

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



-- Πτυχιακή Εργασία --

Ασκήσεις κυβερνοασφάλειας στοχευμένες σε SOC (Security Operation Centers) και συσχέτιση με το εκπαιδευτικό πλαίσιο NICE-NIST

Ελευθέριος Καραβάρας

Επιβλέπων Καθηγητής: – Εμμανουήλ Μάγκος –

October 3, 2024

Επιβλέπων

Εμμανουήλ Μάγκος, Καθηγητής,
Ιόνιο Πανεπιστήμιο

Τριμελής Επιτροπή

Εμμανουήλ Μάγκος, Καθηγητής,
Ιόνιο Πανεπιστήμιο

Παναγιώτης Κουρουθανάσης, Καθηγητής,
Ιόνιο Πανεπιστήμιο

Χριστόφορος Νταντογιάν, Επίκουρος (Μόνιμος) Καθηγητής,
Ιόνιο Πανεπιστήμιο

Περίληψη

Η εργασία επικεντρώνεται στη δημιουργία προηγμένων εκπαιδευτικών χώρων για την ασφάλεια στον κυβερνοχώρο, οι οποίοι σχεδιάζονται ειδικά για να καλύπτουν τις ανάγκες των ομάδων που διαχειρίζονται την ασφάλεια των συστημάτων ενός οργανισμού. Στόχος είναι η βελτίωση της εκπαίδευσης και των δεξιοτήτων των επαγγελματιών σε αυτόν τον τομέα, μέσα από τη χρήση συγκεκριμένων προτύπων και κατευθύνσεων που καθοδηγούν τη διαδικασία εκπαίδευσης. Η ανάγκη για συνεχή εκπαίδευση και βελτίωση είναι ιδιαίτερα σημαντική, καθώς οι απειλές στον κυβερνοχώρο εξελίσσονται διαρκώς. Οι ομάδες που είναι υπεύθυνες για την προστασία των συστημάτων, οι οποίες εντοπίζουν και αντιδρούν στις επιθέσεις, χρειάζονται υψηλού επιπέδου δεξιότητες, κάτι που κάνει την εκπαίδευσή τους αναγκαία. Το άρθρο υποστηρίζει ότι, ενσωματώνοντας συγκεκριμένες προδιαγραφές στον σχεδιασμό των εκπαιδευτικών χώρων, μπορούν να δημιουργηθούν πιο αποτελεσματικά και στοχευμένα προγράμματα εκπαίδευσης. Οι εκπαιδευτικοί αυτοί χώροι είναι εικονικά περιβάλλοντα που επιτρέπουν την προσομοίωση πραγματικών επιθέσεων και καταστάσεων, δίνοντας στους συμμετέχοντες την ευκαιρία να βελτιώσουν τις δεξιότητές τους με ασφάλεια. Αυτά τα περιβάλλοντα βοηθούν στη διαδικασία μάθησης, προσφέροντας ρεαλιστικά σενάρια που καλύπτουν όλες τις φάσεις μιας επίθεσης. Το άρθρο παρουσιάζει παραδείγματα για το πώς αυτοί οι χώροι μπορούν να ωφελήσουν τις ομάδες που διαχειρίζονται την ασφάλεια των συστημάτων, τονίζοντας τα πρακτικά οφέλη, όπως η καλύτερη συνεργασία, η άμεση εφαρμογή των γνώσεων και η βαθύτερη κατανόηση των επιθέσεων. Τέλος, προτείνονται ιδέες για τη μελλοντική ανάπτυξη και βελτίωση αυτών των εκπαιδευτικών χώρων, όπως η εισαγωγή νέων τεχνολογιών και η δημιουργία πιο εξειδικευμένων σεναρίων που να ανταποκρίνονται στις σύγχρονες απειλές και ανάγκες. Συνολικά, υπογραμμίζεται η σημασία της δημιουργίας προσαρμοσμένων, ευέλικτων και υψηλής ποιότητας εκπαιδευτικών χώρων για την ενίσχυση των ομάδων που προστατεύουν τα συστήματα των οργανισμών και την καλύτερη αντιμετώπιση των απειλών στον κυβερνοχώρο.

Πρόλογος και Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Εμμανουήλ Μάγκο για την επίβλεψη αυτής της Πτυχιακής Εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο Εργαστήριο Δικτύων, Πολυμέσων και Ασφάλειας Συστημάτων (NMSLab). Επίσης, ευχαριστώ ιδιαίτερα τον υποψήφιο μεταδιδάκτορα δρ.Στυλιανό Καραγιάννη για την καθοδήγησή του και την εξαιρετική συνεργασία που είχαμε. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου για την καθοδήγηση και την ηθική συμπαράσταση που μου προσέφεραν όλα αυτά τα χρόνια.

Περιεχόμενα

Γλωσσάρι Ξενικών Όρων	1
1 Εισαγωγή	4
1.1 ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ	4
1.2 ΣΥΝΕΙΣΦΟΡΑ	5
1.3 ΜΕΘΟΔΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ	6
1.4 ΠΑΡΟΜΟΙΕΣ ΕΡΓΑΣΙΕΣ	8
1.5 ΔΟΜΗ ΕΡΓΑΣΙΑΣ	9
2 Βιβλιογραφική Επισκόπηση	10
2.1 ΑΝΑΓΚΑΙΟΤΗΤΑ ΤΩΝ VIRTUAL – HANDS ON LABS	10
2.2 TEAM DEFINITIONS	12
2.3 ΤΙ ΕΙΝΑΙ ΤΑ CYBER RANGES	14
2.4 APPROACHES ΤΩΝ CYBER RANGES	16
2.5 ΤΙ ΕΙΝΑΙ ΤΑ CTF (CAPTURE THE FLAG)	17
2.6 CTF APPROACHES	18
2.7 ΕΡΓΑΛΕΙΑ SECURITY LABS	20
2.7.1 Intrusion Detection Systems (IDS)	20
2.7.2 Εργαλεία Ανίχνευσης Ευπαθειών	20
2.7.3 Firewalls	22
2.7.4 Security Information and Event Management (SIEM)	23
2.7.5 Machine Learning & Network Flows	25
2.7.6 Λύσεις Εικονικοποίησης (Virtualization)	25
2.7.7 Digital Forensics	26

<i>Περιεχόμενα</i>	iv
2.7.8 Decision support systems	27
2.7.9 Threat Intelligence	27
3 Εκπαιδευτικά Πλαίσια	29
3.1 ΠΕΡΙΓΡΑΦΗ	29
3.2 NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) FRAMEWORK	30
3.3 ACM CURRICULUM 2017 (CSEC2017)	36
3.4 NATIONAL SECURITY AGENCY - CENTER OF ACADEMIC EXCEL- LENCE IN CYBER DEFENSE (NSA CAE-CD)	39
4 Τλοποιήση	42
4.1 ΣΤΟΧΟΣ ΣΕΝΑΡΙΩΝ ΜΑΘΗΣΗΣ	42
4.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΕΝΑΡΙΩΝ ΜΑΘΗΣΗΣ	43
4.3 ΣΧΕΔΙΑΣΜΟΣ ΤΩΝ ΣΕΝΑΡΙΩΝ ΜΑΘΗΣΗΣ ΚΑΤΑ NICE FRAMEWORK .	44
5 Συμπεράσματα	55

Κατάλογος Σχημάτων

2.1	Ταξινόμηση των Cyber Ranges.	16
3.2	Σχέση μεταξύ των διαφορετικών τμημάτων της δομής του πλαισίου NICE.	33
3.3	Σύνοψη βασικών δομικών στοιχείων των τριών εκπαιδευτικών πλαισίων CSEC2017, NSA CAE-CD &NIST Special Publication 800-181. Εικόνα τροποποιημένη από [38]	41
4.4	Απεικόνιση Αρχιτεκτονικής Δικτύου	44

Κατάλογος Πινάκων

3.1	Πλήρης δομή του <i>NIST Special Publication 800-181</i>	36
3.2	<i>CSEC2017</i> : "Δομικοί λίθοι" και σύντομη περιγραφή αυτών. .	38
3.3	Σύγκριση των τριών εκπαιδευτικών πλαισίων <i>CSEC2017</i> , <i>NSA CAE-CD</i> & <i>NIST Special Publication 800-181</i>	40
4.1	Σενάριο 01: <i>SOC01 Cisco Switch</i>	45
4.2	Σενάριο 02: <i>SOC02 UTM</i>	46
4.3	Σενάριο 03: <i>SOC03 WAF</i>	47
4.4	Σενάριο 04 & Σενάριο 05: <i>SOC04</i> & <i>SOC05 Domain Controller</i>	48
4.5	Σενάριο 06 & Σενάριο 07: <i>SOC06</i> & <i>SOC07 Web Server</i>	48
4.6	Σενάριο 08 & Σενάριο 09: <i>SOC08</i> & <i>SOC09 File Server</i>	49
4.7	Σενάριο 10 & Σενάριο 11: <i>SOC10</i> & <i>SOC11 Database Server</i>	50
4.8	Σενάριο 12: <i>SOC12 Mail Service</i>	51
4.9	Σενάριο 13: <i>SOC13 Mail Gateway</i>	51
4.10	Σενάριο 14: <i>SOC14 Honeypot/Deception Traps</i>	52
4.11	Σενάριο 15: <i>SOC15 SIEM</i>	53
4.12	Σενάριο 16: <i>SOC16 Kali Linux</i>	54
5.1	Αντιστοίχιση της κάλυψης της πλατφόρμας κυβερνοάμυνας με το πλαίσιο <i>NICE</i> για τους πιο σχετικούς ρόλους εργασίας.	56

Γλωσσάρι Ξενικών Όρων

Security Operations Center	Επιχειρησιακό Κέντρο Ασφάλειας
Capture the Flag	Διαδραστική Άσκηση Κατάκτησης Στόχου
Cyber Range	Εικονικό Περιβάλλον Κυβερνοτεχνολογίας
SOC Analyst Level 1	Αναλυτής Περιστατικών Ασφαλείας Επιπέδου 1
Framework	Πλαίσιο/Πρότυπο
Hands on Lab	Διαδραστικό Τεχνικό Εργαστήριο
Teaming	Ομαδοποίηση
Security Labs	Εργαστήρια Κυβερνοασφάλειας
Digital Forensics	Ψηφιακή Εγκληματολογία
Decision Support System	Σύστημα Υποστήριξης Λήψης Αποφάσεων
Threat intelligence	Υπηρεσία Πληροφοριών σχετικά με απειλές

Host	Κόμβος
Virtual Private Network	Εικονικό Ιδιωτικό Δίκτυο
High Availability	Υψηλή Διαθεσιμότητα
Switch	Δικτυακός Μεταγωγέας
Firewall	Τείχος Προστασίας
Network protection	Προστασία Δικτύου
Intrusion Prevention	Αποτροπή Διείσδυσης
Sandboxing	Εκτέλεση σε απομονωμένο περιβάλλον
Web Service	Δικτυακή Υπηρεσία
Web Application Firewall	Τείχος Προστασίας Δικτυακής Εφαρμογής
Domain Controller	Ελεγκτής Τομέα
Active Directory	Κατάλογος Τομέα
Web Server	Δικτυακός Εξυπηρετητής
File Server	Εξυπηρετητής Αρχείων

Database Server	Εξυπηρετητής Βάσης Δεδομένων
Mail Service	Εξυπηρετητής Ηλεκτρονικής Αλληλογραφίας
Mail Gateway	Εξυπηρετητής Προστασίας Ηλεκτρονικής Αλληλο- γραφίας
Honeypot	Παγίδα
Deception Trap	Παγίδα Εξαπάτησης

Κεφάλαιο 1

Εισαγωγή

Στο κεφάλαιο αυτό θα αναλυθεί η κατάσταση καθώς και τα προβλήματα που εντοπίζονται και που η συγκεκριμένη εργασία έχει σκοπό να επιλύσει, τον τρόπο με τον οποίο ερευνητές έχουν προσεγγίσει τα αναφερόμενα προβλήματα όπως επίσης και την ανάλυση της μεθόδου που προτείνεται για την επίλυση αυτών.

1.1 Υφιστάμενη Κατάσταση

Η κυβερνοασφάλεια είναι ένα επιστημονικό πεδίο που γίνεται όλο και πιο σημαντικό, καθώς αυξάνονται τόσο ο αριθμός όσο και η πολυπλοκότητα των ψηφιακών απειλών. Σύμφωνα με το Διεθνές Κονσόρτιουμ Πιστοποίησης για την Ασφάλεια Πληροφοριακών Συστημάτων (ISC²)¹, υπάρχει ένα κενό στην αγορά εργασίας της κυβερνοασφάλειας που ανέρχεται σε περίπου 4 εκατομμύρια θέσεις[1]. Παρά τις προσπάθειες για την επίλυση αυτού του ζητήματος, η έλλειψη δεξιοτήτων παραμένει μια σημαντική πρόκληση στον τομέα. Αυτό γίνεται ακόμα πιο εμφανές σε ένα Security Operations Center (SOC) όπου αποτελεί την πρώτη γραμμή ανίχνευσης μιας κυβερνοεπίθεσης ενός .

Για να αντιμετωπίσει αυτό το κενό στις δεξιότητες και το εργατικό δυναμικό, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας ξεκίνησε την Εθνική Πρωτοβουλία για την Εκπαίδευση στην Κυβερνοασφάλεια (NICE)[2]. Το πλαίσιο NICE έχει ευρέως αναγνωριστεί για την επιτυχία του στη δημιουργία ενός εκτενούς σώματος γνώσης που καθορίζει τις βασικές έννοιες και πρακτικές για τους επαγγελματίες της κυβερνοασφάλειας.

¹<https://www.isc2.org/>

Παράλληλα, η παροχή πρακτικού εκπαιδευτικού υλικού που περιλαμβάνει ασκήσεις σε ρεαλιστικά ψηφιακά περιβάλλοντα είναι ζωτικής σημασίας[3]. Αυτό το ζήτημα έχει αντιμετωπιστεί στο παρελθόν μέσω προκλήσεων Capture the Flag (CTF)[4] και εικονικών εργαστηρίων, οι οποίες όμως έχουν συνήθως εφαρμογή σε Red Teams αν και τα τελευταία χρόνια γίνονται προσπάθειες δημιουργίας πλατφορμών CTF για Blue Teams όπως είναι το Cyberdefenders² και το Blue Team Labs³

Οι προκλήσεις CTF και τα εικονικά εργαστήρια είναι ιδιαίτερα σημαντικά, αλλά η ενσωμάτωση των ανθρώπινων και τεχνολογικών παραμέτρων, καθώς και η διεπιστημονική προσέγγιση στα πολύπλοκα θέματα της κυβερνοασφάλειας, μπορούν να ενισχυθούν περαιτέρω μέσω των Cyber Ranges. Τα Cyber Ranges προσφέρουν προσομοιωμένα δικτυακά περιβάλλοντα για την εκπαίδευση, τη δοκιμή και τα πειράματα στην κυβερνοασφάλεια, προσομοιώνοντας ρεαλιστικά σενάρια. Μέσω αυτών των προσομοιώσεων, τα Cyber Ranges προσφέρουν πρακτική εμπειρία, ενισχύουν τις δεξιότητες επίλυσης προβλημάτων και δίνουν έμφαση στη συνεργασία και την ομαδική εργασία, που είναι θεμελιώδη στοιχεία για την κυβερνοασφάλεια. Παρόλα τα πλεονεκτήματα των Cyber Ranges, κατά την συγγραφή της εργασίας δεν υπάρχουν διαθέσιμα αρκετά Cyber Ranges όσον αφορά τον τομέα της κυβερνοασφάλειας και πιο συγκεκριμένα της κυβερνοάμυνας.

Τόσο τα Cyber Ranges όσο και τα CTF συνήθως δεν βασίζονται σε κάποιο εκπαιδευτικό πλαίσιο ενώ επίσης τις περισσότερες φορές δεν είναι ξεκάθαρος ποιος είναι ο εκπαιδευτικός σκοπός αυτών. Η παρούσα εργασία έρχεται να καλύψει τις παραπάνω ελλείψεις στον τομέα εκπαίδευσης του νέου προσωπικού στον χώρο αυτό.

1.2 Συνεισφορά

Σκοπός της εργασίας είναι να αποδείξει πόσο αποτελεσματική είναι η εφαρμογή του πλαισίου NICE στη βελτίωση του σχεδιασμού σεναρίων και της ανάπτυξης Cyber Ranges για την εκπαίδευση νέου προσωπικού που θα ενταχθεί στην ομάδα ενός SOC, προσφέροντας μια πιο ρεαλιστική και ευέλικτη εμπειρία εκπαίδευσης. Πιο συγκεκριμένα η εργασία επικεντρώνεται στη μεθοδολογία, την ανάλυση και τα αποτελέσματα που μπορούν να βοηθήσουν τους εκπαιδευτές να δημιουργήσουν ή να βελτιώσουν τα Cyber Ranges, κατασκευάζοντας σχετικά σενάρια που ταιριάζουν με τα εκπαιδευτικά πρότυπα. Η κύρια συνεισφορά επικεντρώνεται

²<https://cyberdefenders.org/>

³<https://blueteamlabs.online/>

στους παρακάτω τομείς:

- Ανάλυση και παρουσίαση των διάφορων Εκπαιδευτικών Πλαισίων που έχουν εφαρμογή στον χώρο της Κυβερνοασφάλειας
- Σχεδιασμός ενός Cyber Range και αντιστοίχηση του με εκπαιδευτικό πλαίσιο NICE με σκοπό την εκπαίδευση ενός νεοεισερχόμενου SOC Analyst Level 1
- Ανάπτυξη του παραπάνω Cyber Range με την δημιουργία 16 Σεναρίων ικανά να καλύψουν το μεγαλύτερο ποσοστό των ζητούμενων και με σκοπό την αποτελεσματικότερη, ταχύτερη και πιο διαδραστική εμπειρία του εκπαιδευόμενου

1.3 Μεθοδολογική Προσέγγιση

Στα πλαίσια εκπόνησης της παρούσας εργασία επιλέχθηκε η χρήση του πλαισίου NICE. Η επιλογή αυτή έγινε λόγω της ολοκληρωμένης δομής του και της έμφασης στους δείκτες ικανοτήτων. Αυτοί οι δείκτες βοηθούν στην αξιολόγηση των σεναρίων και διασφαλίζουν ότι αυτά αντικατοπτρίζουν σημαντικές προκλήσεις στον τομέα της κυβερνοασφάλειας. Επιπλέον, το πλαίσιο NICE παραμένει ενημερωμένο με τις τελευταίες εξελίξεις, ενώ εναρμονίζεται με τις απαιτήσεις των σύγχρονων επαγγελματικών ρόλων.

Η προτεινόμενη διαδικασία ανάπτυξης, η οποία αποτελείται από τρία βήματα, ξεκινά με την αναζήτηση στο πλαίσιο NICE για τις κατάλληλες Κατηγορίες Εργασίας αλλά και τις σχετικές Ειδικότητες που συνάδουν με τους εκπαιδευτικούς μας στόχους. Στη συνέχεια, σχεδιάζεται η αρχιτεκτονική της άσκησης κυβερνοασφάλειας, ακολουθούμενη από τον σχεδιασμό των σεναρίων. Το τρίτο και τελευταίο βήμα επικεντρώνεται στην αξιολόγηση των σεναρίων με τη χρήση δεικτών ικανοτήτων από το πλαίσιο NICE, προκειμένου να διευκολυνθούν τυχόν αναθεωρήσεις των ανεπτυγμένων σεναρίων.

Πιο αναλυτικά:

- Βήμα I: Ορισμός των εκπαιδευτικών στόχων. Οι εκπαιδευτικοί στόχοι διαμορφώνονται μέσα από την επιλογή των σχετικών κατηγοριών εργασίας και των αντίστοιχων ειδικοτήτων. Αυτή η διαδικασία περιλαμβάνει τον καθορισμό γενικών, στρατηγικών στόχων που θα καθοδηγήσουν το πλάνο εκπαίδευσης. Η διαμόρφωση αυτών των στόχων βοηθά στην επιλογή μίας ευρείας λίστας πιθανών ρόλων που θα καλυφθούν

από το εκπαιδευτικό περιβάλλον της κυβερνοασφάλειας. Παράλληλα, οι σχετικοί δείκτες ικανοτήτων λειτουργούν ως οδηγός για την ανάπτυξη ενός σαφούς σχεδίου για τον σχεδιασμό των εκπαιδευτικών σεναρίων, εξασφαλίζοντας έτσι την αποτελεσματική κάλυψη όλων των απαραίτητων δεξιοτήτων.

