνται για την αντιμετώπιση σχεδόν οποιουδήποτε είδους πρόκλησης ή εργασίας εντός του τομέα της κυβερνοασφάλειας. Επίσης, χρησιμοποιώντας το ESCF ως βάση αναφοράς, ένα άτομο μπορεί

30https://www.isaca.org/training-and-events/careers-home/career-pathway/european-cybersecurity-skills-framework-and-ισοδιαπιστευτήρια

στη συνέχεια να προσδιορίσει τις ικανότητες που απαιτούνται για τη μετάβαση από τον έναν ρόλο στον άλλο. Αυτό θα ωφελήσει τον διάλογο μεταξύ εργαζομένων και εργοδοτών κατά τον σχεδιασμό της συνεχούς εκπαίδευσης στον τομέα της κυβερνοασφάλειας. Αυτό θα ωφελήσει επίσης ένα άτομο που επιθυμεί να εισέλθει στην κυβερνοασφάλεια, αλλά δεν είναι σίγουρο για το πού θα ξεκινήσει. Για τα περισσότερα άτομα που εμπλουτίζουν προηγούμενες γνώσεις και ικανότητες είναι ευκολότερο να μάθουν κάτι εντελώς νέο.
Με την αποστολή να καταστεί επαγγελματίας κυβερνοασφάλειας της σειράς C σε αυτό το δύσκολο πεδίο, ο Sabine διερεύνησε το περίγραμμα των αρμοδιοτήτων του CISO:

1	Ειδικότητα CISO Αποστολή	Καθορίζει, διατηρεί και κοινοποιεί το όραμα, τη στρατηγική, τις πολιτικές και τις διαδικασίες κυβερνοασφάλειας και διαχειρίζεται την εφαρμογή σε ολόκληρο τον οργανισμό. Διαχειρίζεται τις δραστηριότητες που σχετίζονται με την κυβερνοασφάλεια σε ολόκληρο τον οργανισμό. Διαχειρίζεται συνδέσμους/συνδέσμους με εξωτερικές αρχές και επαγγελματικούς φορείς.

Φιλοδοξία της Sabine είναι να εντοπίσει τα κενά στις δεξιότητές της προκειμένου να προχωρήσει η σταδιοδρομία της με κατάλληλα ευθυγραμμισμένα διαπιστευτήρια στο επόμενο επίπεδο.

Λύση ECSF

Η Sabine διερεύνησε το ECSF PROFILE 1 και εντόπισε κενά στις γνώσεις της:

Βασικές γνώσεις	✓ γνώση των προτύπων, των πλαισίων, των πολιτικών, των κανονισμών, των νομοθεσιών, των πιστοποιήσεων και των βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας και της ιδιωτικής ζωής
	Κατανόηση των δεοντολογικών απαιτήσεων των οργανισμών κυβερνοασφάλειας
	✓ γνώση των ελέγχων ασφαλείας
	Γνώση των μοντέλων ωριμότητας στον τομέα της κυβερνοασφάλειας
	✓ γνώση τακτικών, τεχνικών και διαδικασιών κυβερνοασφάλειας
	Γνώση της διαχείρισης των πόρων
	Γνώση των πρακτικών διαχείρισης
	Γνώση των πλαισίων διαχείρισης κινδύνων

Η Sabine αποφάσισε να πάρει τη συμβουλή του καθοδηγητή της και να παραστεί σε τοπική συνεδρίαση του κεφαλαίου της ISACA για να διαπιστώσει αν ήταν η κατάλληλη. Αμέσως εντυπωσιάστηκε από τις ευκαιρίες που παρείχε. Το κεφάλαιο την καλωσόρισε θερμά, παρουσιάζοντάς την σε πολλούς βασικούς ανθρώπους που εργάζονταν ακριβώς στο είδος των ρόλων που αναζητούσε η Sabine και θα ήταν εξαίρετοι μέντορες ή υποστηρικτές.

Η πρόεδρος πιστοποίησης του κεφαλαίου ενημέρωσε τη Sabine ότι η πιστοποίηση του πιστοποιημένου διαχειριστή ασφάλειας πληροφοριών (CISM) θα ήταν πολύ κατάλληλη για την ίδια, δεδομένου ότι αποδεικνύει ότι διαθέτει σφαιρική γνώση της ασφάλειας των πληροφοριών, καθώς και ισχυρές διευθυντικές δεξιότητες. Η πιστοποίηση αφορά άτομα με πενταετή ή περισσότερα έτη πείρας και, ως εκ τούτου, η Sabine αποφάσισε να καταρτίσει 18μηνο πρόγραμμα σπουδών και πιστοποίησης.