- **Βήμα II: Σχεδιασμός της αρχιτεκτονικής και των σεναρίων.** Σε αυτό το βήμα, δίνεται έμφαση στον καθορισμό της αρχικής αρχιτεκτονικής και της τοπολογίας του περιβάλλοντος κυβερνοασφάλειας, καθώς και στη δημιουργία των σχετικών σεναρίων εκπαίδευσης. Αρχικά, όταν δημιουργείται ένα περιβάλλον κυβερνοασφάλειας (cyber range), η αρχιτεκτονική του καθορίζεται με βάση διάφορους παράγοντες: τους ειδικούς εκπαιδευτικούς στόχους που έχουν τεθεί, τους τύπους των κυβερνοαπειλών που πρόκειται να προσομοιωθούν, τους διαθέσιμους πόρους, και τα χαρακτηριστικά του εκπαιδευόμενου κοινού. Αυτή η αρχική διαμόρφωση της αρχιτεκτονικής χρησιμεύει ως το θεμέλιο για τον μετέπειτα σχεδιασμό και την υλοποίηση του περιβάλλοντος. Ο σχεδιασμός των σεναρίων περιλαμβάνει την ανάπτυξη ρεαλιστικών σεναρίων κυβερνοεπιθέσεων μέσα στο συγκεκριμένο εκπαιδευτικό πλαίσιο. Καθώς ο σχεδιασμός αυτών των σεναρίων προχωρά, μπορεί να αποκαλυφθεί ότι ορισμένα στοιχεία της αρχικής αρχιτεκτονικής του περιβάλλοντος κυβερνοασφάλειας χρειάζονται προσαρμογή ή αλλαγή, ώστε να υποστηρίξουν καλύτερα τα σενάρια που έχουν δημιουργηθεί και να διασφαλίζουν την αποτελεσματικότητα της εκπαιδευτικής διαδικασίας. Συμπληρωματικά στο Βήμα I, οι επιλεγμένες Ειδικότητες συνδέονται με μικρότερα, πιο εξειδικευμένα σενάρια, τα οποία συμβάλλουν στη διαμόρφωση μιας ολοκληρωμένης εκπαιδευτικής πορείας, διασφαλίζοντας ότι οι συμμετέχοντες αποκτούν τις απαραίτητες δεξιότητες με στοχευμένο και συστηματικό τρόπο.
- **Βήμα III: Αξιολόγηση.** Σε αυτό το βήμα πραγματοποιείται η αξιολόγηση για τον υπολογισμό της συνολικής κάλυψης των δεικτών ικανοτήτων και για να διαπιστωθεί αν τα σενάρια καλύπτουν τους επιλεγμένους ρόλους εργασίας. Η διαδικασία αξιολόγησης βοηθά στον εντοπισμό τυχόν κενών ή ελλείψεων, επιτρέποντας έτσι τη συνεχή βελτίωση και προσαρμογή των σεναρίων, ώστε να επιτευχθούν οι εκπαιδευτικοί στόχοι που έχουν τεθεί. Η αξιολόγηση μπορεί να χρησιμοποιηθεί για την αναγνώριση των ελλειπόντων στοιχείων στα αναπτυγμένα σενάρια και να προσφέρει προτάσεις για αναθεώρηση ή επέκταση, προκειμένου να ενισχυθεί η αποτελεσματικότητά τους στην εκπαίδευση των εννοιών της κυβερνοασφάλειας. Οι πληροφορίες που συλλέγονται κατά τη διάρκεια της αξιολόγησης μπορούν να αξιοποιηθούν για τον ανασχεδιασμό ή την ενημέρωση των σεναρίων στο Βήμα II της μεθοδολογίας.

1.4 Παρόμοιες Εργασίες

Πολλοί ερευνητές τα τελευταία χρόνια έχουν φέρει στο επίκεντρο της προσοχής την σημαντικότητα ύπαρξης των Cyber Ranges καθώς μέσω αυτών καλύπτεται το κενό στην εκπαίδευση των νεοεισερχομένων στον χώρο της Κυβερνοασφάλειας.

Η μελέτη των Chouliaras et. al. [5] εξετάζει cyber ranges και τον ρόλο τους στην εκπαίδευση και την ανάπτυξη ικανοτήτων στον τομέα της κυβερνοασφάλειας. Αναλύει τις διάφορες εφαρμογές των cyber ranges, όπως την εκπαίδευση προσωπικού, την προσομοίωση επιθέσεων, και την ανάπτυξη και δοκιμή νέων τεχνολογιών ασφαλείας. Επιπλέον, η μελέτη εντοπίζει και συζητά τις προκλήσεις που αντιμετωπίζουν οι πλατφόρμες αυτές, όπως η πολυπλοκότητα στη σχεδίαση και ανάπτυξη, το υψηλό κόστος και οι απαιτήσεις σε εξειδικευμένο προσωπικό. Τέλος, προτείνονται λύσεις και μελλοντικές κατευθύνσεις για την περαιτέρω βελτίωση και υιοθέτηση των cyber ranges στην εκπαίδευση και την έρευνα της κυβερνοασφάλειας.

Αντίστοιχα στην μελέτη των Russo et. al. [6] εξετάζεται η βιβλιογραφία σχετικά με την εκπαίδευση στην κυβερνοασφάλεια μέσω σεναρίων. Περιγράφονται τα πλεονεκτήματα της χρήσης σεναρίων για την εκπαίδευση των επαγγελματιών, όπως η ρεαλιστική προσομοίωση επιθέσεων και η ενίσχυση της ετοιμότητας και των δεξιοτήτων αντιμετώπισης περιστατικών. Η μελέτη εντοπίζει επίσης τις προκλήσεις στην υλοποίηση αυτής της προσέγγισης, όπως η ανάγκη για συνεχή ενημέρωση των σεναρίων και η εξασφάλιση ότι τα σενάρια αντικατοπτρίζουν τις πραγματικές απειλές.

Η μελέτη από τους Vykopal et. al. [7] εξετάζει τα διδάγματα από τη διεξαγωγή σύνθετων ασκήσεων άμυνας σε περιβάλλον κυβερνοασκήσεων. Η έρευνα επικεντρώνεται στις προκλήσεις και τις βέλτιστες πρακτικές για τη σχεδίαση και υλοποίηση αυτών των ασκήσεων, οι οποίες προσομοιώνουν ρεαλιστικά σενάρια κυβερνοεπιθέσεων. Τα βασικά συμπεράσματα περιλαμβάνουν την ανάγκη για προσεκτικό σχεδιασμό, τη σημασία της συνεργασίας και ομαδικής δουλειάς, τις τεχνικές απαιτήσεις για αξιόπιστη υποδομή και την αξία της ανατροφοδότησης για τη βελτίωση των δεξιοτήτων των συμμετεχόντων. Συνολικά, η μελέτη υπογραμμίζει τη σημασία των κυβερνοασκήσεων για την αποτελεσματική εκπαίδευση στην κυβερνοασφάλεια.

Η μελέτη των Vielberth et. al. [8] παρουσιάζει μια προσέγγιση που Εβασίζεται στη δημιουργία ψηφιακών διδύμων, τα οποία αποτελούν ρεαλιστικά αντίγραφα δικτύων και συστημάτων ενός οργανισμού. Αυτά τα αντίγραφα επιτρέπουν στους SOC αναλυτές να εξασκούνται σε πραγματικές συνθήκες, εντοπίζοντας και αντιμετωπίζοντας κυβερνοεπιθέσεις με ασφάλεια και ακρίβεια. Η χρήση τέτοιων συστημάτων ενισχύει την προετοιμασία των επαγγελματιών, βελτιώνοντας

τις αντιδράσεις τους σε πραγματικές επιθέσεις και ενισχύοντας την ανθεκτικότητα των πληροφοριακών συστημάτων.

Παράλληλα ερευνητές έχουν αξιοποιήσει το πρότυπο NICE με σκοπό είτε την αξιολόγηση της έρευνας τους είτε με σκοπό την υποβοήθηση αυτής.

Πρώτο παράδειγμα είναι η μελέτη των Dawson et. al. [9] η οποία εξετάζει την ενσωμάτωση εργαστηρίων ασφαλούς μηχανικής λογισμικού για την κάλυψη των καθηκόντων που ορίζονται από το πλαίσιο NICE για την κυβερνοασφάλεια και τη διασφάλιση λογισμικού. Η έρευνα αναλύει πώς τα εργαστήρια αυτά μπορούν να ενισχύσουν τις δεξιότητες των φοιτητών και των επαγγελματιών στον τομέα της κυβερνοασφάλειας, προσφέροντας πρακτική εμπειρία σε πραγματικά σενάρια ασφάλειας λογισμικού. Τα κύρια συμπεράσματα περιλαμβάνουν τη σημασία της πρακτικής εκπαίδευσης για την ανάπτυξη των απαραίτητων δεξιοτήτων και γνώσεων, καθώς και την ανάγκη για συνεχή ανανέωση των εργαστηριακών ασκήσεων ώστε να αντικατοπτρίζουν τις σύγχρονες απειλές και τεχνολογίες.

Με αφορμή την δημιουργία προγραμμάτων σπουδών στον τομέα της Κυβερνοασφάλειας, οι Hajny et. al. [10] εστιάζουν στις ανάγκες της αγοράς εργασίας και στις απαιτήσεις δεξιοτήτων κυβερνοασφάλειας, καθορίζοντας τις κατευθυντήριες γραμμές για τα εκπαιδευτικά ιδρύματα. Η μελέτη επισημαίνει τη σύνδεση με το πλαίσιο NICE, το οποίο προσφέρει μια δομημένη προσέγγιση για την εκπαίδευση και την ανάπτυξη δεξιοτήτων κυβερνοασφάλειας. Η υιοθέτηση του πλαισίου NICE βοηθά τα εκπαιδευτικά ιδρύματα να διαμορφώσουν προγράμματα που ανταποκρίνονται στις σύγχρονες απαιτήσεις και προκλήσεις της κυβερνοασφάλειας.

1.5 Δομή Εργασίας

Το υπόλοιπο της εργασίας διαμορφώνεται ως εξής: Στην ενότητα 2 αναλύονται όροι, ορισμοί και τεχνολογίες που θα βοηθήσουν στην κατανόηση της εργασίας ενώ στην Ενότητα 3, παρέχονται πληροφορίες σχετικά με τα διαφορετικά εκπαιδευτικά πλαίσια και λεπτομέρειες για το πλαίσιο NICE πάνω στο οποίο βασίζεται και η εργασία αυτή. Η Ενότητα 4 περιγράφει τα βήματα σχεδίασης και ανάπτυξης ενός Cyber Range που είναι σχεδιασμένο βάσει του NICE. Τέλος, στο κεφάλαιο 5 παρουσιάζονται τα συμπεράσματα και οι πιθανές προεκτάσεις της εργασίας.

Κεφάλαιο 2

Βιβλιογραφική Επισκόπηση

Σε αυτό το κεφάλαιο, πραγματοποιείται βιβλιογραφική διερεύνηση σε ολόκληρο το πεδίο και μια εκτενής παρουσίαση διαφόρων υλοποιήσεων, προτύπων, frameworks, πρωτοκόλλων και τεχνολογιών. Ειδικότερα, περιλαμβάνει εκτενή αναφορά και ανάλυση σε έννοιες όπως Hands on labs, Teaming, Cyber Ranges, Capture The Flag, και σε βασικά εργαλεία για Security Labs, Digital Forensics, Decision support systems, Threat intelligence.

2.1 Αναγκαιότητα των Virtual – Hands on labs

Ο τομέας του information security (ασφάλεια των πληροφοριών) παρουσιάζει συνεχείς μεταβολές. Η αναγκαιότητα της διαρκούς εξέλιξης του έγκειται στο γεγονός ότι καλείται να αντιμετωπίσει καθημερινά νέους τύπους απειλών και εγκλημάτων που έχουν ως στόχο επιχειρήσεις, οργανισμούς και κυβερνήσεις [11]. Συνεπώς, οι εργαζόμενοι στον εν λόγω τομέα οφείλουν να έχουν επαρκή κατάρτιση και επίγνωση των διαθέσιμων διαχειριστικών, επιχειρησιακών και τεχνικών ελέγχων που απαιτούνται, για την προστασία των πόρων για τους οποίους είναι υπεύθυνοι [12].

Η ύπαρξη ικανών ειδικευμένων επαγγελματιών στην ασφάλεια πληροφοριών και δικτύου συνδέεται άρρηκτα με την ποιότητα εκπαίδευσης που λαμβάνουν, σε θέματα ασφάλειας λογισμικού στην επιστήμη των υπολογιστών ή σε συναφή προγράμματα [13]. Το παραπάνω, επιτυγχάνεται όταν η εκμάθηση του θεωρητικού πλαισίου συνοδεύεται από εμπειρίες σε πρακτικό επίπεδο, προκειμένου να αποκτηθεί μια σφαιρική γνώση του αντικειμένου. Για παράδειγμα, είναι

ωφέλιμο για τους εκπαιδευόμενους να δουν πώς σχεδιάζεται και εκτελείται μια επίθεση, ώστε να αναζητήσουν τον καλύτερο τρόπο προστασίας από τέτοιες απειλές. Η πρακτική εφαρμογή της θεωρίας πραγματοποιείται άλλοτε με τη χρήση πραγματικών πρακτικών στα εργαστήρια, ή με τη χρήση λογισμικού προσομοίωσης στη διδασκαλία και εκμάθηση της δικτύωσης υπολογιστών [14]. Ορισμένες φορές προτείνεται η χρήση και των δύο προσεγγίσεων για τη μεγιστοποίηση των δυνάμεων και την ελαχιστοποίηση των αδυναμιών κάθε προσέγγισης.

Τα Hands - On virtual labs αποτελούν ένα μέσο που επιτρέπει την απόκτηση πρακτικής εμπειρίας σε ένα ασφαλές εικονικό περιβάλλον, απαλλάσσοντας τον εκπαιδευόμενο από τυχόν ηθικούς ή νομικούς περιορισμούς [12]. Μεταξύ των διαφόρων εκπαιδευτικών μεθόδων στην εκπαίδευση στην επιστήμη των υπολογιστών, τα Hands - On virtual labs έχουν μοναδικές ιδιότητες κατανόησης της συμπεριφοράς του εκπαιδευόμενου και αξιολόγησης της επίδοσης του, παρέχοντας μια εξατομικευμένη εμπειρία μάθησης [15]. Πλατφόρμες όπως η εκπαίδευση του Amazon AWS, MyIT Lab της Pearson, Microsoft Azure στην εκπαίδευση και το Cloud-Lab υποστηρίζουν τους μαθητές ώστε να έχουν απομακρυσμένη πρόσβαση σε πόρους για ένα πρακτικό εργαστήριο πληροφορικής με σκοπό την εκμάθηση προγραμματισμού, δικτύωσης και ασφάλειας στον κυβερνοχώρο [15].

Οι δε Li και Xie [16] αναφέρουν ότι τα Hands - On labs αποτελούν σημαντικά και αποτελεσματικά μέσα για την εκπαίδευση και την κατάρτιση στον κυβερνοχώρο, καθώς μπορούν να τονώσουν σημαντικά το ενδιαφέρον των εκπαιδευόμενων για την ασφάλεια και να ενισχύσουν τις γνώσεις και τις δεξιότητές τους σε θέματα ασφάλειας. Στην εργασία τους, παρουσιάζουν το “Platoon”, μια εικονική πλατφόρμα χαμηλού κόστους, προσανατολισμένη στην ομάδα για ασκήσεις κυβερνοασφάλειας. Το παραπάνω έρχεται σαν λύση στην θεωρία τους πως είναι συχνά δύσκολο ή δαπανηρό να εφαρμοστούν ομαδικές ασκήσεις ασφαλείας χρησιμοποιώντας αυτές τις πλατφόρμες, καθώς στοχεύουν κυρίως μεμονωμένους μαθητές.

Οι Deng et al. [17] αναφέρουν πως οι περισσότερες από τις υπάρχουσες πρακτικές ασκήσεις ή εργαστηριακά υλικά συνήθως διαχειρίζονται με προβληματικό τρόπο ή δεν διαθέτουν συνεκτικό τρόπο διαχείρισης των υφιστάμενων εργαστηρίων και παροχής παραγωγικού εργαστηρίου για την άσκηση των εκπαιδευόμενων στον κυβερνοχώρο. Επιπλέον, παρά το γεγονός ότι η αποτελεσματική εκπαίδευση στον κυβερνοχώρο βασίζεται κυρίως σε πρακτικά εργαστήρια, με έμφαση σε πρακτικές δεξιότητες επίλυσης προβλημάτων αντί σε θεωρία και μοντέλα, στις περισσότερες περιπτώσεις δεν εφαρμόζεται. Σε γενικές γραμμές, είναι δύσκολο να δημιουργηθεί ένα αποτελεσματικό και προσαρμοστικό πρόγραμμα μάθησης για τους φοιτητές πληροφορικής ανάλογα με το προσωπικό τους υπόβαθρο και τους μαθησιακούς τους στόχους [17].

Συνοψίζοντας, οι δραστηριότητες σε πρακτικό επίπεδο για την εκπαίδευση και κατάρτιση στον τομέα της κυβερνοασφάλειας είναι κρίσιμες, δεδομένου ότι οι κυβερνοεπιθέσεις συμβαίνουν σήμερα σε ολοένα αυξανόμενη κλίμακα. Μόνο τέτοιες πρακτικές δραστηριότητες μπορούν να διασφαλίσουν ότι οι ασκούμενοι θα αποκτήσουν τις πραγματικές δεξιότητες που είναι αναγκαίες για την άμεση αντιμετώπιση συμβάντων ασφάλειας σε πραγματικές καταστάσεις [15]. Ωστόσο, λόγω της εγγενούς ποικιλομορφίας των γνώσεων και των δεξιοτήτων στον τομέα της κυβερνοασφάλειας, είναι δύσκολο να εξατομικευθεί η διαδικασία μάθησης και να παρακολουθηθεί το επίπεδο μάθησης μεμονωμένων μαθητών.

2.2 Team Definitions

Μια ομάδα άσκησης στην κυβερνοασφάλεια, απαρτίζεται από άτομα τα οποία που σχεδιάζουν, αναπτύσσουν, διαχειρίζονται και συμμετέχουν σε αυτή. Με βάση το ρόλο που έχει μια ομάδα για στην υλοποίηση της άσκησης, ανατίθενται διαφορετικά χρώματα προκειμένου να προσδιοριστεί ο ρόλος αυτός. Σύμφωνα με τους Yamin, Katt και Gkioulos [18], οι ομάδες έχουν ως εξής:

- Η **κόκκινη ομάδα (red team)** είναι μια ομάδα αξιολόγησης της ασφάλειας των πληροφοριών μέσω του εντοπισμού ευπαθειών που υπάρχουν σε ένα σύστημα κατά τη διάρκεια μιας άσκησης ή μιας δοκιμής. Η κόκκινη ομάδα είναι υπεύθυνη για τον εντοπισμό και την εκμετάλλευση των πιθανών τρωτών σημείων που υπάρχουν στο περιβάλλον άσκησης.
- Η **μπλε ομάδα (blue team)** αναλαμβάνει να αμυνθεί ενάντια σε μια ενεργή επίθεση σε ένα περιβάλλον άσκησης και δοκιμής κυβερνοασφάλειας. Η μπλε ομάδα είναι υπεύθυνη για τον εντοπισμό και την επιδιόρθωση πιθανών τρωτών σημείων που μπορούν να αξιοποιηθεί από την κόκκινη ομάδα.
- Η **λευκή ομάδα (white team)** σχεδιάζει το σενάριο άσκησης και πειράματος, τους στόχους, τους κανόνες και τα κριτήρια αξιολόγησης. Θέτουν ένα σύνολο κανόνων εμπλοκής μεταξύ της κόκκινης και της μπλε ομάδας, δημιουργούν τα τρωτά σημεία του περιβάλλοντος για την επιδιόρθωση και την εκμετάλλευση και μερικές φορές ενεργούν ως εκπαιδευτές για να δώσουν συμβουλές στις συμμετέχουσες ομάδες.
- Η **πράσινη ομάδα (green team)** είναι υπεύθυνη για την ανάπτυξη, παρακολούθηση

και συντήρηση της υποδομής άσκησης που σχεδιάστηκε από τη λευκή ομάδα. Είναι επίσης υπεύθυνοι για τη διόρθωση σφαλμάτων που μπορεί να προκύψουν στην υποδομή κατά τη διάρκεια εκτέλεσης άσκησης.