Προσχώρησε στην ISACA ως μέλος τη νύχτα και αξιοποίησε πλήρως τους πόρους που προσέφερε η ένωση τόσο σε παγκόσμιο όσο και σε τοπικό επίπεδο. Προσχώρησε στις διαδικτυακές κοινότητες της ένωσης, άρχισε να συμμετέχει σε διαδικτυακά σεμινάρια και τοπικές συνεδριάσεις κεφαλαίου που προσφέρονται μέσω του SheLeadsTech, ενός προγράμματος που προσφέρει το Ίδρυμα «One in Tech» του ISACA. Και συμμετείχε σχεδόν σε κάθε συνεδρίαση του τοπικού κεφαλαίου που προσφέρθηκε.

Μόλις έξι μήνες μετά την ένταξή της, ένα άλλο μέλος του κεφαλαίου την προσέγγισε για μια θέση

αναλυτή ασφάλειας πληροφοριών στην οργάνωσή του.

Αποτέλεσμα

Ο Sabine είναι πλέον μέλος της ISACA εδώ και επτά χρόνια. Απέκτησε την πιστοποίηση CISM και σύντομα προωθήθηκε σε διευθύντρια ασφάλειας των πληροφοριών. Σήμερα είναι διευθύντρια ασφάλειας των πληροφοριών, με σαφή πορεία προς έναν ρόλο CISO.

Εκτός από την εξεύρεση διαπιστευτηρίων και θέσεων εργασίας μέσω της ISACA, η Sabine βρήκε επίσης αρκετούς πόρους που την βοήθησαν να προσθέσει αξία στην οργάνωσή της. Πριν από την έναρξη ισχύος του ΓΚΠΔ, η Sabine ήταν σε θέση να αξιοποιήσει τον κόμβο πόρων του ΓΚΠΔ που προσέφερε η ISACA για να την βοηθήσει να κατανοήσει διεξοδικά την κατάσταση και να μάθει ποια ήταν τα πλέον κρίσιμα μέτρα που έπρεπε να λάβει στο πλαίσιο του τρέχοντος ρόλου της.

Το ενδιαφέρον και η πείρα που απέκτησε στον τομέα της προστασίας ως αποτέλεσμα του εν λόγω σχεδίου, της επέτρεψαν να αποκτήσει το διαπιστευτήριο του «Certified Data Privacy Solutions Engineer» (CDPSE) της ISACA μέσω του προγράμματος πρώιμης υιοθεσίας.

Παρουσίασε σε διασκέψεις της ISACA σχετικά με το κεφάλαιο και τα εθνικά επίπεδα, ακονίζοντας τις επικοινωνιακές της δεξιότητες και πέρυσι έλαβε θέση επιτροπής κεφαλαίου. Ως διευθύντρια,

είχε την ευκαιρία να προσλάβει ορισμένες θέσεις και οι περισσότεροι από τους προσληφθέντες της προέρχονταν από το κεφάλαιο ISACA ακριβώς όπως βρήκε την πρώτη προαγωγή της πριν από έξι χρόνια. Έχοντας δει την αξία της πιστοποίησης CISM στη δική της σταδιοδρομία, άρχισε να προσφέρει την πιστοποίηση CISM στην ομάδα της μέσω προσφορών επιχειρηματικής κατάρτισης της ISACA.

Ο πλέον πρόσφατος τομέας εστίασης της Sabine, καθώς προετοιμάζεται για τον ρόλο της ως CISO, είναι η διασφάλιση των αναδυόμενων τεχνολογιών. Δεδομένης της αυξημένης ρυθμιστικής εστίασης στην ΤΝ στην Ευρώπη, έχει κατευθύνει πρώτα τις προσπάθειές της σε αυτόν τον τομέα, και πρόσφατα απέκτησε πιστοποιητικό βασικών αρχών τεχνητής νοημοσύνης από το ISACA.

Επτά χρόνια μετά το περπάτημα των θυρών της πρώτης συνεδρίασης του κεφαλαίου ISACA, η Sabine έχει διευρύνει το δίκτυό της από εκατοντάδες επαγγελματίες σε τοπικό επίπεδο και χιλιάδες παγκοσμίως.

Είναι με αυτοπεποίθηση ηγέτης και ομιλήτρια, και τώρα είναι καθοδηγήτρια πολλών άλλων που ήταν κάποτε στη θέση της. Μεταξύ των συμβουλών της προς τα μέλη της είναι να μαθαίνει πάντα και ότι η ISACA, ως παγκόσμια κοινότητα μάθησης, αποτελεί σπουδαίο πόρο.