- Τα μέλη της **πορτοκαλί ομάδας (orange team)** Παναθέτουν διαφορετικές τεχνικές εργασίες στα μέλη της μπλε ομάδας κατά τη διάρκεια της άσκησης. Τα μέλη της μπλε ομάδας μπορούν να κερδίσουν πόντους εάν είναι σε θέση να ολοκληρώσουν με επιτυχία τις εργασίες.
- Η **μωβ ομάδα (purple team)** εκτελεί το ρόλο επικοινωνίας μεταξύ πολλαπλών ομάδων ασκήσεων. Μέρος των αρμοδιοτήτων της είναι η ανταλλαγή πληροφοριών με σκοπό την αύξηση της αποτελεσματικότητας της άσκησης. Αυτό έχει σαν αποτέλεσμα την ενίσχυση ενισχύει της αποτελεσματικότητας της κόκκινης ομάδας όσον αφορά την επίθεση στο περιβάλλον ασκήσεων και αυξάνει την ικανότητα της μπλε ομάδας στην υπεράσπιση του δικτύου.
- Τα μέλη της **κίτρινης ομάδας (yellow team)** προσομοιώνουν τη συμπεριφορά των κανονικών χρηστών που χρησιμοποιούν την υποδομή που δημιουργείται από την πράσινη ομάδα. Εκτελούν εργασίες όπως η δημιουργία νόμιμης κίνησης στο δίκτυο η οποία μπορεί να χρησιμοποιηθεί από την κόκκινη και την μπλε ομάδα στην επίθεση και την άμυνα αντίστοιχα.

Από τις προαναφερθείσες ομάδες, τις κυριότερες αποτελούν οι κόκκινη, άσπρη, μπλε και πράσινη. Οι πορτοκαλί, μωβ και κίτρινες ομάδες περιλαμβάνονται σε ορισμένες, πιο ειδικές, ασκήσεις κυβερνοασφάλειας. Οι ονομασίες κόκκινη και μπλε ομάδα προέρχονται από στρατιωτικές ασκήσεις, στις οποίες η μπλε ομάδα είναι υπεύθυνη για την προστασία ενός “περιουσιακού στοιχείου”, ενώ ο ρόλος της κόκκινης ομάδας είναι να αμφισβητεί κατ’ επανάληψη το σχέδιο άμυνας της μπλε ομάδας. Το αποτέλεσμα θα πρέπει να είναι η ολοκληρωμένη κατανόηση των μηχανισμών / πρωτοκόλλων ασφαλείας του “περιουσιακού στοιχείου”, των αδυναμιών τους καθώς και η αποτελεσματική ανταπόκριση σε αυτές. Σε ορισμένες περιπτώσεις, μια λευκή ομάδα είναι υπεύθυνη για την επίβλεψη ολόκληρης της άσκησης, το συντονισμό μεταξύ των ομάδων και την ανάλυση της απόδοσής τους [19]. Η εκπαίδευση λαμβάνει χώρα συνήθως σε ένα ελεγχόμενο περιβάλλον το οποίο ονομάζεται Cyber Range.

2.3 Τι είναι τα Cyber Ranges

Όπως προαναφέρθηκε, τα τελευταία χρόνια, υπάρχει αυξανόμενη ζήτηση για ειδικούς στην κυβερνοασφάλεια και η ζήτηση αυτή φαίνεται ότι θα συνεχίσει να αυξάνεται. Η άσκηση δοκιμών ασφαλείας στα συστήματα παραγωγής είναι αδύνατη, ως εκ τούτου πολλοί οργανισμοί ενδιαφέρονται να εκπαιδεύσουν το προσωπικό ασφαλείας στα λεγόμενα Cyber Ranges [20].

Τα Cyber Ranges έχουν τη δυνατότητα να καλύψουν αυτό το κενό, αφού συνδυάζουν την πρακτική εμπειρία με τη θεωρητική κατάρτιση [5]. Ειδικότερα, πρόκειται για ένα προκαθορισμένο εικονικό περιβάλλον που επιτρέπει στους εκπαιδευόμενους να προσομοιώνουν ρεαλιστικά σενάρια επίθεσης και άμυνας, σε ένα πλαίσιο που μιμείται το πραγματικό επιχειρησιακό περιβάλλον [19] [6]. Ως εκ τούτου, οι συμμετέχοντες μπορούν να αλληλοεπιδρούν με μια εικονική υποδομή χωρίς οι ενέργειές τους να μπορούν να επηρεάσουν το πραγματικό επιχειρησιακό περιβάλλον [7]. Τα Cyber Ranges χρησιμοποιούνται όχι μόνο για την εκπαίδευση στον κυβερνοχώρο, αλλά και για την ανάπτυξη της τεχνολογίας στον κυβερνοχώρο, την εγκληματολογική ανάλυση και άλλα θέματα που σχετίζονται γενικότερα με τον κυβερνοχώρο [7]. Ένας πρόσθετος λόγος για τη χρήση ενός Cyber Range, είναι το γεγονός ότι κατά την προσομοίωση απειλών και επιθέσεων από την κόκκινη ομάδα, μπορεί να δημιουργηθούν ψευδείς συναγερμοί, οι οποίοι είναι δύσκολο να ξεχωρίσουν από τις πραγματικές επιθέσεις [21].

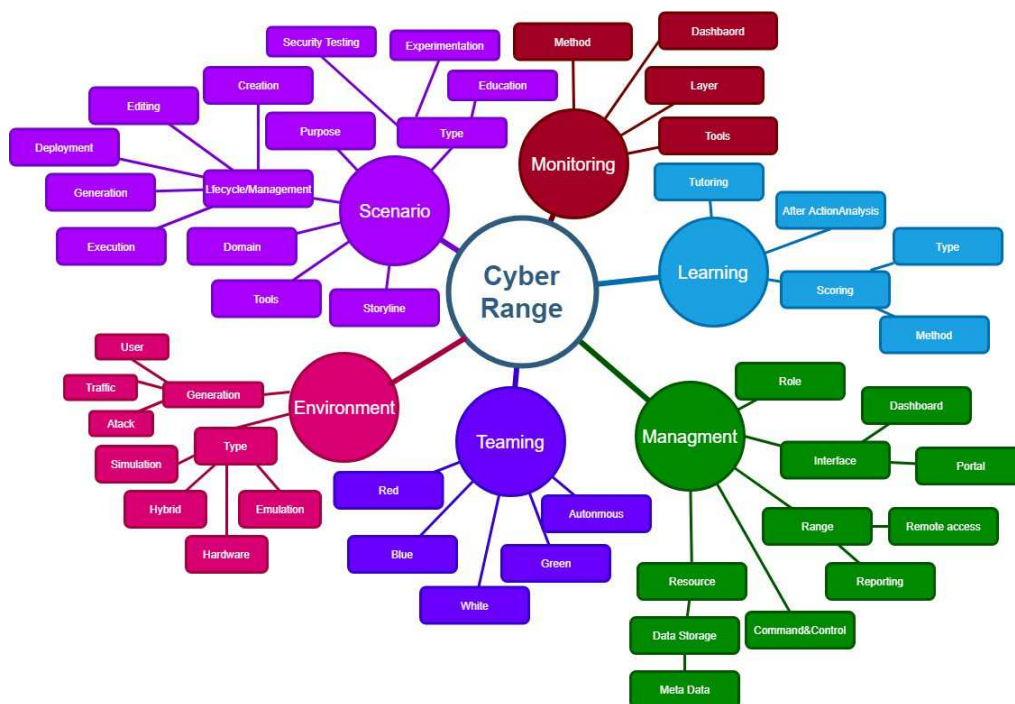
Τα Cyber Ranges περιλαμβάνουν δραστηριότητες όπως η ανακάλυψη τρωτών σημείων και η ενίσχυση των υφιστάμενων συστημάτων, η αξιολόγηση της ασφαλείας ενός νέου στοιχείου, η διδασκαλία ασφαλών πρακτικών προγραμματισμού, η εκτέλεση απόκρισης σε περιστατικά καθώς επίσης και μια πλατφόρμα για δραστηριότητες του τύπου “μπλε εναντίον κόκκινης ομάδας” [20].

Το περιβάλλον των Cyber Ranges, ως προς την ανάπτυξή του, μπορεί να κατηγοριοποιηθεί σε τρεις κύριους τύπους, την προσομοίωση, την εξομοίωση και τον υβριδικό τύπο [5]. Ειδικότερα, μια προσομοίωση περιλαμβάνει τη χρήση ενός μοντέλου, μιας εικονικής παρουσίας προκειμένου να αναδημιουργηθεί ένα πολύπλοκο περιβάλλον δικτύου με βάση τη συμπεριφορά των πραγματικών στοιχείων δικτύου. Η δε εξομοίωση πραγματοποιείται όταν το Cyber Range εκτελείται στην αποκλειστική φυσική υποδομή δικτύου. Ο υβριδικός τύπος προκύπτει από έναν προσαρμοσμένο συνδυασμό από τους δύο παραπάνω τύπους.

Οι Yamin, Katt και Gkioulos [18], μέσα από τη βιβλιογραφική τους ανασκόπηση, προτείνουν μια ενημερωμένη ταξινόμηση των Cyber Ranges σε ενότητες, όπως αυτή φαίνεται στην εικόνα 1. Πιο συγκεκριμένα, η ταξινόμηση περιλαμβάνει τις εξής ενότητες:

- **Σενάρια ασφάλειας (Scenarios)** και διαχείριση του κύκλου ζωής τους στον κυβερνοχώρο (δημιουργία, παραγωγή, επεξεργασία, ανάπτυξη και εκτέλεση).
- **Έλεγχος (Monitoring)** των περιβαλλόντων άσκησης, όπως είναι τα Cyber ranges, η οποία περιέχει μεθόδους και εργαλεία που χρησιμοποιούνται για την επίτευξη του ελέγχου.
- **Εκμάθηση (Learning)** η οποία περιλαμβάνει τη διδασκαλία, το μηχανισμό ανάλυσης των δράσεων και τις τεχνικές βαθμολόγησης που υπάρχουν.
- **Διαχείριση (Management)** ήτοι οι ρόλοι, οι διεπαφές, η διαχείριση εύρους, οι εντολές και ο έλεγχος, καθώς και η διαχείριση πόρων εντός των Cyber Ranges.
- **Ομάδες (Teaming)** περιλαμβάνει τα είδη των ομάδων, τα οποία αναφέρονται στο προηγούμενο κεφάλαιο.
- **Περιβάλλον (Environment)** που περιλαμβάνει τον τύπο περιβάλλοντος εκτέλεσης σεναρίου και διαφορετικά εργαλεία δημιουργίας συμβάντων που χρησιμοποιούνται σε περιβάλλοντα σεναρίων.

Στο Σχήμα 2.1 παρουσιάζεται σχηματικά μια αρχική ταξινόμηση για την κατηγοριοποίηση των Cyber Ranges όπως αυτή προέκυψε από την αρχική επισκόπηση της βιβλιογραφίας στην δημοσίευση των Yamin et. al.[18]



Σχήμα 2.1: Ταξινόμηση των Cyber Ranges.

Πηγή : [18]

Μια άλλη κατηγοριοποίηση των Cyber Ranges σχετίζεται με τον χειριστή τους, ήτοι τους υπεύθυνους για την ανάπτυξη των Cyber Ranges, και άλλων παρόμοιων δοκιμαστικών περιβαλόντων, όπως τα πανεπιστήμια, οι κυβερνητικές υπηρεσίες, τα στρατιωτικά ερευνητικά κέντρα, οι διεθνείς οργανισμοί και οι θυγατρικές αυτών [5].

2.4 Approaches των Cyber Ranges

Πρόσφατα, η προσοχή στα Cyber Ranges έχει αυξηθεί και πλέον χρησιμοποιούνται σε τρεις βασικούς τομείς: στην έρευνα, στην εκπαίδευση και σε διαγωνισμούς για την ασφάλεια στον κυβερνοχώρο [7]. Στον τομέα της έρευνας αξιοποιούνται δοκιμάζοντας υλοποιήσεις διαφόρων μεθόδων, εργαλείων, δομικών στοιχείων και συστημάτων, στον τομέα της εκπαίδευσης πραγματοποιούνται σε ακαδημαϊκούς χώρους εξειδικευμένα μαθήματα ασφάλειας και χορηγούνται πιστοποιήσεις κυβερνοασφάλειας, ενώ οι διαγωνισμοί για την ασφάλεια στον κυβερνοχώρο αφορούν την εκπαίδευση σε θέματα ασφάλειας μέσω ασκήσεων όπως για παράδειγμα το Capture the Flag ή οι Ασκήσεις Κυβερνοάμυνας [7].

Τα Κέντρα Επιχειρήσεων Ασφαλείας (Security Operations Centers - SOC) παρέχουν μια ολιστική άποψη των λειτουργιών ασφαλείας μιας εταιρείας. Σύμφωνα με την έρευνα των Vielberth et al. [8], οι εταιρείες δεν διαθέτουν επαρκώς ειδικευμένους αναλυτές κυβερνοασφάλειας. Αυτό συμβαίνει είτε διότι είναι δύσκολη η αναζήτηση αρκετά καλά εκπαιδευμένων αναλυτών, είτε επειδή αυτοί που εργάζονται ήδη σε εταιρείες εξαντλούνται καθημερινά όντας σε συνεχή επαγρύπνηση για απειλές, με αποτέλεσμα να αδυνατούν να αναζητήσουν επιπρόσθετη, πιο εξειδικευμένη κατάρτιση. Για το λόγο αυτό, οι Vielberth, Manfred, et al. [8] προτείνουν μια προσέγγιση για την κάλυψη αυτής της απαίτησης, μέσω της δημιουργίας ενός “Digital Twin - Based Cyber Range”, δηλαδή μιας εικονική αναπαράστασης ενός συστήματος, το οποίο δύναται να εξοπλίσει τους πιθανούς αναλυτές με τις απαιτούμενες δεξιότητες. Ωστόσο, εξ όσων γνωρίζουμε, δεν έχει επιχειρηθεί ακόμη η αξιοποίηση αυτής της δυνατότητας για την εκπαίδευση αναλυτών SOC.

2.5 Τι είναι τα CTF (capture the flag)

Η εκπαίδευση στην ασφάλεια των υπολογιστών ενισχύεται με την χρήση πρακτικών διαδραστικών δραστηριοτήτων μάθησης. Το Capture the flag (CTF) έχει εφαρμοστεί με επιτυχία στην εκπαίδευση και λειτουργεί ιδιαίτερα καλά στην εκμάθηση τεχνικών επίθεσης. Το CTF είναι ένας τύπος παιχνιδιού ασφάλειας στον κυβερνοχώρο που περιλαμβάνει τη συλλογή σημαιών με την επίλυση προκλήσεων ασφάλειας. Τα CTF δίνουν σε επαγγελματίες και φοιτητές την ευκαιρία να δοκιμάσουν τις δεξιότητές τους σε θέματα ασφάλειας [22]

Ένας από τους στόχους αυτών των εκδηλώσεων είναι συνήθως για μια ομάδα συμμετεχόντων να υπερασπιστεί έναν host στον οποίο εκτελούνται ευάλωτες υπηρεσίες ενώ ταυτόχρονα να επιτίθεται στους hosts άλλων ομάδων που εκτελούνται οι ίδιες υπηρεσίες (CTF τύπου επίθεσης/άμυνας). Μια άλλη προσέγγιση είναι αυτή της λύσης αυτόνομων προκλήσεων από μια σειρά κατηγοριών, όπως η αντίστροφη μηχανική, η εγκληματολογία και η ασφάλεια ιστού, χωρίς την ανάγκη άμεσης επίθεσης σε άλλες ομάδες (CTF τύπου Jeopardy). Σε κάθε περίπτωση, η επιτυχής εκμετάλλευση μιας ευάλωτης υπηρεσίας ή η επίλυση μιας πρόκλησης αποκαλύπτει μια “σημαία” στον νικητή, η οποία κερδίζει πόντους για την ομάδα όταν αυτή υποβληθεί στον διακομιστή σημαιών των διοργανωτών του CTF. Η υποβολή σημαιών που αφορούν πιο δύσκολες προκλήσεις ανταμείβεται με μεγαλύτερο αριθμό πόντων για την ομάδα και η ομάδα που θα συγκεντρώσει τους περισσότερους πόντους κατά τη διάρκεια του διαγωνισμού ανακηρύσσεται νικήτρια [23].

Οι εφαρμογές των σεναρίων CTF έχουν αποδείξει παιδαγωγική χρησιμότητα όταν χρησιμοποιούνται στην Τριτοβάθμια Εκπαίδευση [22]. Μεταξύ των πιο συχνά αναφερόμενων πλεονεκτημάτων, είναι τα αυξημένα κίνητρα των μαθητών να μάθουν για την κυβερνοασφάλεια, η απόλαυση και η ικανοποίηση του ανταγωνισμού και η βελτιωμένη πρακτική γνώση των θεωρητικών πτυχών της κυβερνοασφάλειας ως αποτέλεσμα της συμμετοχής [23].

Ωστόσο, υπάρχουν πολλά εμπόδια για την εισαγωγή των CTF στο ακαδημαϊκό πρόγραμμα σπουδών [23]. Σύμφωνα με τους Švábenský, Čeleda, Vykopal και Brišáková [24], δεν είναι σαφές πώς οι δεξιότητες που εξασκούνται από αυτές τις δοκιμασίες ταιριάζουν με τα επίσημα προγράμματα σπουδών κυβερνοασφάλειας που ορίζονται από ειδικούς στον τομέα της ασφάλειας. Επιπρόσθετα, η υποδομή που υποστηρίζει ένα CTF είναι συνήθως μεγάλη και πολύπλοκη, ενώ η υπολογιστική ισχύς που απαιτείται για την ομαλή λειτουργία του συνήθως δεν είναι διαθέσιμη για διδακτικούς σκοπούς [23]. Τα CTF απαιτούν επίσης συνεχή επίβλεψη από τους διοργανωτές τους, ώστε να εγγυηθεί η ομαλή διεξαγωγή τους. Τέλος, περιλαμβάνουν αναπόφευκτα επίθεση σε ευάλωτες υπηρεσίες που είναι διαθέσιμες σε ένα δίκτυο, ωστόσο το προσωπικό υποστήριξης πληροφορικής ενός πανεπιστημίου ενδεχομένως να διστάζει να επιτρέψει κακόβουλη κίνηση να περάσει σε οποιοδήποτε δίκτυο ελέγχουν [23]. Παρά τα παραπάνω μειονεκτήματα, το Capture The Flag εξακολουθεί να είναι η πιο δημοφιλής κατηγορία χρήσης των Cyber Ranges στις μέρες μας. Στο επόμενο κεφάλαιο ακολουθούν προσεγγίσεις του Capture The Flag, όπως προκλήσεις Hack The Box και άλλα παιχνίδια επίθεσης/άμυνας.

2.6 CTF Approaches

Όπως προαναφέρθηκε, οι δοκιμασίες Capture the Flag είναι μια δημοφιλής μορφή εκπαίδευσης στον κυβερνοχώρο, όπου οι εκπαιδευόμενοι επιλύουν πρακτικές εργασίες σε ένα ανεπίσημο περιβάλλον που μοιάζει με παιχνίδι. Οι ασκήσεις των CTF περιλαμβάνουν ποικίλες αναθέσεις, όπως η εκμετάλλευση ιστότοπων, το "σπάσιμο" κωδικών πρόσβασης και η παραβίαση μη ασφαλών δικτύων [24]. Στο παρόν κεφάλαιο αναπτύσσονται προσεγγίσεις του Capture The Flag, όπως αυτή του Hack The Box και άλλα παιχνίδια επίθεσης/άμυνας.

Ειδικότερα, το **Hack The Box (HTB)**¹ αποτελεί μια κοινότητα hacking και infosec με περισσότερα από 859.000 μέλη που μαθαίνουν, παίζουν, ανταλλάσσουν ιδέες και μεθοδολογίες.

¹<https://www.hackthebox.com/>

Πρόκειται για μια διαδικτυακή πλατφόρμα εκπαίδευσης στον κυβερνοχώρο που επιτρέπει σε άτομα, επιχειρήσεις, πανεπιστήμια και κάθε είδους οργανισμούς από όλο τον κόσμο να βελτιώσουν τις επιθετικές και αμυντικές τους δεξιότητες ασφάλειας, μέσα από ένα πλήρως παιχνιδοποιημένο και ελκυστικό περιβάλλον μάθησης. Το HTB ενθαρρύνει τους χρήστες να "χακάρουν" την πρώτη του σελίδα, προκειμένου να αποκτήσουν έναν κωδικό πρόσκλησης για εγγραφή, χρησιμοποιώντας παράλληλα ανταγωνιστικούς βαθμολογικούς πίνακες [25]. Το επίπεδο δυσκολίας των ασκήσεων είναι διαβαθμισμένο και κατηγοριοποιημένο έτσι ώστε να υπάρχει η δυνατότητα εξάσκησης συγκεκριμένων ικανοτήτων.

Ένας διασκεδαστικός τρόπος εξάσκησης στην ασφάλεια στο διαδίκτυο αποτελεί το **Try Hack Me**², καθώς παρέχει μία Hands - On εκπαίδευση με τη χρήση ρεαλιστικών σεναρίων. Πιο συγκεκριμένα, το TryHackMe επιτρέπει στους χρήστες να μαθαίνουν τρόπους επίθεσης και άμυνας σε δίκτυα υπολογιστών που χρησιμοποιούνται στη σημερινή εποχή από διάφορους οργανισμούς. Το HackTheBox και το TryHackMe απαιτούν πρόσβαση σε ένα Virtual Private Network με την χρήση προγράμματος όπως το OpenVPN, προκειμένου να εκτελούνται με ασφάλεια τα σενάρια σε ένα απομονωμένο δίκτυο [25].

Μία άλλη προσέγγιση των CTF αποτελεί το **Vulnhub**³, ένας ιστότοπος που παρέχει συστήματα τα οποία είναι σκόπιμα ευάλωτα προς παραβίαση [26]. Στόχος του είναι να παρέχει την υποδομή η οποία θα επιτρέπει την απόκτηση μιας Hands - On εμπειρίας στην ψηφιακή ασφάλεια, στο λογισμικό υπολογιστών και στη διαχείριση δικτύων.

Το δε **CyberDefenders**⁴ είναι μια πλατφόρμα εκπαίδευσης που επικεντρώνεται στην αμυντική πλευρά της ασφάλειας στον κυβερνοχώρο, με στόχο να παρέχει την ευκαιρία στις μπλε ομάδες να εξασκηθούν, να επικυρώσουν τις δεξιότητες που έχουν και να αποκτήσουν περαιτέρω από αυτές.

Τέλος, το **Hackerbot**[22] είναι μια μοναδική προσέγγιση για τη διδασκαλία της ασφάλειας υπολογιστών: οι μαθητές αλληλεπιδρούν με έναν κακόβουλο εισβολέα chatbot, ο οποίος τους προκαλεί να ολοκληρώσουν μια ποικιλία εργασιών ασφαλείας, συμπεριλαμβανομένων αμυντικών και διερευνητικών προκλήσεων. Οι προκλήσεις τυχαioποιούνται χρησιμοποιώντας το SecGen και αναπτύσσονται σε μια υποδομή oVirt. Τα αποτελέσματα της παραπάνω έρευνας ήταν ενθαρρυντικά, βρίσκοντας την προσέγγιση βολική, ελκυστική, διασκεδαστική και διαδραστική.

²<https://tryhackme.com/>

³<https://www.vulnhub.com/>

⁴<https://cyberdefenders.org/>

2.7 Εργαλεία Security Labs

Στο κεφάλαιο αυτό πραγματοποιείται βιβλιογραφική ανασκόπηση των βασικών εργαλείων για Security Labs, Digital Forensics, Decision Support Systems και Threat intelligence.

2.7.1 Intrusion Detection Systems (IDS)

Το **SNORT**⁵ είναι ένα ισχυρό σύστημα ανίχνευσης εισβολής (IDS) ανοιχτού κώδικα και σύστημα πρόληψης εισβολής (IPS) που παρέχει ανάλυση του δικτύου σε πραγματικό χρόνο με καταγραφή πακέτων δεδομένων [27]. Χρησιμοποιεί μια γλώσσα που βασίζεται σε κανόνες και συνδυάζει μεθόδους ανίχνευσης ανωμαλιών, πρωτοκόλλου και υπογραφής για τον εντοπισμό δυνητικά κακόβουλης δραστηριότητας. Το Snort έχει τρεις κύριες χρήσεις: ως ανιχνευτής πακέτων όπως το tcpdump, ως καταγραφέας πακέτων που είναι χρήσιμος για το network traffic debugging ή μπορεί να χρησιμοποιηθεί και ως πλήρες σύστημα πρόληψης εισβολής δικτύου.

Ένα άλλο εργαλείο ανίχνευσης εισβολής (IDS) είναι το **Suricata**⁶. Το Suricata είναι ένας κορυφαίος ανεξάρτητος ανιχνευτής απειλών ανοιχτού κώδικα, ο οποίος συμπεριλαμβάνει την ανίχνευση εισβολής (IDS), την πρόληψη εισβολής (IPS), την παρακολούθηση ασφάλειας δικτύου (NSM) και την επεξεργασία PCAP, ώστε να μπορεί να εντοπίσει, να σταματήσει και να αξιολογήσει γρήγορα ακόμη και τις πιο εξελιγμένες επιθέσεις.

2.7.2 Εργαλεία Ανίχνευσης Ευπαθειών

Για τον εντοπισμό των υφιστάμενων αδυναμιών ασφαλείας, υπάρχει μια ποικιλία προσεγγίσεων μεταξύ των οποίων είναι το λειτουργικό σύστημα **Kali Linux**⁷. Το Kali Linux είναι ένα από τα καλύτερα λειτουργικά συστήματα ανοιχτού κώδικα, που περιέχει ένα σύνολο εργαλείων διαιρούμενο σε κατηγορίες και παρέχει ότι εργαλεία χρειάζεται για εργασίες όπως Penetration Testing, Security Research, Computer Forensics και Reverse Engineering [28]. Είναι το αποκορύφωμα των ετών τελειοποίησης και το αποτέλεσμα μιας συνεχούς εξέλιξης της πλατφόρμας, από το WHoppiX στο WHAX, στο BackTrack, και τώρα σε ένα πλήρες πλαίσιο Penetration Testing, αξιοποιώντας πολλά χαρακτηριστικά του Debian GNU/Linux και της

⁵<https://www.snort.org/>

⁶<https://suricata.io/>

⁷<https://www.kali.org/>

κοινότητας ανοιχτού κώδικα παγκοσμίως [28]. Το Kali Linux δεν έχει κατασκευαστεί για να είναι μια απλή συλλογή εργαλείων, αλλά ένα ευέλικτο πλαίσιο που οι επαγγελματίες, οι μαθητές και οι ερασιτέχνες μπορούν να προσαρμόσουν για να ταιριάζει στις συγκεκριμένες ανάγκες τους.

Το **CALDERA**⁸ είναι μια πλατφόρμα κυβερνοασφάλειας που έχει σχεδιαστεί για να αυτοματοποιεί την εξομοίωση των αντιπάλων, να βοηθά τις κόκκινες ομάδες και να αυτοματοποιεί την απόκριση σε περιστατικά. Είναι χτισμένο στο πλαίσιο MITRE ATT&CK και είναι ένα ενεργό ερευνητικό έργο το οποίο είναι μια ανοιχτή βάση γνώσης τακτικών και τεχνικών αντιπάλου που ενημερώνεται συνεχώς με βάση τις πραγματικές παρατηρήσεις. Το πλαίσιο αποτελείται από δύο συνιστώσες: το κεντρικό σύστημα, στο οποίο περιλαμβάνεται ένας ασύγχρονος διακομιστής εντολών και ελέγχου με REST API και περιβάλλον εργασίας web, και τις προσθήκες, οι οποίες επεκτείνουν τις βασικές δυνατότητες πλαισίου και παρέχουν πρόσθετες λειτουργίες [19]. Όλες οι επιθέσεις στο Caldera λαμβάνονται από τον πίνακα MITRE ATT&CK και πληροφορίες σχετικά με τις διαδικασίες βρίσκονται στην τεκμηρίωση του MITRE. Οι διαδικασίες επίθεσης μπορούν να επιλεγούν από τη βιβλιοθήκη της και να συνδυαστούν μαζί για να δημιουργήσουν προσαρμοσμένες επιθέσεις πολλαπλών διαδικασιών. Σε γενικές γραμμές, το Caldera παρέχει φιλικό προς το χρήστη περιβάλλον εργασίας και λειτουργικότητα για τη σύνταξη νέων επιθέσεων από υπάρχουσες διαδικασίες.

Το **Atomic Red Team**⁹ είναι μια βιβλιοθήκη εξομοίωσης απειλής δοκιμών ασφαλείας που μπορούν να εκτελεστούν γρήγορα από τις ομάδες ασφαλείας. Τα σενάρια επίθεσης μπορούν να εκτελούνται χρησιμοποιώντας τη γραμμή εντολών, το PowerShell και το Shell. Αυτή είναι συμβατή με όλα τα γνωστά λειτουργικά συστήματα. Το Atomic Red Team υποστηρίζει πολλαπλές τεχνικές για την επίτευξη Persistence, Privilege Escalation, Defense Evasion, Credential Access. Επιπλέον, το Atomic Red Team χρησιμοποιεί εργαλεία τρίτων, όπως το mimikatz για την εκτέλεση τεχνικής αρπαγής διαπιστευτηρίων. Οι περισσότερες διαδικασίες δεν ανιχνεύονται από εργαλεία προστασίας από ιούς. Το Atomic Red Team στερείται λειτουργιών καταγραφής και εκκαθάρισης. Η τεκμηρίωση παρέχεται μόνο ως σχόλια στις δέσμες ενεργειών των διαδικασιών. Ένας από τους κύριους στόχους του Atomic Red Team είναι να επιτρέψει στον χειριστή να εκτελεί διαδικασίες γρήγορα χωρίς να απαιτείται οποιαδήποτε εγκατάσταση λογισμικού, ωστόσο μπορεί να απαιτήσει γνώσεις κυβερνοασφάλειας για να χρησιμοποιηθεί αποτελεσματικά. [19].

⁸<https://caldera.mitre.org/>

⁹<https://atomicredteam.io/>

Το **Infection Monkey**¹⁰ είναι ένας εξομοιωτής απειλών που χρησιμοποιείται για τη δοκιμή και την αξιολόγηση των αμυνών ενάντια στις πλευρικές τακτικές μετακίνησης και ανακάλυψης (κυρίως αρχική πρόσβαση). Το Infection Monkey έχει λειτουργία CnC και απαιτεί την εγκατάσταση ενός RAT στα τελικά σημεία. Δεδομένου ότι τα εργαλεία προστασίας από ιούς αναγνωρίζουν το RAT που χρησιμοποιείται από το Infection Monkey ως απειλή, απαιτείται να απενεργοποιηθούν τα εργαλεία προστασίας από ιούς για να λειτουργήσει σωστά. Το Infection Monkey μπορεί να εγκατασταθεί σε οποιοδήποτε λειτουργικό σύστημα ενώ το RAT μπορεί να εγκατασταθεί σε λειτουργικά συστήματα Windows και Linux (αλλά όχι σε MAC OS). Κατά την εκτέλεση υπάρχει πλήρης αναφορά για μηχανές που μολύνθηκαν κατά τη διαδικασία πλευρικής κίνησης. Οι τεχνικές που χρησιμοποιούνται από το Infection Monkey προέρχονται από πραγματικά σενάρια, καθιστώντας το κοντά στη συμπεριφορά ενός πραγματικού εισβολέα όταν πρόκειται για πλευρική κίνηση. Συγκεκριμένα, οι περισσότερες διαδικασίες, εάν εκτελούνται ξεχωριστά χωρίς το RAT, θα παρέμεναν απαρατήρητες από τις Antivirus λύσεις. Η πρόοδος κάθε εκτέλεσης επίθεσης καταγράφεται και παρέχεται λεπτομερής ανασκόπηση των αποτελεσμάτων.

2.7.3 Firewalls

Το **τείχος προστασίας (Firewall)** είναι μια συσκευή ασφαλείας δικτύου που παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση του δικτύου και αποφασίζει εάν θα επιτρέψει ή θα αποκλείσει συγκεκριμένη κίνηση με βάση ένα καθορισμένο σύνολο κανόνων ασφαλείας. Τα τείχη προστασίας αποτελούν την πρώτη γραμμή άμυνας στην ασφάλεια δικτύου για περισσότερα από 25 χρόνια, καθώς δημιουργούν ένα εμπόδιο μεταξύ ασφαλών, αξιόπιστων και ελεγχόμενων εσωτερικών δικτύων και των μη αξιόπιστων εξωτερικών δικτύων, όπως είναι το Διαδίκτυο. Ένα τείχος προστασίας μπορεί να είναι software, hardware ή και τα δύο. Υπάρχουν επίσης πολλοί τύποι firewall, όπως για παράδειγμα Proxy firewall, Stateful inspection firewall, Unified threat management (UTM) firewall, Next-generation firewall (NGFW), Threat-focused NGFW και Virtual firewall.

Ειδικότερα, τα **Checkpoint Gateways**¹¹, εντάσσονται στην κατηγορία Next Generation Firewalls και αποτελούν λύση της Checkpoint. Είναι σχεδιασμένα έτσι ώστε να υποστηρίζουν την τεχνολογία του Sandblast Zero Day Protection, ενώ το τελευταίο διάστημα προσφέρονται και με διαχειριστικό περιβάλλον στο Cloud. Εκτός του Zero Day Protection, ενσωματώνει

¹⁰<https://www.akamai.com/infectionmonkey>

¹¹<https://www.checkpoint.com/quantum/next-generation-firewall/>

τεχνολογίες όπως IPS/IDS, Antivirus, Data Loss Prevention και VPN.

Παράλληλα, το **Cisco Adaptive Security Appliance (ASA)**¹², είναι η λύση που προσφέρει η Cisco στην κατηγορία των Firewalls, για οποιοδήποτε περιβάλλον καταναμεμημένου δικτύου. Επιπρόσθετα, ενσωματώνεται με άλλες τεχνολογίες ασφάλειας όπως IPS, VPN, για να παρέχει ολοκληρωμένες λύσεις που καλύπτουν συνεχώς εξελισσόμενες ανάγκες ασφαλείας.

Έχοντας υψηλή απόδοση προστασίας από απειλές με αυτοματοποιημένη ορατότητα για τη διακοπή επιθέσεων, τα **FortiGate NGFW**¹³, που αποτελούν λύση της Fortinet, επιτρέπουν δικτύωση με γνώμονα την ασφάλεια και κατέχουν υψηλές δυνατότητες ασφάλειας, όπως το σύστημα πρόληψης εισβολής (IPS), το φιλτράρισμα ιστού, την επιθεώρηση SSL, και την αυτοματοποιημένη προστασία από απειλές. Το FortiGate NGFW επιθεωρεί την κυκλοφορία καθώς εισέρχεται και εξέρχεται από το δίκτυο με απaráμιλλη ταχύτητα, κλίμακα και απόδοση, αποτρέποντας από ransomware έως επιθέσεις DDoS.

Το **pfSense project**¹⁴ είναι μια δωρεάν διανομή τείχους προστασίας, που βασίζεται στο λειτουργικό σύστημα FreeBSD με προσαρμοσμένο πυρήνα και περιλαμβάνει πακέτα ελεύθερου λογισμικού τρίτων για πρόσθετη λειτουργικότητα. Το λογισμικό pfSense, με τη βοήθεια του συστήματος πακέτων, είναι σε θέση να παρέχει την ίδια ή ακόμα και μεγαλύτερη λειτουργικότητα από τα κοινά εμπορικά τείχη προστασίας, χωρίς κανέναν από τους τεχνικούς περιορισμούς. Έχει αντικαταστήσει με επιτυχία κάθε μεγάλο εμπορικό τείχος προστασίας, σε πολλές εγκαταστάσεις σε όλο τον κόσμο ενώ Φιλοξενείται και αναπτύσσεται από τη Rubicon Communications, LLC (Netgate).

2.7.4 Security Information and Event Management (SIEM)

Κάθε Security Operations Center, διαθέτει ένα σύστημα SIEM (Security Information and Event Management), το οποίο παρέχει το πραγματικό σημείο αλληλεπίδρασης με τον εκπαιδευόμενο. Το SIEM είναι το σύστημα για το οποίο εκπαιδεύεται ένας αναλυτής και ιδανικά είναι επίσης σε πρακτική χρήση στον οργανισμό του εκπαιδευόμενου [8]. Αυτό διασφαλίζει ότι ο εκπαιδευόμενος μαθαίνει να εργάζεται σε ένα σύστημα που είναι όσο το δυνατόν πιο κοντά στο πραγματικό SIEM ή ακόμα και πανομοιότυπο με αυτό [29]. Τα δεδομένα καταγραφής των εταιρικών συστημάτων τροφοδοτούνται στο SIEM. Στο πρώτο βήμα, ο εκπαιδευόμενος

¹²<https://www.cisco.com/site/us/en/products/security/firewalls/index.html>

¹³<https://www.fortinet.com/products/next-generation-firewall>

¹⁴<https://www.pfsense.org/>

αλληλεπιδρά με το SIEM για να αναλύσει και να εντοπίσει χειροκίνητα τις προσομοιωμένες επιθέσεις με βάση τα διαθέσιμα δεδομένα. Στο επόμενο βήμα, ο εκπαιδευόμενος μπορεί να το χρησιμοποιήσει για να δημιουργήσει κανόνες συσχέτισης στο SIEM, οι οποίοι εντοπίζουν αυτόματα τις επιθέσεις [8].

Το IBM Security QRadar Security Information and Event Management (SIEM)¹⁵ βοηθά τις ομάδες ασφαλείας να εντοπίζουν, να ιεραρχούν και να ανταποκρίνονται σε απειλές σε μια επιχείρηση. Αναλύει και συγκεντρώνει αυτόματα δεδομένα καταγραφής και ροών από χιλιάδες συσκευές και εφαρμογές σε όλο το δίκτυο, παρέχοντας μεμονωμένες ειδοποιήσεις για την επιτάχυνση της ανάλυσης και αποκατάστασης περιστατικών.

Το ELK Stack¹⁶ είναι ένα δημοφιλές εργαλείο ανοιχτού κώδικα για την ανάλυση των καταγραφών. Παρέχει μια ολοκληρωμένη προβολή των κρίσιμων δεδομένων ασφαλείας σε μια ενιαία πλατφόρμα. Το ELK είναι ένα αρκτικόλεξο που χρησιμοποιείται για να περιγράψει μια στοίβα που αποτελείται από τρία δημοφιλή έργα ανοιχτού κώδικα: Elasticsearch, Logstash και Kibana. Εντοπίζεται και ως Elasticsearch και παρέχει τη δυνατότητα συγκέντρωσης αρχείων καταγραφής από όλα τα συστήματα και τις εφαρμογές, ανάλυσης αυτών και δημιουργίας απεικονίσεων για παρακολούθηση εφαρμογών και υποδομών, ταχύτερη αντιμετώπιση προβλημάτων και πολλά άλλα.