Ο Sabine έχει περιγράψει τα μέτρα που πρέπει να ληφθούν για την απόκτηση της σειράς C και σχεδιάζει να αναλάβει ρόλο CISO εντός πέντε ετών. Είναι πεπεισμένη ότι το δίκτυο ISACA και τα διαπιστευτήριά της θα αποτελέσουν σημαντικό πλεονέκτημα καθώς επιδιώκει τους στόχους της.

Σταδιοδρομία:

- Αναλυτής SOC
- Ασφάλεια πληροφοριώνΑναλυτής
- Ασφάλεια πληροφοριώνΔιαχειριστής

- Διευθυντής Ασφάλειας Πληροφοριών.

Β.7 ΠΕΡΊΠΤΩΣΗ ΧΡΉΣΗΣ ΑΠΌ SANS/GIAC

Το παρόν τμήμα περιλαμβάνει μέρη από την περίπτωση χρήσης που συνέταξαν το ίδρυμα SANS και η GIAC (Global Information Assurance Certification)31.

Γιατί τα πλαίσια εργατικού δυναμικού και οι πιστοποιήσεις έχουν σημασία για την κυβερνοασφάλεια

Η οδηγία για τα δίκτυα και τις πληροφορίες (NIS) II αποτελεί επικαιροποίηση της υφιστάμενης εντολής για την Ευρωπαϊκή Ένωση. Αυτό θα συμβάλει στην ενθάρρυνση μιας κοινής γλώσσας για την ασφάλεια στον κυβερνοχώρο σε ευρύτερο φάσμα τομέων της οικονομίας και θα απαιτήσει την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών και μεταξύ των διαφόρων τομέων. Οδηγίες όπως η παρούσα έχουν όλο και μεγαλύτερη σημασία για τη δημιουργία προστατευτικών κιγκλιδωμάτων για τις δραστηριότητες στον κυβερνοχώρο. Για την προστασία της αξίας των μετόχων, η Επιτροπή Ασφάλειας και Ανταλλαγής (SEC) εξετάζει το ενδεχόμενο υποβολής έκθεσης στον κυβερνοχώρο για τις εισηγμένες στο χρηματιστήριο εταιρείες, η οποία θα απαιτεί την υποβολή εκθέσεων σχετικά με τον τρόπο με τον οποίο οι ομάδες ασφαλείας τους θα διαχειρίζονται τους κινδύνους, τα συμβάντα και την εμπειρογνωμοσύνη του διοικητικού συμβουλίου στον κυβερνοχώρο. Η έκθεση μετριασμού των κινδύνων για την ασφάλεια θα συνδέεται με τα σύνολα δεξιοτήτων για τους ρόλους εργασίας.

Τα πλαίσια συμβάλλουν στη διαμόρφωση αυτών των εργασιακών ρόλων. Οι περισσότερες θέσεις εργασίας που άνοιξαν μέχρι πρόσφατα ήταν γενικές καταχωρίσεις που ζητούσαν επαγγελματίες της ασφάλειας στον κυβερνοχώρο χωρίς σαφώς καθορισμένα καθήκοντα, δεξιότητες ή γνώσεις σχετικά με το τι απαιτείται για την προστασία των περιουσιακών στοιχείων των οργανισμών. Τα πλαίσια για το εργατικό δυναμικό, όπως το ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας του ECSF (ECSF), αρχίζουν να τυποποιούν τα ταλέντα που απαιτούνται για θέσεις ως ανταποκρινόμενος στον κυβερνοχώρο, ερευνητής ψηφιακών εγκληματολογικών ερευνών και υπεύθυνος ασφάλειας πληροφοριών. Η τυποποίηση επιτρέπει στους οργανισμούς να εντοπίζουν τα κατάλληλα ταλέντα για την αντιμετώπιση μελλοντικών απειλών. Αυτό συνάδει με άλλα επαγγέλματα. Για παράδειγμα, οι γιατροί διαθέτουν εξειδικευμένους τομείς, όπως ακτινολόγους, παιδιάτρους και εγκεφαλικούς χειρουργούς, οι οποίοι διαθέτουν την εμπειρογνωμοσύνη που απαιτείται στην περιοχή τους για την παροχή κατάλληλης θεραπείας.

Η πιστοποίηση διαδραματίζει σημαντικό ρόλο στην προετοιμασία των ατόμων για συγκεκριμένους εργασιακούς ρόλους. Η πιστοποίηση επικυρώνει το άτομο χρησιμοποιώντας βέλτιστες πρακτικές και κατευθυντήριες γραμμές για εκπαιδευτικές και ψυχολογικές εξετάσεις, όπως τα διεθνή πρότυπα ISO/IEC 17024. Παράδειγμα πιστοποίησης που θεωρείται παγκόσμιο πρότυπο είναι ο πιστοποιημένος δημόσιος λογιστής (CPA). Η επαγγελματική πείρα μπορεί να καταστήσει κάποιον εμπειρογνώμονα, αλλά η CPA αποτελεί τη βάση αναφοράς ενός πιστοποιημένου επαγγελματία και μπορεί ακόμη και να αποτελεί απαίτηση συμμόρφωσης σε συγκεκριμένα έργα ή ελέγχους.

Ορισμένα παραδείγματα στα οποία τα πλαίσια για το εργατικό δυναμικό συνέβαλαν στην προώθηση του κλάδου της ασφάλειας στον κυβερνοχώρο είναι τα εξής:

- Οι μεγάλες εταιρείες τεχνολογίας και οι χρηματοπιστωτικές εταιρείες συχνά διαθέτουν πολλαπλές ομάδες ασφάλειας που τυποποιούν τους εργασιακούς τους ρόλους και τις απαιτήσεις τους μέσω του πλαισίου για την εκ νέου τοποθέτηση και την ταχεία εναλλαγή των εργαζομένων με βάση την αποστολή.

- Οι οργανισμοί μπορούν να χαρτογραφήσουν την εμπειρία και την πιστοποίηση του εργατικού δυναμικού τους για την ταχεία αντιστοίχιση των δεξιοτήτων του προσωπικού

31 https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

με τις απαιτήσεις του σχεδίου. Αυτό είναι ιδιαίτερα σημαντικό για τις εταιρείες παροχής συμβουλών, τις εταιρείες τεχνολογίας και τους αναδόχους.

- Τα πλαίσια παρέχουν μια κοινή γλώσσα στο εργατικό δυναμικό σε όλους τους κλάδους, όπως η τεχνολογία, ο χρηματοπιστωτικός τομέας, η υγειονομική περίθαλψη, το λιανικό εμπόριο και οι υπηρεσίες κοινής ωφελείας, επιτρέποντας στις ομάδες να συνεργάζονται για την προστασία των απειλών κατά της ασφάλειας στον κυβερνοχώρο και της σωματικής ασφάλειας.

- Τα πλαίσια παρέχουν ένα υπόδειγμα ώστε τα ακαδημαϊκά ιδρύματα να γεφυρώσουν το χάσμα μεταξύ των εκπαιδευτικών τους προσφορών και των υφιστάμενων δεξιοτήτων κυβερνοασφάλειας που απαιτούνται σε όλους τους κλάδους, προετοιμάζοντας τους φοιτητές τους για θέσεις εργασίας.

Οι Sans και το GIAC κατανοούν τη σημασία των πλαισίων και έχουν ευθυγραμμίσει τα μαθήματα και τις πιστοποιήσεις με τα εν λόγω πλαίσια. Τα πλαίσια αποτελούν υπόδειγμα για την τυποποίηση των εργασιακών απαιτήσεων από τους οργανισμούς, παρόλο που κάθε οργανισμός και αποστολή θα χρειαστεί κάποια προσαρμογή ανάλογα με τη συγκεκριμένη αποστολή τους. Βοηθήσαμε να σχεδιάσουμε και να υλοποιήσουμε προγράμματα ανάπτυξης του εργατικού δυναμικού χρησιμοποιώντας πλαίσια ως υπόδειγμα για εταιρείες, κρατικούς οργανισμούς και οργανισμούς όλων των μεγεθών της Fortune 500.

TP-09-22-509-EN-N

ΣΧΕΤΙΚΆ ΜΕ ΤΟΝ ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ENISA, είναι ο οργανισμός της Ένωσης που ασχολείται με την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο οποίος ιδρύθηκε το 2004 και ενισχύθηκε με την πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στην πολιτική της ΕΕ για τον κυβερνοχώρο, ενισχύει την αξιοπιστία των προϊόντων, των υπηρεσιών και των διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, συνεργάζεται με τα κράτη μέλη και τα όργανα της ΕΕ και βοηθά την Ευρώπη να ετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της ευαισθητοποίησης, ο Οργανισμός συνεργάζεται με τα βασικά ενδιαφερόμενα μέρη για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την ενίσχυση της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας της κοινωνίας και των πολιτών της Ευρώπης. Περισσότερες πληροφορίες σχετικά με τον ENISA και το έργο του διατίθενται στη διεύθυνση: Βλ. www.enisa.europa.eu.

ENISA
Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Γραφείο Αθηνών
ΑΓΑΜΕΜΝΟΣ 14, ΧΑΛΑΝΔΗ 15231, ΑΤΤΙΚΗ, ΕΛΛΑΔΑ

Γραφείο Ηρακλείου
Νικολάου Πλάστρα 95
Βασιλική Βούτων 700 13, Ηράκλειο, Ελλάδα