Το Splunk SIEM¹⁷ είναι μια προηγμένη πλατφόρμα ασφαλείας σε κλίμακα που μπορεί να παρακολουθεί, να ανιχνεύει, να ερευνά και να ανταποκρίνεται σε απειλές με streaming, cloud-based security analytics [30]. Το Splunk SIEM χρησιμοποιείται για τη συλλογή ομοιογενών αλλά και ετερογενών καταγραφών από διάφορες συσκευές. Οι διάφορες δυνατότητες του Splunk είναι οι εξής: Συλλογή και συγκέντρωση συμβάντων, μορφοποίηση συμβάντων, συσχέτιση γεγονότων, Machine Learning [30].

Το OpenText ArcSight¹⁸ είναι ένα προϊόν ασφαλείας, το οποίο παρέχει αναλυτικά στοιχεία δεδομένων για τη διαχείριση πληροφοριών ασφαλείας. Το ArcSight έχει σχεδιαστεί για να βοηθά τους πελάτες να εντοπίζουν και να ιεραρχούν τις απειλές ασφαλείας, να οργανώνουν και να παρακολουθούν δραστηριότητες αντιμετώπισης περιστατικών και να απλοποιούν τις δραστηριότητες ελέγχου και συμμόρφωσης.

¹⁵<https://www.ibm.com/qradar>

¹⁶<https://www.elastic.co/security/siem>

¹⁷<https://www.splunk.com/>

¹⁸<https://www.opentext.com/products/arcsight-enterprise-security-manager>

2.7.5 Machine Learning & Network Flows

Ο όρος Machine learning (μηχανική μάθηση) αντιπροσωπεύει μια συλλογή μεθόδων για την ανακάλυψη της γνώσης αναζητώντας μοτίβα. Η μηχανική μάθηση βελτιώνει τη βάση γνώσεων μαθαίνοντας από την εμπειρία. Οι βασικοί τύποι μάθησης είναι η ταξινόμηση των εισροών σε εξόδους με ετικέτα, η ομαδοποίηση εισόδων σε συμπλέγματα, η συσχέτιση των χαρακτηριστικών και η πρόβλεψη ενός αποτελέσματος [31]. Οι εφαρμογές μηχανικής μάθησης απαιτούν τη συλλογή συνόλων δεδομένων εκπαίδευσης και δοκιμών και εξαρτώνται από αλγορίθμους για εξαγωγή δυνατοτήτων, επιλογή δυνατοτήτων και μάθηση. Αρχικά, το σύστημα εκπαιδεύεται χρησιμοποιώντας παραδείγματα δεδομένων για την εκμάθηση συγκεκριμένων συσχετισμών δεδομένων. Στη συνέχεια, το σύστημα αναπτύσσεται σε παρόμοιο περιβάλλον όπου χρησιμοποιούνται δεδομένα δοκιμών για ταξινόμηση.

Οι προσεγγίσεις μηχανικής μάθησης σε εφαρμογές NetFlow περιλαμβάνουν την ταξινόμηση κυκλοφορίας, την ανίχνευση ανωμαλιών και την ευαισθητοποίηση σχετικά με την ασφάλεια. Τα Network flows υποστηρίζονται από ένα ευρύ φάσμα προϊόντων, συμπεριλαμβανομένου του Cisco NetFlow. Ως Network flow ορίζεται μια μονόπλευρη ή αμφίδρομη ακολουθία πακέτων μεταξύ δύο τελικών σημείων (από διακομιστή σε υπολογιστή-πελάτη ή από υπολογιστή-πελάτη σε διακομιστή) με ορισμένα κοινά χαρακτηριστικά [31]. Οι πρόσφατες ερευνητικές προσεγγίσεις, ωστόσο, έχουν επικεντρωθεί περισσότερο στην ανάλυση ασφάλειας δικτύου με στόχο τον εντοπισμό ανώμαλων δραστηριοτήτων που οι παραδοσιακές υποδομές ασφαλείας, όπως τα συστήματα ανίχνευσης εισβολής (IDS), τα τείχη προστασίας και τα εργαλεία προστασίας από ιούς, δεν μπορούν να χειριστούν.

2.7.6 Λύσεις Εικονικοποίησης (Virtualization)

Στους υπολογιστές, η εικονικοποίηση (Virtualization) είναι η πράξη δημιουργίας μιας εικονικής (και όχι πραγματικής) έκδοσης ενός αντικειμένου, και συγκεκριμένα των εικονικών πλατφορμών υλικού υπολογιστών, συσκευών αποθήκευσης και πόρων δικτύου υπολογιστών. Το Network Virtualization αναφέρεται στην αφαίρεση πόρων δικτύου που παραδοσιακά παραδίδονταν από υλικό και αντικατάσταση αυτών με λογισμικό. Μπορεί να συνδυάσει πολλά φυσικά δίκτυα σε ένα εικονικό δίκτυο που βασίζεται σε λογισμικό ή μπορεί να διαιρέσει ένα φυσικό δίκτυο σε ξεχωριστά, ανεξάρτητα εικονικά δίκτυα.

Το VMWare ESXi¹⁹ είναι μια πλατφόρμα εικονικοποίησης υποδομής, η οποία παρέχει ένα περιβάλλον εικονικών μηχανών (VMs) για την εκτέλεση πολλαπλών λειτουργικών συστημάτων σε έναν φυσικό υπολογιστή. Κατασκευασμένο για τη διαχείριση ευέλικτων και αξιόπιστων επιχειρηματικών περιβαλλόντων, το ESXi παρέχει υψηλή απόδοση, ασφάλεια και εύκολη διαχείριση. Με την ενσωμάτωση προηγμένων δυνατοτήτων όπως το vMotion και το High Availability, το ESXi επιτρέπει τη δυναμική μετακίνηση εργασιών από έναν υπολογιστή σε έναν άλλο χωρίς διακοπή λειτουργίας, προσφέροντας έτσι υψηλό επίπεδο διαθεσιμότητας και επιχειρησιακής αξιοπιστίας.

Το Oracle VM VirtualBox²⁰ είναι μια εφαρμογή εικονικοποίησης πολλαπλών πλατφορμών. Εγκαθίσταται σε υπάρχοντες υπολογιστές που βασίζονται σε Intel ή AMD, είτε χρησιμοποιούν λειτουργικά συστήματα Windows, Mac OS X, Linux ή Oracle Solaris (OS). Επίσης, επεκτείνει τις δυνατότητες του υπάρχοντος υπολογιστή ώστε να μπορεί να τρέχει ταυτόχρονα πολλαπλά λειτουργικά συστήματα, μέσα σε πολλαπλές εικονικές μηχανές (virtual machines). Μπορούν να εγκατασταθούν πολλές εικονικές μηχανές μαζί, με μοναδικούς περιορισμούς το χώρο στο δίσκο και τη μνήμη του υπολογιστή. Οι τεχνικές και οι δυνατότητες που παρέχει το Oracle VM VirtualBox είναι χρήσιμες στα ακόλουθα σενάρια: εκτέλεση πολλαπλών λειτουργικών συστημάτων ταυτόχρονα, ευκολότερες εγκαταστάσεις λογισμικού, δοκιμές και αποκατάσταση από καταστροφές, ενοποίηση υποδομής.

Το Proxmox Virtual Environment²¹ είναι μια πλήρης πλατφόρμα διαχείρισης διακομιστή ανοιχτού κώδικα για εταιρική εικονικοποίηση. Ενσωματώνει KVM hypervisor και LXC, software-defined storage και λειτουργίες δικτύωσης σε μια ενιαία πλατφόρμα. Η ενσωματωμένη διεπαφή χρήστη που βασίζεται στον ιστό, καθιστά εύκολη τη διαχείριση των Virtual Machines.

2.7.7 Digital Forensics

Ο κλάδος της Ψηφιακής Εγκληματολογίας (Digital Forensics) είναι κλάδος της παραδοσιακής εγκληματολογικής επιστήμης, ο οποίος στοχεύει στην αποκάλυψη και ερμηνεία ηλεκτρονικών δεδομένων [32]. Οι επαγγελματίες του εν λόγω κλάδου ασχολούνται με συγκεκριμένα βήματα της ψηφιακής εγκληματολογικής έρευνας, ήτοι την αναγνώριση, τη συλλογή, την ανάκτηση, την ανάλυση και τη διατήρηση ψηφιακών στοιχείων, που βρίσκονται σε διάφορους τύπους ηλεκτρονικών συσκευών [33]. Επιπρόσθετα, η έρευνα πρέπει να εκτελείται χρησιμοποιώντας

¹⁹<https://www.vmware.com/products/cloud-infrastructure/esxi-and-esxr>

²⁰<https://www.virtualbox.org/>

²¹<https://www.proxmox.com/en/>

επικυρωμένα εργαλεία και επιστημονικά αποδεδειγμένη μεθοδολογία, η οποία αναπτύσσεται και επικυρώνεται συνεχώς με τη χρήση νέων εργαλείων, προκειμένου να συμβαδίζει με τις εξελίξεις και να εγγυάται την ακριβή και έγκαιρη εξαγωγή δεδομένων [34]. Σύμφωνα με τους [5], η ψηφιακή εγκληματολογία διδάσκεται ως μάθημα σε πολλές σχολές τεχνολογίας και πληροφοριών, χρησιμοποιώντας ως πλατφόρμα τα Cyber Ranges.

2.7.8 Decision support systems

Λόγω του σημαντικού αριθμού αλγορίθμων και παραμέτρων για την ανάλυση δεδομένων, οι αποφάσεις που βασίζονται στη διαίσθηση δεν μπορούν να οδηγήσουν σε βέλτιστες λύσεις [35]. Κατά συνέπεια, η χρήση τεχνικών εξόρυξης δεδομένων κρίνεται απαραίτητη. Ένα σύστημα υποστήριξης αποφάσεων (Decision support system) είναι ένα πληροφοριακό σύστημα που βοηθά σε δραστηριότητες λήψης αποφάσεων που απαιτούν κρίση καθώς και μια σειρά ενεργειών²². Συγκεκριμένα, μέσω αυτού αναλύονται όγκοι μη δομημένων δεδομένων και πληροφορίες που μπορούν να βοηθήσουν στην επίλυση προβλημάτων και στη λήψη αποφάσεων.

Τα τρία κύρια στοιχεία ενός Decision support system είναι: α) το σύστημα διαχείρισης μοντέλων, το οποίο αποθηκεύει μοντέλα που μπορούν να χρησιμοποιήσουν οι διαχειριστές στη λήψη των αποφάσεών τους β) τη διεπαφή χρήστη, η οποία περιλαμβάνει εργαλεία που βοηθούν τον τελικό χρήστη ενός DSS να πλοηγηθεί στο σύστημα και γ) τη βάση γνώσεων, η οποία περιλαμβάνει πληροφορίες από εσωτερικές και εξωτερικές πηγές.

2.7.9 Threat Intelligence

Το οικοσύστημα ανταλλαγής πληροφοριών πληροφοριών για τις απειλές στον κυβερνοχώρο (cyber threat intelligence information exchange ecosystem) αποτελεί μια προσέγγιση για την αυτοματοποιημένη κοινή χρήση πληροφοριών σχετικών με τις απειλές [27]. Υπάρχουν πολυάριθμες οντολογίες που προσπαθούν να επιτρέψουν την κοινή χρήση απειλών στον κυβερνοχώρο, οι οποίες αναλύονται στη συνέχεια.

Η Trusted Automated eXchange of Indicator Information (TAXII)²³ ορίζει ένα σύνολο υπηρεσιών και ανταλλαγών μηνυμάτων για την ανταλλαγή πληροφοριών σχετικά με την απειλή στον κυβερνοχώρο [27]. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν διευθύνσεις IP, email, ονόματα τομέα και κακόβουλο λογισμικό για ευπάθειες που ανακαλύφθηκαν και αμυντικούς

²²<https://corporatefinanceinstitute.com/resources/knowledge/other/decision-support-system-dss/>

²³<https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf/>

τρόπους δράσης μεταξύ αξιόπιστων συνεργατών. Χρησιμοποιεί πρωτόκολλα δικτύου όπως το HTTP/S για την παροχή ασφάλειας μεταφοράς, υποστηρίζει μοντέλα κοινής χρήσης απειλών, όπως hub-and-spoke, peer-to-peer και public-subscribe και βασίζεται σε πρωτόκολλα δικτύου και κρυπτογράφηση σε επίπεδο δικτύου για την προστασία ολόκληρου του μηνύματος TAXII κατά τη μεταφορά.

Το Structured Threat Information Expression (STIX)²⁴ είναι μια συλλογική προσπάθεια για τον καθορισμό και την ανάπτυξη μιας δομημένης γλώσσας που να αντιπροσωπεύει τις πληροφορίες για τις απειλές στον κυβερνοχώρο [27]. Η γλώσσα STIX μεταφέρει όλο το φάσμα των πληροφοριών για πιθανές απειλές στον κυβερνοχώρο και προσπαθεί να είναι πλήρως εκφραστική, ευέλικτη, επεκτάσιμη, αυτοματοποιήσιμη και όσο το δυνατόν πιο αναγνώσιμη από τον άνθρωπο. Όλα τα ενδιαφερόμενα μέρη είναι ευπρόσδεκτα να συμμετάσχουν στην εξελισσόμενη STIX ως μέρος της ανοιχτής, συνεργατικής κοινότητάς του. Οι περιπτώσεις χρήσης STIX περιλαμβάνουν την Ανάλυση Κυβερνοαπειλών, τον Καθορισμό μοτίβων δεικτών για απειλές στον κυβερνοχώρο, τη Διαχείριση Δραστηριοτήτων Πρόληψης και Αντιμετώπισης Κυβερνοαπειλών και την Κοινή χρήση πληροφοριών κυβερνοαπειλής.

Τέλος, το IBM X-Force Exchange²⁵ είναι μια πλατφόρμα κοινής χρήσης πληροφοριών απειλών που βασίζεται σε σύννεφο, η οποία μπορεί να χρησιμοποιηθεί για την ταχεία έρευνα των πιο πρόσφατων παγκόσμιων απειλών για την ασφάλεια, τη συγκέντρωση πληροφοριών με δυνατότητα δράσης, τη διαβούλευση με ειδικούς και τη συνεργασία με άλλες λύσεις.

²⁴<https://stix.mitre.org/>

²⁵<https://exchange.xforce.ibmcloud.com/>

Κεφάλαιο 3

Εκπαιδευτικά Πλαίσια



ε αυτό το κεφάλαιο, πραγματοποιείται παρουσίαση των πιο σημαντικών Εκπαιδευτικών Πλαισίων σε τεχνολογικό και γνωσιακό επίπεδο με σκοπό την πλήρη κατανόηση αυτών.

3.1 Περιγραφή

Τα εκπαιδευτικά πλαίσια αναδεικνύονται ως ουσιαστική και αναπόσπαστη πτυχή της διαδικασίας εκπαίδευσης, σκοπεύοντας να καθορίσουν και να διαμορφώσουν τις βασικές και τις θεμελιώδεις αρχές πάνω στις οποίες θα οικοδομηθούν και θα εδραιωθούν οι εκπαιδευτικές δομές. Πέραν του ότι αποσκοπούν στην ενίσχυση των εκπαιδευτικών, τα εκπαιδευτικά πλαίσια παρέχουν ένα ευρύ φάσμα μέσων και εργαλείων μέσω των οποίων μπορούν να καθοριστούν και να διατυπωθούν οι ανώτεροι στόχοι και οι προοπτικές της μάθησης, καθώς και να ενσωματωθεί η αξιολόγηση των μαθητών στην εκπαιδευτική διαδικασία. Επιπλέον, εξυπηρετούν τους μαθητές, καθιστώντας τους ικανούς να κατανοήσουν και να αντλήσουν οφέλη από τις γνώσεις που αποκτούν. Είναι σημαντικό να υπογραμμιστεί ότι, αν και μοιράζονται μια κοινή προσέγγιση, δεν αποτελούν απλώς αντίγραφα μεταξύ δομών. Καθένα απαιτεί προσεκτική προσαρμογή στις ιδιαίτερες ανάγκες και το πλαίσιο λειτουργίας της κάθε εκπαιδευτικής δομής. Επιπρόσθετα, η συνεχής εκτίμηση και προσαρμογή τους αποτελεί απολύτως ζωτικό παράγοντα για την αποτελεσματική υποστήριξη και προώθηση της διαδικασίας μάθησης και ανάπτυξης.

Η εφαρμογή ενός εκπαιδευτικού πλαισίου έχει θετικό αντίκτυπο στην εκπαιδευτική διαδικασία καθώς δημιουργεί μια συνεκτική κουλτούρα διδασκαλίας και μάθησης. Επιπλέον, όσο οι εκ-

παιδευτικές ανάγκες παραμένουν οι ίδιες, το εκπαιδευτικό προσωπικό μπορεί να εναλλάσσεται, χωρίς αυτό να επηρεάζει την ποιότητα και το αποτέλεσμα της εκπαιδευτικής διαδικασίας, ενώ ταυτόχρονα προσφέρει μια άμεση εικόνα του οράματος της εκπαιδευτικής δομής και ένα σημείο αναφοράς για το πώς οι ίδιοι θα ενταχθούν σε αυτή. Τέλος, η εφαρμογή ενός εκπαιδευτικού πλαισίου, επιτρέπει κάθε τμήμα εντός της ίδιας δομής να αντιμετωπίζεται ως ξεχωριστή οντότητα με διαφορετικές ανάγκες, αλλά στη μεγάλη εικόνα όλα συνδέονται και κινούνται προς μια ενιαία κατεύθυνση.

Με τις ολοένα και πιο συχνές επιθέσεις στον κυβερνοχώρο και τις παραβιάσεις δεδομένων, η ανάγκη για καταρτισμένους επαγγελματίες στο χώρο της ασφάλειας παραμένει επιτακτική. Αν και υπάρχει πληθώρα πιστοποιήσεων και σεμιναρίων μέσω των οποίων οι υπάρχοντες επαγγελματίες μπορούν να βοηθήσουν στην ανάπτυξη του τομέα και την μερική κάλυψη των αναγκών του, η εδραίωση της ασφάλειας στον κυβερνοχώρο ως χωριστός ακαδημαϊκός κλάδος παραμένει για πολλούς αναγκαία. Ήδη αρκετά πανεπιστήμια έχουν εντάξει τέτοιου είδους προγράμματα τόσο σε προπτυχιακό όσο και σε μεταπτυχιακό επίπεδο. Παρ' όλα αυτά ακόμη δεν έχουν καθοριστεί οι προσδοκίες της αγοράς εργασίας όσον αφορά τις γνώσεις και τις ικανότητες των αποφοίτων αυτών των προγραμμάτων. Συνεπώς, η εφαρμογή διαφόρων εκπαιδευτικών πλαισίων μπορεί να συνδράμει στη διαμόρφωση οικουμενικών στάνταρ για την ποιότητα και το είδος της γνώσης και εμπειρίας που θα προσφέρεται μέσω τέτοιου είδους ακαδημαϊκών προγραμμάτων.

3.2 National Initiative for Cybersecurity Education (NICE) Framework

Το National Initiative for Cybersecurity Education (NICE) αποτελεί ένα εθνικής πρωτοβουλίας πρόγραμμα στις Ηνωμένες Πολιτείες, που δημιουργήθηκε με αίτημα της προώθησης της εκπαίδευσης και κατάρτισης στον κλάδο της κυβερνοασφάλειας. Το πρόγραμμα λειτουργεί υπό την αιγίδα του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) και αντιπροσωπεύει ένα συνεργατικό πλαίσιο που συνδυάζει τον δημόσιο και ιδιωτικό τομέα, τον ακαδημαϊκό κόσμο, και άλλους ενδιαφερόμενους φορείς. Ο κεντρικός στόχος του NICE εστιάζεται στην προώθηση της ανάπτυξης εξειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας, παρέχοντας πλαίσια εκπαίδευσης και πιστοποίησης, καθώς ενισχύοντας την εκπαίδευση και την επαγγελματική ανάπτυξη στον συγκεκριμένο τομέα.

Το NICE έχει καθιερώσει ένα ευρύ φάσμα προτύπων, προγραμμάτων και πόρων που εστιάζονται στην κυβερνοασφάλεια. Ένα από τα κύρια εργαλεία που διαθέτει το NICE είναι το Framework for Improving Critical Infrastructure Cybersecurity, το οποίο είναι ευρέως γνωστό ως NIST Cybersecurity Framework. Αυτό το πλαίσιο παρέχει ένα κοινό γλωσσάριο και προσφέρει μια ολοκληρωμένη προσέγγιση για τη διαχείριση κινδύνων και την προστασία κρίσιμων υποδομών από κυβερνοεπιθέσεις ενώ αποτελεί επίσης ένα κοινό γλωσσάριο και μια δομή για την κατανόηση των ρόλων και των αρμοδιοτήτων στον τομέα της κυβερνοασφάλειας.

Το NICE διευκολύνει επίσης τη δημιουργία συνεργιών μεταξύ διαφόρων φορέων και προάγει την ανταλλαγή βέλτιστων πρακτικών και την ανάπτυξη κοινοτικών προγραμμάτων και πρωτοβουλιών. Επιπλέον, το NICE ενθαρρύνει την έρευνα και την ανάπτυξη σε θέματα κυβερνοασφάλειας και παρέχει πλατφόρμες για τη διάδοση γνώσεων και την επικοινωνία μεταξύ επαγγελματιών στον τομέα.

Ένα σημαντικό στοιχείο του NICE είναι η προώθηση της εκπαίδευσης και της κατάρτισης σε όλα τα επίπεδα. Αυτό περιλαμβάνει προγράμματα σπουδών στα πανεπιστήμια, επιμορφωτικά σεμινάρια και εκπαιδευτικά προγράμματα πιστοποίησης για επαγγελματίες στον τομέα της κυβερνοασφάλειας. Μέσω αυτών των πρωτοβουλιών, το NICE προάγει την ανάπτυξη εξειδικευμένων επαγγελματιών στην κυβερνοασφάλεια και συμβάλλει στην αντιμετώπιση των αυξανόμενων απειλών στον τομέα της κυβερνοασφάλειας.

Η δομή του πλαισίου NICE αποτελείται από 7 κύριες κατηγορίες που προσδίδουν τον πρωταρχικό σκελετό αυτής. Αυτές οι κατηγορίες είναι οι εξής: Ασφαλής Παροχή (Securely Provision [SP]), Λειτουργία και Συντήρηση (Operate and Maintain [OM]), Επίβλεψη και Κυβέρνηση (Oversee and Govern [OV]), Προστασία και Υπεράσπιση (Protect and Defend [PR]), Ανάλυση (Analyze [AN]), Συλλογή και Λειτουργία (Collect and Operate [CO]) και Έρευνα (Investigate [IN]). Κάθε μία από τις προαναφερθείσες κατηγορίες αποτελείται από τομείς ειδικότητας (specialty areas) και εργασιακούς ρόλους (work roles). Αξίζει να σημειωθεί ότι ο εκάστοτε τομέας ειδικότητας αντιπροσωπεύει μια ομάδα συναφών εργασιών ή λειτουργιών στο χώρο της ασφάλειας του κυβερνοχώρου (T). Παρομοίως οι εργασιακοί ρόλοι, παρέχουν μια λεπτομερή περιγραφή των γνώσεων, δεξιοτήτων και ικανοτήτων (KSAs) που απαιτούνται για την εκτέλεση του ρόλου αυτού.

Πιο αναλυτικά:

Εργασίες (T): Οι εργασίες είναι συγκεκριμένα καθορισμένα κομμάτια δουλειάς που αποτελούν μέρος ενός συγκεκριμένου εργασιακού ρόλου σε μια ειδικότητα. Για παράδειγμα, μια εργασία

μπορεί να περιλαμβάνει την εφαρμογή τεκμηρίωσης ασφαλούς κώδικα (T0014) ή την ανάπτυξη περιεχομένου για εργαλεία κυβερνοάμυνας (T0020). Οι εργασίες (T) είναι συγκεκριμένοι στόχοι που πρέπει να ολοκληρωθούν για να καλυφθεί ένας εργασιακός ρόλος.

Γνώσεις (K): Οι γνώσεις αποτελούν ένα σύνολο πληροφοριών απαραίτητων για την εκτέλεση μιας συγκεκριμένης λειτουργίας στην κυβερνοασφάλεια. Για παράδειγμα, η γνώση των εννοιών και των πρωτοκόλλων δικτύωσης υπολογιστών και των μεθοδολογιών ασφάλειας δικτύων (K0001) μπορεί να θεωρηθεί απαραίτητη για την εκτέλεση αξιολογήσεων ευπαθειών και διαγνωστικών δικτύων, τα οποία είναι σημαντικά για τον εργασιακό ρόλο του "Αναλυτή Κυβερνοάμυνας—PR-CDA-001". Ορισμένα στοιχεία των TKSA υποδεικνύουν υψηλή σημασία για διαφορετικούς εργασιακούς ρόλους και ειδικότητες σε διάφορες κατηγορίες εργατικού δυναμικού.

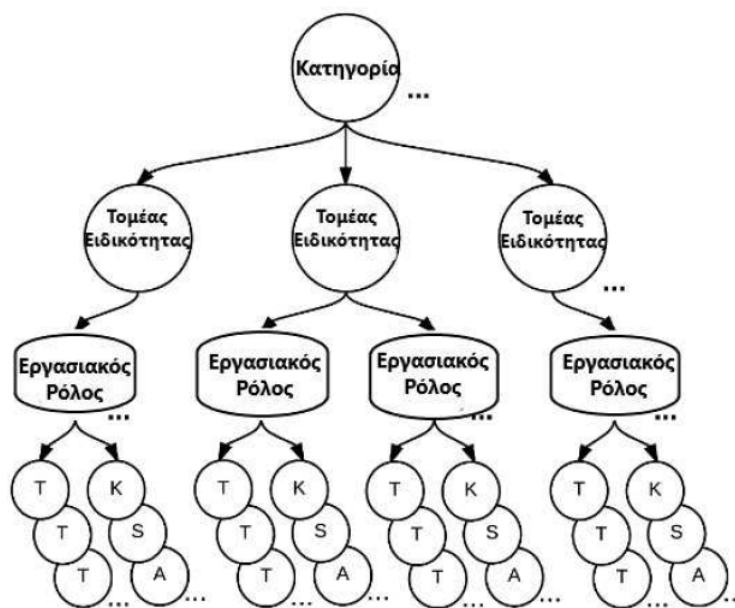
Δεξιότητες (S): Οι δεξιότητες είναι παρατηρήσιμες ικανότητες που αποκτώνται μέσω της χρήσης των γνώσεων (K) και επικεντρώνονται στις ενέργειες του μαθητευόμενου. Για παράδειγμα, ένα άτομο μπορεί να αναπτύξει ή να αποκτήσει τη δεξιότητα να αναγνωρίζει, να καταγράφει, να περιορίζει και να αναφέρει κακόβουλο λογισμικό (S0003) ή να αναπτύσσει και να αναπτύσσει υπογραφές (S0020). Οι δεξιότητες (S) είναι πιο συγκεκριμένες και προσανατολισμένες στη δράση σε σχέση με τις γνώσεις (K) και αναπτύσσονται μέσω πρακτικής και εμπειρίας. Αντιπροσωπεύουν την ικανότητα εκτέλεσης συγκεκριμένων ενεργειών και εργασιών (T) και είναι συνήθως πιο πρακτικές.

Ικανότητες (A): Οι ικανότητες αναφέρονται στην ενδογενή ικανότητα ενός ατόμου να εκτελεί ορισμένες εργασίες ή λειτουργίες σε περιβάλλον κυβερνοασφάλειας. Πρόκειται για έμφυτες ή αναπτυγμένες δυνατότητες που επιτρέπουν σε κάποιον να ανταποκρίνεται σε απαιτήσεις και προκλήσεις στον τομέα της κυβερνοασφάλειας. Για παράδειγμα, η ικανότητα να σκέφτεται κριτικά και να λαμβάνει αποφάσεις υπό πίεση (A0010) ή η ικανότητα να αναλύει και να ερμηνεύει δεδομένα από διάφορες πηγές για την ανίχνευση ανωμαλιών και πιθανών απειλών (A0025) είναι βασικές ικανότητες που απαιτούνται για τον εργασιακό ρόλο του "Αναλυτή Κυβερνοάμυνας—PR-CDA-001". Οι ικανότητες (A) είναι θεμελιώδεις για την ανάπτυξη δεξιοτήτων (S) και γνώσεων (K), καθώς αποτελούν τη βάση πάνω στην οποία στηρίζονται οι πρακτικές εφαρμογές στον τομέα της κυβερνοασφάλειας.

Από το 2010 έως και σήμερα έχουν δημιουργηθεί και εφαρμοστεί 4 εκδοχές του NICE. Η πρώτη έκδοση του πλαισίου NICE (NICE Framework, version 1.0) δημοσιοποιήθηκε το Σεπτέμβριο του 2012 ενώ η δεύτερη (NICE Framework, version 2.0) το 2014. Η τρίτη

εκδοχή δημοσιεύτηκε τον Αύγουστο του 2017 με το όνομα "NIST Special Publication 800-181", η δομή του οποίου συνοψίζεται στον πίνακα 1. Αξίζει να σημειωθεί πως η 2.0 version περιλάμβανε 32 τομείς ειδικότητας ενώ στη "NIST Special Publication 800-181" προστέθηκε ακόμη μία. Τέλος, η τελευταία εκδοχή του πλαισίου NICE, η οποία χρησιμοποιείται έως και σήμερα δημοσιεύτηκε το Νοέμβριο του 2020 και ονομάζεται "NIST Special Publication 800-181 revision 1, the Workforce Framework for Cybersecurity".

Στο Σχήμα 3.2 παρουσιάζεται η συσχέτιση μεταξύ των διαφορετικών συνιστωσών του εκπαιδευτικού πλαισίου NICE. Τα αποσιωπητικά (...) δηλώνουν την ύπαρξη και άλλων συνιστωσών της ίδιας τάξης ενώ τα γράμματα T αντιπροσωπεύει το καθήκον, το K τη γνώση, το S τη δεξιότητα και το A την ικανότητα. Στον Πίνακα 3.1 αποτυπώνεται η πλήρης δομή του **NIST Special Publication 800-181**, που δημοσιοποιήθηκε το 2020. Τόσο το σχήμα όσο και ο πίνακας βασίζονται στο [36].



Σχήμα 3.2: Σχέση μεταξύ των διαφορετικών τμημάτων της δομής του πλαισίου NICE.

Κατηγορίες	Τομέας Ειδικότητας	Εργασιακοί Ρόλοι
Ασφαλής Παροχή	Διαχείριση Κινδύνου	Εξουσιοδοτημένος Επίσημος Αντιπρόσωπος
		Αξιολογητής Ελέγχου Ασφαλείας
	Ανάπτυξη Λογισμικού	Προγραμματιστής λογισμικού
		Ασφαλής Αξιολογητής Λογισμικού
	Αρχιτεκτονική Συστημάτων	Αρχιτέκτονας Επιχείρησης
		Αρχιτέκτονας Ασφαλείας
	Τεχνολογία R&D	Ειδικός Έρευνας & Ανάπτυξης
	Προγραμματισμός Συστηματικών Απαιτήσεων	Προγραμματιστής Συστηματικών Απαιτήσεων
	Δοκιμή και Αξιολόγηση	Ειδικός Δοκιμών και Αξιολόγησης Συστήματος
Λειτουργία & Συντήρηση	Ανάπτυξη Συστημάτων	Προγραμματιστής Ασφάλειας Πληροφοριακών Συστημάτων
		Προγραμματιστής Συστημάτων
	Διαχείριση Δεδομένων	Διαχειριστής Βάσης Δεδομένων
		Αναλυτής Δεδομένων
	Διαχείριση Γνώσης	Διαχειριστής Γνώσης
	Εξυπηρέτηση Πελατών και Τεχνική Υποστήριξη	Ειδικός Τεχνικής Υποστήριξης
	Υπηρεσίες Δικτύου	Ειδικός Λειτουργίας Δικτύου
	Διαχείριση Συστημάτων	Διαχειριστής Συστημάτων
	Ανάλυση Συστημάτων	Αναλυτής Ασφάλειας Συστημάτων

Επίβλεψη & Κυβέρνηση	Νομικές Συμβουλές και Συνηγορία	Νομικός Σύμβουλος Κυβερνοχώρου
		Υπεύθυνος Προστασίας Προσωπικών Δεδομένων
	Κατάρτιση, Εκπαίδευση και Ευαισθητοποίηση	Δημιουργός Εκπαιδευτικού Προγράμματος Σπουδών Κυβερνοχώρου
		Εκπαιδευτής Κυβερνοχώρου
		Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων
	Διαχείριση Κυβερνοασφάλειας	Διαχειριστής Ασφάλειας Επικοινωνιών
	Στρατηγικός Σχεδιασμός και Πολιτική	Προγραμματιστής και Διευθυντής Εργατικού Δυναμικού Κυβερνοχώρου
		Σχεδιαστής Κυβερνοπολιτικής και Στρατηγικής
	Εκτελεστική Ηγεσία Κυβερνοχώρου	Εκτελεστικός Ηγέτης Κυβερνοχώρου
	Διαχείριση Έργου και Απόκτηση	Υπεύθυνος Προγράμματος
		Υπεύθυνος Έργου Πληροφορικής
		Υπεύθυνος Υποστήριξης Προϊόντων
		Υπεύθυνος Επενδύσεων Πληροφορικής
		Ελεγκτής Προγράμματος Πληροφορικής
Προστασία & Υπεράσπιση	Ανάλυση Κυβερνοάμυνας	Αναλυτής Κυβερνοάμυνας
	Υποστήριξη Κυβερνοαμυντικής Υποδομής	Ειδικός Υποστήριξης Κυβερνοαμυντικής Υποδομής
	Αντιμετώπιση Περιστατικού	Αντιμετώπιση Περιστατικών Άμυνας στον Κυβερνοχώρο
	Αξιολόγηση και Διαχείριση Ευπάθειας	Αναλυτής Αξιολόγησης Ευπάθειας
Ανάλυση	Ανάλυση Απειλών	Αναλυτής Απειλής
	Ανάλυση εκμετάλλευσης	Αναλυτής εκμετάλλευσης
	Ανάλυση All-Source	Αναλυτής All-Source
		Ειδικός Αξιολόγησης Αποστολών
	Στόχοι	Προγραμματιστής Στόχων
	Γλωσσική Ανάλυση	Πολυεπιστημονικός Αναλυτής Γλωσσών
Συλλογή & Λειτουργία	Λειτουργίες συλλογής	Διευθυντής Συλλογής All-Source
		Διευθυντής Απαιτήσεων Συλλογής All-Source
	Επιχειρησιακός Σχεδιασμός στον Κυβερνοχώρο	Σχεδιαστής Κυβερνοχώρου Intel
		Σχεδιαστής Κυβερνοχώρου Ops
		Σχεδιαστής ολοκλήρωσης συνεργατών
	Επιχειρήσεις στον Κυβερνοχώρο	Χειριστής Κυβερνοχώρου
Έρευνα	Έρευνα Κυβερνοχώρου	Ερευνητής Ηλεκτρονικού Εγγλήματος

	Ψηφιακή Εγκληματολογία	Αναλυτής Εγκληματολογικής Αν- τικατασκοπείας
		Αναλυτής Εγκληματολογικής Άμυνας στον Κυβερνοχώρο

Πίνακας 3.1: Πλήρης δομή του **NIST Special Publication 800-181**

3.3 ACM Curriculum 2017 (CSEC2017)

Τα τελευταία χρόνια έχουν γίνει πολλές προσπάθειες καθοδήγησης για τη δημιουργία ολοκληρωμένων και αποτελεσματικών προγραμμάτων προπτυχιακών σπουδών, όπως για παράδειγμα μέσω του πλαισίου NICE. Παρ' όλα αυτά το συγκεκριμένο εκπαιδευτικό πλαίσιο καλύπτει σχεδόν εξ ολοκλήρου τις ανάγκες για αποτελεσματικό εργατικό δυναμικό στο τομέα της κυβερνοασφάλειας και ελάχιστα έως καθόλου τις ακαδημαϊκές ανάγκες για τη δημιουργία νέων πλήρως καταρτισμένων επαγγελματιών. Η λύση σε αυτό το πρόβλημα ήρθε μέσω του "Cybersecurity Curricula 2017 report" (CSEC 2017), που είναι το αποτέλεσμα συνεργασίας πολλών οργανισμών πληροφορικής μεταξύ των οποίων η ACM και η IEEE.

Το Association for Computing Machinery (ACM) Curriculum 2017, γνωστό και ως CSEC 2017, είναι ένα σημαντικό έγγραφο που παρέχει κατευθυντήριες γραμμές για τη διδασκαλία της πληροφορικής σε πανεπιστήμια και εκπαιδευτικά ιδρύματα σε παγκόσμιο επίπεδο. Η σχέση του CSEC2017 με την κυβερνοασφάλεια είναι ιδιαίτερα σημαντική, καθώς αφορά την εκπαίδευση και την κατάρτιση επαγγελματιών πληροφορικής που ασχολούνται με την προστασία των συστημάτων πληροφορικής από κυβερνοεπιθέσεις και απειλές.

Το CSEC2017 περιλαμβάνει στοιχεία που αφορούν στην κυβερνοασφάλεια, καθώς αναγνωρίζει τη σημασία της στη σύγχρονη κοινωνία της πληροφορίας. Μέσα από τα προγράμματα διδασκαλίας που προτείνει, το CSEC 2017 ενθαρρύνει την έμφαση στην κυβερνοασφάλεια ως ένα από τα κύρια θέματα που πρέπει να καλύπτονται στην εκπαίδευση των φοιτητών πληροφορικής. Παρέχει επίσης οδηγίες για την ενσωμάτωση θεμάτων ασφάλειας στο πρόγραμμα σπουδών, συμπεριλαμβανομένων μαθημάτων που καλύπτουν θέματα όπως η κρυπτογραφία, οι κυβερνοεπιθέσεις, η ανάλυση κινδύνων και η προστασία δεδομένων.

Ένας από τους βασικούς στόχους του CSEC 2017 είναι να διασφαλίσει ότι οι φοιτητές πληροφορικής αποκτούν τις απαραίτητες γνώσεις και δεξιότητες για να προστατεύουν τα συστήματα πληροφορικής από επιθέσεις και απειλές κυβερνοασφάλειας. Μέσω μαθημάτων και εργαστηρι-

ακών εργασιών που εστιάζουν στην ανάπτυξη ασφαλών συστημάτων και στην αντιμετώπιση κυβερνοεπιθέσεων, οι φοιτητές μπορούν να εξοικειωθούν με τις βασικές αρχές της κυβερνοασφάλειας και να αναπτύξουν τις δεξιότητες που απαιτούνται για να αντιμετωπίζουν τις σύγχρονες κυβερνοεπιθέσεις.

Επιπλέον, το CSEC 2017 προάγει την έρευνα και την καινοτομία στον τομέα της κυβερνοασφάλειας. Προτείνει την ενσωμάτωση προγραμμάτων έρευνας στα πανεπιστημιακά προγράμματα πληροφορικής, τα οποία εστιάζουν σε θέματα όπως η ανάλυση κυβερνοεπιθέσεων, η ανάπτυξη ασφαλών δικτύων και η προστασία των δεδομένων. Μέσω αυτών των ερευνητικών προγραμμάτων, οι φοιτητές μπορούν να συμβάλουν στην πρόοδο του τομέα της κυβερνοασφάλειας και να αναπτύξουν νέες τεχνικές και λύσεις για την προστασία των πληροφοριακών συστημάτων.

Το CSEC 2017 επιδιώκει επίσης τη συνεργασία με τη βιομηχανία και τον κλάδο της κυβερνοασφάλειας, προωθώντας πρακτικές εμπειρίες εργασίας και πρακτικά εκπαιδευτικά προγράμματα. Μέσω αυτών των συνεργασιών, οι φοιτητές έχουν τη δυνατότητα να εργαστούν σε πραγματικά προβλήματα ασφάλειας και να αποκτήσουν πρακτική εμπειρία στον τομέα της κυβερνοασφάλειας.

Το CSEC 2017 αποτελεί ένα κρίσιμο ρόλο στην προετοιμασία των μελλοντικών επαγγελματιών πληροφορικής για τις προκλήσεις του κυβερνοχώρου. Μέσω των κατευθυντήριων γραμμών και των προτεινόμενων προγραμμάτων σπουδών, εξασφαλίζει ότι οι φοιτητές αποκτούν τις απαραίτητες γνώσεις, δεξιότητες και εμπειρίες για να γίνουν αποτελεσματικοί επαγγελματίες στον τομέα της κυβερνοασφάλειας. Μέσω αυτού του προγράμματος, η εκπαίδευση στην κυβερνοασφάλεια γίνεται πιο προσβάσιμη και πιο πλήρης, προετοιμάζοντας τους μελλοντικούς επαγγελματίες να αντιμετωπίσουν τις απαιτήσεις και τις προκλήσεις του σύγχρονου κυβερνοχώρου.

Οι οδηγίες που παρέχονται μέσω του CSEC 2017 αφορούν τρεις κατηγορίες: τομείς γνώσης, εγχαρσίες έννοιες και ένα σύνολο πειθαρχικών απόψεων. Αξίζει να σημειωθεί ότι το CSEC 2017 δεν οριοθετεί το περιεχόμενο των προγραμμάτων σπουδών αλλά θέτει το υπόβαθρο πάνω στο οποίο οι σπουδές κυβερνοασφάλειας μπορούν να υπάρχουν. Ο Πίνακας 3.2 είναι βασισμένος στο [37] και περιγράφει εν συντομία τις τρεις αυτές βασικές κατηγορίες

Τομείς Γνώσης	Εγκάρσιες Έννοιες	Πειθαρχικές Απόψεις
Ασφάλεια Δεδομένων: Προστασία δεδομένων κατά την επεξεργασία και τη μεταφορά	Εμπιστευτικότητα: Περιορισμός της πρόσβασης σε δεδομένα και πληροφορίες συστήματος μόνο σε εξουσιοδοτημένα πρόσωπα	Επιστήμη των Υπολογιστών
Ασφάλεια Λογισμικού: Ανάπτυξη και χρήση λογισμικού που με αξιοπιστία διατηρεί ασφαλείς τις πληροφορίες και τα συστήματα	Ακεραιότητα: Διαβεβαίωση ότι τα δεδομένα και οι πληροφορίες είναι ακριβή και αξιόπιστα	Μηχανικός Υπολογιστών
Ασφάλεια Συστήματος: Πτυχές ασφάλειας συστημάτων που χρησιμοποιούν λογισμικό και αποτελούνται από εξαρτήματα και συνδέσεις	Διαθεσιμότητα: Τα δεδομένα, οι πληροφορίες και τα συστήματα είναι προσβάσιμα	Πληροφοριακά Συστήματα
Ανθρώπινη Ασφάλεια: Μελέτη της ανθρώπινης συμπεριφοράς στο πλαίσιο της προστασίας δεδομένων και του μετριασμού απειλών	Κίνδυνος: Δυνατότητα κέρδους ή απώλειας	Πληροφορική
Οργανωτική Ασφάλεια: Προστασία των οργανισμών από απειλές στο κυβερνοχώρο και διαχείριση του κινδύνου για την επιτυχή υποστήριξη των οργανισμών	Ανταγωνιστικός Τρόπος Σκέψης: Μια διαδικασία σκέψης που εξετάζει τις πιθανές ενέργειες του “αντιπάλου” που εργάζεται κατά του θεμιτού αποτελέσματος	Μηχανική Λογισμικού
Κοινωνική Ασφάλεια: Πτυχές της κυβερνοασφάλειας που επηρεάζουν ευρέως την κοινωνία στο σύνολό της	Ανταγωνιστικός Τρόπος Σκέψης: Μια διαδικασία σκέψης που εξετάζει τις πιθανές ενέργειες του “αντιπάλου” που εργάζεται κατά του θεμιτού αποτελέσματος	Μικτό Πειθαρχικό
Ασφάλεια Εξαρτημάτων: Πτυχές ασφάλειας του σχεδιασμού, της δοκιμής και της συντήρησης εξαρτημάτων που αποτελούν μέρος μεγαλύτερων συστημάτων	Συστημική σκέψης: Διαδικασία σκέψης που εξετάζει την αλληλεπίδραση μεταξύ κοινωνικών και τεχνικών περιορισμών για τη πραγματοποίηση εξασφαλισμένων λειτουργιών	Μικτό Πειθαρχικό
Ασφάλεια Σύνδεσης: Ασφάλεια φυσικών και λογικών συνδέσεων μεταξύ εξαρτημάτων	Συστημική σκέψης: Διαδικασία σκέψης που εξετάζει την αλληλεπίδραση μεταξύ κοινωνικών και τεχνικών περιορισμών για τη πραγματοποίηση εξασφαλισμένων λειτουργιών	Μικτό Πειθαρχικό

Πίνακας 3.2: CSEC2017: ”Δομικοί λίθοι” και σύντομη περιγραφή αυτών.

3.4 National Security Agency - Center of Academic Excellence in Cyber Defense (NSA CAE-CD)

Το NSA CAE-CD (National Security Agency - Center of Academic Excellence in Cyber Defense) είναι ένα πρόγραμμα που αναπτύχθηκε από τον Εθνικό Οργανισμό Ασφάλειας (NSA) των Ηνωμένων Πολιτειών με σκοπό την προώθηση της κυβερνοασφάλειας μέσω της εκπαίδευσης, της έρευνας και της ακαδημαϊκής συνεργασίας. Το πρόγραμμα αποσκοπεί στην ανάπτυξη εξειδικευμένων γνώσεων και δεξιοτήτων σε θέματα κυβερνοασφάλειας σε φοιτητές, εκπαιδευτικούς και ερευνητές, με στόχο την προετοιμασία τους για την αντιμετώπιση των απειλών και των προκλήσεων που αντιμετωπίζουν οι οργανισμοί στον κυβερνοχώρο.

Το πρόγραμμα NSA CAE-CD προσφέρει πιστοποιήσεις και προηγμένα εκπαιδευτικά προγράμματα σε σχέση με την κυβερνοασφάλεια, καλύπτοντας ένα ευρύ φάσμα θεμάτων όπως η κρυπτογραφία, η ανάλυση κινδύνων, η προστασία δικτύων, η ανίχνευση εισβολών, η ανάλυση κυβερνοεπιθέσεων και η ανάπτυξη ασφαλών λογισμικών. Τα προγράμματα αυτά παρέχουν στους συμμετέχοντες τις απαραίτητες γνώσεις και δεξιότητες για την αντιμετώπιση προηγμένων κυβερνοαπειλών και την ανάπτυξη αποτελεσματικών στρατηγικών προστασίας.

Ένα σημαντικό χαρακτηριστικό του προγράμματος NSA CAE-CD είναι η επικέντρωσή του στην πρακτική εκπαίδευση και την εφαρμοσμένη έρευνα. Οι συμμετέχοντες έχουν τη δυνατότητα να εργαστούν σε πραγματικά προβλήματα κυβερνοασφάλειας και να αποκτήσουν πρακτική εμπειρία μέσω εργαστηριακών ασκήσεων και προσομοιώσεων κυβερνοεπιθέσεων. Αυτή η πρακτική προσέγγιση επιτρέπει στους συμμετέχοντες να αναπτύξουν τις δεξιότητές τους σε πραγματικά περιβάλλοντα και να αποκτήσουν αξιόπιστες εμπειρίες για την αντιμετώπιση κυβερνοεπιθέσεων.

Επιπλέον, το πρόγραμμα NSA CAE-CD συνεργάζεται στενά με τη βιομηχανία και τον δημόσιο τομέα για την ανάπτυξη προηγμένων λύσεων κυβερνοασφάλειας και την επίλυση σύνθετων προβλημάτων. Η συνεργασία αυτή επιτρέπει την ανταλλαγή γνώσεων και την ανάπτυξη καινοτόμων τεχνολογιών που συμβάλλουν στην ενίσχυση της κυβερνοασφάλειας σε διάφορους τομείς, όπως οι τράπεζες, οι επιχειρήσεις, ο δημόσιος τομέας και οι κυβερνήσεις.

Τέλος, το NSA CAE-CD παίζει σημαντικό ρόλο στην προώθηση της ευαισθητοποίησης και της εκπαίδευσης για την κυβερνοασφάλεια σε διεθνές επίπεδο. Μέσω συνεργασιών και προγραμμάτων ανταλλαγής, συμβάλλει στην εκπαίδευση επαγγελματιών κυβερνοασφάλειας σε διάφορες χώρες και περιφέρειες, ενισχύοντας έτσι την παγκόσμια ασφάλεια στον κυβερνοχώρο.

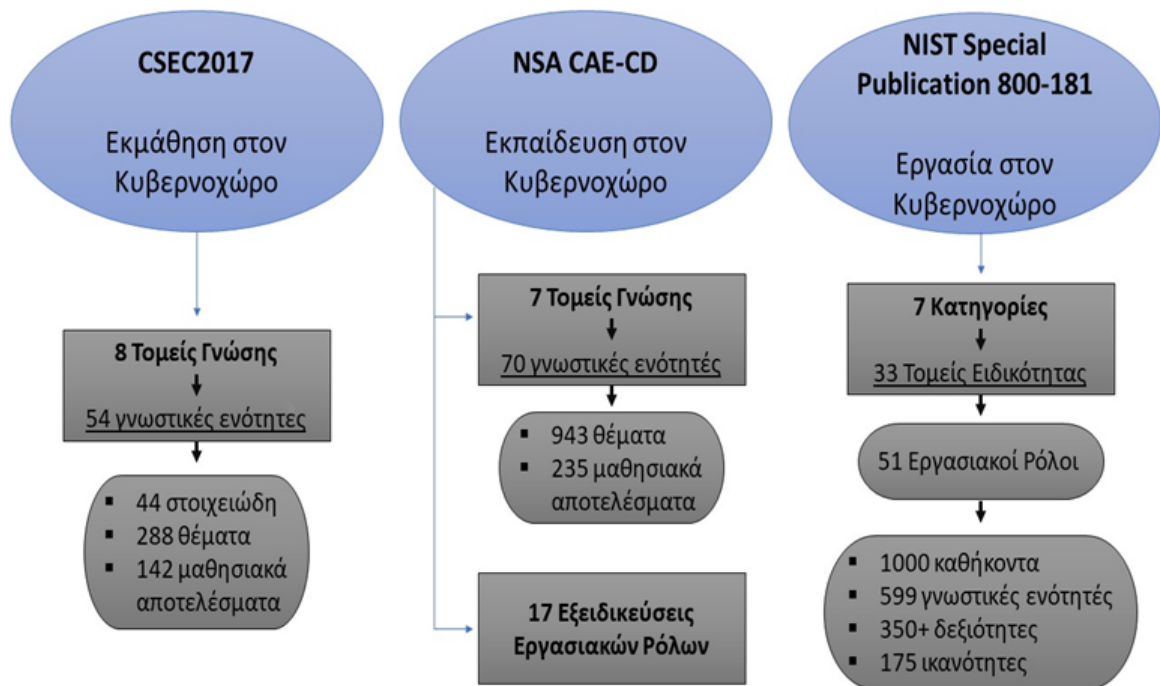
και συμβάλλοντας στη δημιουργία ενός πιο ασφαλούς και αξιόπιστου ψηφιακού περιβάλλοντος.

Η τελευταία έκδοση του CAE-CD δημοσιοποιήθηκε το 2019 και αποτελείται από συνολικά 70 γνωστικές ενότητες, από τις οποίες οι 3 είναι θεμελιώδεις, οι 10 είναι κορμού (5 τεχνικές και 5 μη-τεχνικές) και οι υπόλοιπες 57 είναι προαιρετικές. Η εκάστοτε γνωστική ενότητα εμπεριέχει και καλύπτει συγκεκριμένα θέματα καθώς επίσης και επιθυμητά αποτελέσματα. Επιπλέον, οι γνωστικές ενότητες είναι σχεδιασμένες έτσι ώστε όχι μόνο να υποστηρίζουν και να προετοιμάζουν τους σπουδαστές για συγκεκριμένους ρόλους εργασίας στην ασφάλεια του κυβερνοχώρου, αλλά και να αξιοποιούνται πλήρως μέσα στο ακαδημαϊκό περιβάλλον. Τέλος, αξίζει να αναφερθεί ότι έως και το Μάρτιο του 2019, 159 τετραετή προγράμματα σπουδών ακολουθούν το πρόγραμμα CAE-CD.

Εκπαιδευτικό Πλαίσιο	CSEC 2017	CAE-CD	NICE Framework
Κατηγορίες	8	7	7
Γνωστικές Ενότητες	54	67	599
Μαθησιακά Αποτελέσματα, Δεξιότητες & Ικανότητες	42	235	525
Θέματα/ Καθήκοντα	288	943	1000
Πεδίο Εφαρμογής	Διευρυμένο	Ενδιάμεσο	Εστιασμένο
Ακρίβεια	Περιορισμένη	Ενδιάμεση	Υψηλή
Κοινό-Στόχος	Ακαδημαϊκή κοινότητα	Ακαδημαϊκή κοινότητα, Κυβέρνηση, Εταιρείες	Κυβέρνηση, Εταιρείες

Πίνακας 3.3: Σύγκριση των τριών εκπαιδευτικών πλαισίων CSEC2017, NSA CAE-CD & NIST Special Publication 800-181.

Στο Σχήμα 3.3 και τον Πίνακα 3.3, παρουσιάζεται μια σύγκριση τριών διαφορετικών πλαισίων που χρησιμοποιούνται για την εκπαίδευση και την ανάπτυξη δεξιοτήτων στον τομέα της κυβερνοασφάλειας (CSEC2017, NSA CAE-CD & NICE). Οι Hunall et. al. [38] στην εργασία τους περιγράφουν πώς κάθε πλαίσιο καλύπτει συγκεκριμένους τομείς γνώσης και δεξιοτήτων και πώς αυτά τα πλαίσια μπορούν να αντιστοιχισθούν μεταξύ τους για να ενισχύσουν την εκπαίδευση και την επαγγελματική κατάρτιση στην κυβερνοασφάλεια.



Σχήμα 3.3: Σύνοψη βασικών δομικών στοιχείων των τριών εκπαιδευτικών πλαισίων CSEC2017, NSA CAE-CD & NIST Special Publication 800-181. Εικόνα τροποποιημένη από [38]

Κεφάλαιο 4

Υλοποίηση

Έχοντας ολοκληρώσει την αναφορά στο θεωρητικό υπόβαθρο του NICE Framework, σε αυτό το κεφάλαιο περιγράφεται ο σχεδιασμός των σεναρίων.

4.1 Στόχος Σεναρίων Μάθησης

Κατά το σχεδιασμό του πεδίου κυβερνοάμυνας, θα επικεντρωθούμε κυρίως στους παρακάτω Ειδικούς Τομείς κατά NICE οι οποίοι και θεωρούνται οι σημαντικότεροι για τον ρόλο ενός SOC Analyst.

Ειδικότητα 01 — Ανάλυση Κυβερνοάμυνας (CDA): Η ειδικότητα CDA αφορά την ταυτοποίηση, ανάλυση και αναφορά συμβάντων ασφάλειας σε προσομοιωμένα δίκτυα ή συστήματα. Οι δείκτες ικανότητας περιλαμβάνουν την ανάλυση της κίνησης δικτύου, την εφαρμογή ελέγχων ασφάλειας, την πραγματοποίηση εκτιμήσεων ευπάθειας, τη διαχείριση περιστατικών, την αξιολόγηση της αποτελεσματικότητας της ασφάλειας και την παροχή τεχνικών οδηγιών. Ο σχετικός εργασιακός ρόλος είναι ο Αναλυτής Κυβερνοάμυνας (PR-CDA-001).

Ειδικότητα 02 — Διαχείριση Συστημάτων (ADM): Η ειδικότητα ADM περιλαμβάνει τη διαμόρφωση εξυπηρετητών και τειχών προστασίας, την αντιμετώπιση προβλημάτων και τη συντήρηση με σκοπό την ομαλή λειτουργία. Συμπληρώνει άλλα θέματα κυβερνοασφάλειας και υποστηρίζει τη διαχείριση συστημάτων και δικτύων. Ο σχετικός εργασιακός ρόλος είναι ο Διαχειριστής Συστημάτων (OM-ADM-001).

Ειδικότητα 03 — Υπηρεσίες Δικτύου (NET): Η ειδικότητα NET επικεντρώνεται στη δι-

αχείριση δικτύων, τειχών προστασίας και τη διαμόρφωση δικτυακών συσκευών για ασφάλεια. Οι εργασίες περιλαμβάνουν τον σχεδιασμό, την υλοποίηση και την ανάπτυξη υλικού και εικονικών περιβαλλόντων και τη ρύθμιση συσκευών για μείωση των κινδύνων κυβερνοεπιθέσεων και προστασία των δεδομένων και των περιουσιακών στοιχείων του οργανισμού. Ο σχετικός εργασιακός ρόλος είναι ο Ειδικός Λειτουργιών Δικτύου (OM-NET-001).

Ειδικότητα 04 — Υποστήριξη Υποδομών Κυβερνοάμυνας (INF): Η ειδικότητα INF επικεντρώνεται στην ανάλυση δεδομένων από εργαλεία κυβερνοάμυνας για την αντιμετώπιση απειλών. Περιλαμβάνει την κατανόηση της χρήσης εργαλείων, την ανάλυση συμβάντων και την αξιολόγηση της ασφάλειας κυβερνοάμυνας. Ο σχετικός εργασιακός ρόλος είναι ο Ειδικός Υποστήριξης Υποδομών Κυβερνοάμυνας (PR-INF-001).

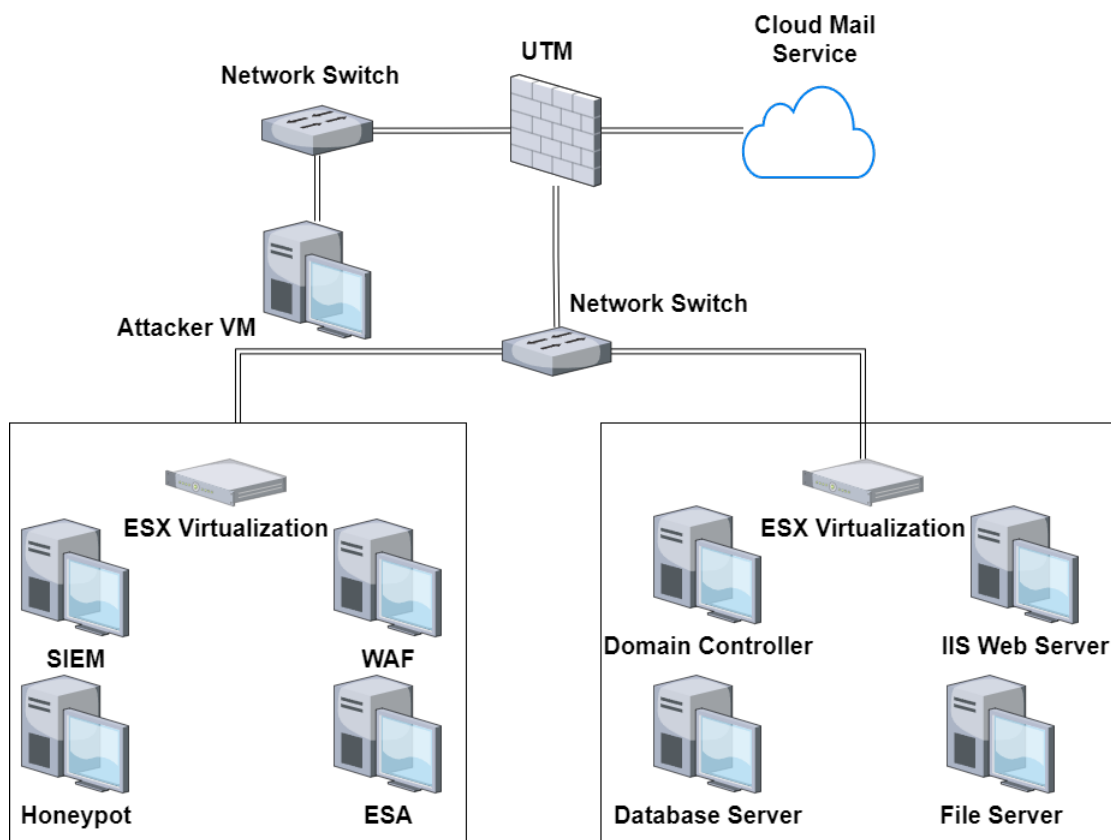
Ειδικότητα 05 — Αξιολόγηση και Διαχείριση Ευπαθειών (VAM): Η ειδικότητα VAM αφορά την αναγνώριση ευπαθειών, τη διενέργεια εκτιμήσεων και την εφαρμογή μέτρων για τη μείωση των κινδύνων. Είναι κατάλληλη για αρχάριους και επικεντρώνεται στις αρχές διαχείρισης ευπαθειών και περιουσιακών στοιχείων. Ο σχετικός εργασιακός ρόλος είναι ο Αναλυτής Αξιολόγησης Ευπαθειών (PR-VAM-001).

Από τα παραπάνω, σκοπός είναι η όσο το δυνατόν μεγαλύτερη κάλυψη του ρόλου Αναλυτής Κυβερνοάμυνας (PR-CDA-001).

4.2 Αρχιτεκτονική Σεναρίων Μάθησης

Για την δημιουργία του πεδίου κυβερνοάμυνας χρησιμοποιήθηκαν δύο εξυπηρετητές HP ProLiant με εγκατάσταση λογισμικού εικονικοποίησης VMware ESXi. Σκοπός αυτής της επιλογής είναι η μείωση του κόστους ενώ από διαχειριστικής άποψης η ευκολία στην διαδικασία λήψης αντίγραφου ασφαλείας όπως και στιγμιαίου αντιγράφου (Snapshot) σε περίπτωση που απαιτηθεί η επαναφορά του για επανάληψη της άσκησης.

Στο Σχήμα 4.4 αναφέρεται ενδεικτικά η Αρχιτεκτονική Δομή της λύσης καθώς και οι τεχνολογίες που την απαρτίζουν.



Σχήμα 4.4: Απεικόνιση Αρχιτεκτονικής Δικτύου

4.3 Σχεδιασμός των Σεναρίων Μάθησης κατά NICE Framework

Σενάριο 01 (SOC01) - Παραμετροποίηση και Ανάλυση Καταγραφών Δικτυακού Switch

Κατά τον σχεδιασμό των σεναρίων ελήφθη υπόψιν η εφαρμογή των KSATs με σκοπό την κάλυψη όσων περισσότερων εξ αυτών ήταν δυνατό με βάση τον ρόλο του Αναλυτή Περιστατικών Ασφαλείας. Στους παρακάτω πίνακες αναλύεται η αντιστοίχιση κατηγοριών Γνώσεων, Δεξιοτήτων, Ικανοτήτων και Εργασιών με το εκάστοτε σενάριο. Ο σχεδιασμός των σεναρίων και η αντιστοίχιση των κατηγοριών έγινε με τρόπο που θα επέτρεπε την σταδιακή εισαγωγή των εκπαιδευόμενων στον τομέα της Κυβερνοασφάλειας. Εκτός της κάλυψης των προαπαιτούμενων κατηγοριών, ο σχεδιασμός περιλαμβάνει την κάλυψη KSATs που δεν ανήκουν

στον ρόλο του εκπαιδευόμενου με βάση το Πρότυπο Εκπαίδευσης NICE, αλλά θεωρούντε εξίσου σημαντικά για την κατανόηση και ορθή διαπεράτωση των εργασιών που θα κληθούν οι αναλυτές ασφαλείας να εκτελέσουν σε ένα εργασιακό περιβάλλον.

Οι συμμετέχοντες της άσκησης, εκπαιδεύονται στον τρόπο παραμετροποίησης μια πόρτας του Switch ως Access ή Trunk όπως επίσης και στον ορισμό διαφορετικών ομάδων (VLANs). Επιπλέον γίνεται μια εισαγωγή στον ορισμό των Net Flows και πως αυτά μπορούν να προωθηθούν σε ένα SIEM που τα υποστηρίζει για ανάλυση. **Τρόπος Υλοποίησης:** Φυσικός Δικτυακός Εξοπλισμός με διαφορετικές παραμετροποιήσεις το καθένα.

Πίνακας 4.1: Σενάριο 01: SOC01 Cisco Switch.

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst, Network Operations Specialist
Κωδικός Ρόλου Εργασίας	PR-CDA-001, OM-NET-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF), Network Services (NET)
Κατηγορία Εργασίας	Protect and Defend (PR), Operate and Maintain (OM)
Γνώσεις	Ανάλυση της τοπολογίας δικτύου και κατανόηση των Ροών Δεδομένων. (T0291)
Δεξιότητες	Απόκτηση γνώσης σχετική με την ασφάλεια των δικτύων, την ανάλυση της δικτυακής κίνησης, πολιτικών ασφαλείας και γενικότερα της σχεδίασης αρχιτεκτονικής ενός ασφαλούς δικτύου. (K0001, K0033, K0059, K0060, K0061, K0075, K0098, K0112, K0113, K0157, K0179, K0221, K0300, K0318, K0332)
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0011, K0029, K0255, K0296, K0516, K05555

Σενάριο 02 (SOC02) - Ενιαία Διαχείριση Απειλών

Οι συμμετέχοντες στην παρούσα άσκηση εμβαθύνουν στον τρόπο με τον οποίο λειτουργεί το Firewall, τις διαφορές ανάμεσα σε Network Protection, Intrusion Prevention και Sandboxing. Εκτός αυτών, εξοικειώνονται με την ανάλυση καταγραφών του Firewall και με τον τρόπο που αυτές προωθούνται στις λύσεις SIEM. **Τρόπος Υλοποίησης:** Checkpoint

UTM Μοντέλο 2200 με ενεργοποιημένες τις εξής προστασίες: Firewall, IPS/IDS, Anti-Bot, Anti-Virus, Threat Emulation, Monitoring, QOS

Πίνακας 4.2: Σενάριο 02: SOC02 UTM

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist
Κωδικός Ρόλου Εργασίας	PR-CDA-001, PR-INF-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF)
Κατηγορία Εργασίας	Protect and Defend (PR)
Γνώσεις	Χρήση εργαλείων με σκοπό την αναγνώριση και ανάλυση ειδοποιήσεων εισβολής, προσπάθειες εκμετάλλευσης ευπαθειών και εκτέλεση κακόβουλου λογισμικού.(T0023, T0088, T0259, T0260, T0290, T0295, T0297, T0310)
Δεξιότητες	Απόκτηση γνώσης σχετική με την ασφάλεια δικτύων, μοντέλο OSI, τοπολογία δικτύου, συστήματα ανίχνευσης και αποτροπής εισβολών καθώς επίσης και της σημαντικότητας ύπαρξης Firewall.(K0001, K0005, K0013, K0046, K0049, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0104, K0106, K0110, K0112, K0113, K0157, K0160, K0161, K0179, K0191, K0221, K0300, K0318, K0324, K0332, K0624).
Ικανότητες	Αναγνώριση προσπαθειών εκμετάλλευσης ευπαθειών και εισβολών στο δίκτυο όπως επίσης και ενδυνάμωση της ικανότητας ανάλυσης των πακέτων δικτύου.(S0020, S0025, S0027, S0036, S0078, S0096, S0156)
Προαπαιτούμενα	Ικανότητα αναγνώρισης εισβολών στο δίκτυο (A0128)
Επιπλέον KSAs που καλύπτονται	- K0009, K0100, K0115, K0187, K0189, K0314, K0326, K0392, K0471, K0481, K0488, K0634

Σενάριο 03 (SOC03) - Τοίχος Προστασίας Διαδικτυακών Εφαρμογών

Οι εκπαιδευόμενοι, κατανοούν τις διαφορές ανάμεσα σε επιθέσεις ανιχνευόμενες με την χρήση υπογραφών και επιθέσεις ανιχνευόμενες με την χρήση μοτίβου. Παράλληλα εμβαθύνουν στον τρόπο λειτουργίας των Web Service, και στους διαφορετικούς κωδικούς κατάστασης των εφαρμογών αυτών. Τέλος δίνεται η δυνατότητα να εξετάσουν πως ένα Web Application Firewall εντοπίζει πιο εξειδικευμένες επιθέσεις σε διαδικτυακές εφαρμογές. **Τρόπος Υλοποίησης** Εικονική μηχανή με λειτουργικό CentOS 8 και ενεργοποιημένο το Apache

Mod Security.

Πίνακας 4.3: Σενάριο 03: SOC03 WAF

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist
Κωδικός Ρόλου Εργασίας	PR-CDA-001, PR-INF-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF)
Κατηγορία Εργασίας	Protect and Defend (PR)
Γνώσεις	Χρήση εργαλείων με σκοπό την αναγνώριση και ανάλυση των ευπαθειών και του τρόπου εκμετάλλευσης αυτών στις διαδικτυακές εφαρμογές. (T0088, T0259, T0260)
Δεξιότητες	Απόκτηση γνώσης σχετική με τις επιθέσεις σε διαδικτυακές εφαρμογές καθώς επίσης και τρόπους αντιμετώπισης αυτών. (K0001, K0005, K0013, K0049, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0110, K0112, K0157, K0160, K0161, K0192, K0318, K0624).
Ικανότητες	Κατανόηση πως ένα Σύστημα Ασφαλείας λειτουργεί έτσι ώστε να αντιμετωπίζει επιθέσεις σε διαδικτυακές εφαρμογές. (S0027, S0036, S0078)
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0115, K0129, K0326, K0612, S0046

Σενάριο 04 (SOC04) & Σενάριο 05 (SOC05) - Domain Controller

Οι συμμετέχοντες του παραπάνω σεναρίου εμβαθύνουν στον τρόπο που δημιουργείται ένα Domain, στον τρόπο που οι χρήστες δημιουργούνται και πως αυτοί εντάσσονται στα Security Groups, ποια είναι τα Groups με αυξημένα δικαιώματα καθώς και το τι ρυθμίσεις μπορούν να οριστούν μέσω του Group Policy. **Τρόπος Υλοποίησης** Εικονικές Μηχανές με Λογισμικό Windows Server 2016 και ενεργοποιημένη την υπηρεσία Active Directory. (Μια εικονική Μηχανή πλήρως αναβαθμισμένη με τις ενημερώσεις ασφαλείας και μια χωρίς καμία εγκατεστημένη αναβάθμιση ασφαλείας).

Πίνακας 4.4: Σενάριο 04 & Σενάριο 05: SOC04 & SOC05 Domain Controller

Όνομα Ρόλου Εργασίας	System Administrator
Κωδικός Ρόλου Εργασίας	OM-ADM-001
Πεδίο Εξειδίκευσης	Systems Administration (ADM)
Κατηγορία	Operate and Maintain (OM)
Εργασίες	-
Γνώσεις	Απόκτηση γνώσης σχετική με τις μεθόδους αυθεντικοποίησης, πολιτικές ασφάλειας, τρόπους θωράκισης των συστημάτων του Οργανισμού, Πρωτόκολλα και πόρτες που χρησιμοποιούνται σε Windows Συστήματα καθώς επίσης και Διαχείριση Ευπαθειών στα εν λόγω συστήματα. (K0005, K0007, K0019, K0059, K0060, K0070, K0106, K0157, K0167, K0192, K0332).
Δεξιότητες	-
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0077, K0158, K0205, A0055, A0058

Σενάριο 06 (SOC06) & Σενάριο 07 (SOC07) - Web Server

Οι συμμετέχοντες στο σενάριο εξοικειώνονται στην εγκατάσταση IIS Web Server, τους ασφαλέστερους τρόπους παραμετροποίησης και τις διάφορες επιλογές στον Πίνακα Διαχείρισης. **Τρόπος Υλοποίησης** Εικονικές Μηχανές με Λογισμικό Windows Server 2012 και ενεργοποιημένη την υπηρεσία Internet Information Services (IIS). (Μια εικονική Μηχανή πλήρως αναβαθμισμένη με τις ενημερώσεις ασφαλείας και μια χωρίς καμία εγκατεστημένη αναβάθμιση ασφαλείας).

Πίνακας 4.5: Σενάριο 06 & Σενάριο 07: SOC06 & SOC07 Web Server

Όνομα Ρόλου Εργασίας	System Administrator
Κωδικός Ρόλου Εργασίας	OM-ADM-001
Πεδίο Εξειδίκευσης	Systems Administration (ADM)
Κατηγορία	Operate and Maintain (OM)
Εργασίες	-

Γνώσεις	Απόκτηση γνώσης σχετική με τρόπους θωράκισης των συστημάτων του Οργανισμού, Πρωτόκολλα και πόρτες που χρησιμοποιούνται σε Windows Συστήματα καθώς επίσης και Διαχείριση Ευπαθειών στα εν λόγω συστήματα. (K0005, K0059, K0060, K0070, K0106, K0167, K0192).
Δεξιότητες	-
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0077, K0105, K0205, K0398, A0055, A0058

Σενάριο 08 (SOC08) & Σενάριο 09 (SOC09) - File Server

Οι αναλυτές ασφάλειας εμβαθύνουν στον τρόπο που δίνονται τα δικαιώματα σε κοινόχρηστους φακέλους και πως η πρόσβαση από τους χρήστες καταγράφεται στα συστήματα ασφαλείας. Επιπλέον εξοικειώνονται στον τρόπο εντοπισμού μιας διαρροής δεδομένων ή επίθεση κρυπτογράφησης δεδομένων. **Τρόπος Υλοποίησης** Εικονικές Μηχανές με Λογισμικό Windows Server 2008 R2 και ενεργοποιημένη την File Server. (Μια εικονική Μηχανή πλήρως αναβαθμισμένη με τις ενημερώσεις ασφαλείας και μια χωρίς καμία εγκατεστημένη αναβάθμιση ασφαλείας).

Πίνακας 4.6: Σενάριο08 & Σενάριο 09: SOC08 & SOC09 File Server

Όνομα Ρόλου Εργασίας	System Administrator
Κωδικός Ρόλου Εργασίας	OM-ADM-001
Πεδίο Εξειδίκευσης	Systems Administration (ADM)
Κατηγορία	Operate and Maintain (OM)
Εργασίες	-
Γνώσεις	Απόκτηση γνώσης σχετική με τρόπους θωράκισης των συστημάτων του Οργανισμού, Πρωτόκολλα και πόρτες που χρησιμοποιούνται σε Windows Συστήματα καθώς επίσης και Διαχείριση Ευπαθειών στα εν λόγω συστήματα. (K0005, K0059, K0060, K0070, K0106, K0167, K0192).
Δεξιότητες	-
Ικανότητες	-
Προαπαιτούμενα	-

Επιπλέον KSAs που K0077, K0205, A0055, A0058
καλύπτονται

Σενάριο 10 (SOC10) & Σενάριο 11 (SOC11) - Database Server

Οι συμμετέχοντες εμβαθύνουν στον τρόπο λειτουργίας των βάσεων δεδομένων καθώς και της γλώσσας ερωτήσεων με σκοπό την αναγνώριση επιθέσεων τύπου SQL Injection. **Τρόπος Υλοποίησης** Εικονικές Μηχανές με Λογισμικό Windows Server 2012 και εγκατεστημένο SQL 2012 Έκδοση Developer. (Μια εικονική Μηχανή πλήρως αναβαθμισμένη με τις ενημερώσεις ασφαλείας και μια χωρίς καμία εγκατεστημένη αναβάθμιση ασφαλείας).

Πίνακας 4.7: Σενάριο10 & Σενάριο11: SOC10 & SOC11 Database Server

Όνομα Άσκησης	SOC10 & SOC11 Database Server
Όνομα Ρόλου Εργασίας	System Administrator
Κωδικός Ρόλου Εργασίας	OM-ADM-001
Πεδίο Εξειδίκευσης	Systems Administration (ADM)
Κατηγορία	Operate and Maintain (OM)
Εργασίες	-
Γνώσεις	Απόκτηση γνώσης σχετική με συστήματα Βάσεων Δεδομένων, τρόπους θωράκισης των συστημάτων του Οργανισμού, Πρωτόκολλα και πόρτες που χρησιμοποιούνται σε Windows Συστήματα καθώς επίσης και Διαχείριση Ευπαθειών στα εν λόγω συστήματα. (K0005, K0024, K0059, K0060, K0070, K0106, K0167, K0192).
Δεξιότητες	-
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0069, K0205, A0055, A0058

Σενάριο 12 (SOC12) - Mail Service

Οι εκπαιδευόμενοι αποκτούν γνώσεις σχετικές με το πρωτόκολλο SMTP καθώς επίσης και τον τρόπο αναγνώρισης και αντιμετώπισης περιστατικών Phishing. **Τρόπος Υλοποίησης** Office 365 Tenant

Πίνακας 4.8: Σενάριο 12: SOC12 Mail Service

Όνομα Ρόλου Εργασίας	System Administrator
Κωδικός Ρόλου Εργασίας	OM-ADM-001
Πεδίο Εξειδίκευσης	Systems Administration (ADM)
Κατηγορία	Operate and Maintain (OM)
Εργασίες	-
Γνώσεις	Απόκτηση γνώσης σχετική με τις τελευταίες τεχνολογίες και τους διαφορετικούς τρόπους επίθεσης σε Cloud υποδομή. (K0059).
Δεξιότητες	-
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0131, K0362, K0536

Σενάριο 13 (SOC13) - Mail Gateway

Στους εκπαιδευόμενους της παρούσας άσκησης παρουσιάζεται η ανάγκη για την προστασία της υποδομής ηλεκτρονικής αλληλογραφίας ενός οργανισμού και οι διάφοροι μηχανισμοί που μπορούν να επιτύχουν την προστασία της. **Τρόπος Υλοποίησης** Υπηρεσία Σύννεφου Check-point Harmony – Email & Office

Πίνακας 4.9: Σενάριο 13: SOC13 Mail Gateway

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist
Κωδικός Ρόλου Εργασίας	PR-CDA-001, PR-INF-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF)
Κατηγορία	Protect and Defend (PR)
Εργασίες	Χρήση εργαλείων με σκοπό την ανίχνευση και ανάλυση πιθανών ευπαθειών και τρόπων εκμετάλλευσης αυτών στο περιβάλλον ενός οργανισμού. (T0088, T0259, T0260).
Γνώσεις	Απόκτηση γνώσης σχετικές με τις τελευταίες τεχνολογίες προστασίας των οργανισμών από επιθέσεις στην Cloud υποδομή τους. (K0001, K0013, K0049, K0059, K0060, K0061, K0075, K0098, K0106, K0110, K0112, K0116, K0157, K0318).

Δεξιότητες	Εξειδίκευση στον τρόπο λειτουργίας των συστημάτων ασφαλείας ενός οργανισμού και στον τρόπο που μια αλλαγή στα συστήματα αυτά μπορεί να επηρεάσουν τον οργανισμό. (S0027, S0036).
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	-

Σενάριο 14 (SOC14) - Honeytrap/Deception Traps

Οι συμμετέχοντες της άσκησης, εμβαθύνουν στον τρόπο που μια συσκευή με τις κατάλληλες ρυθμίσεις μπορεί να δώσει στο Blue Team την δυνατότητα ανίχνευσης και εξουδετέρωσης μιας απειλής πριν αυτή επηρεάσει τον οργανισμό. **Τρόπος Υλοποίησης** Εικονική Μηχανή με εγκατεστημένο το λογισμικό Deception Grid.

Πίνακας 4.10: Σενάριο 14: SOC14 Honeytrap/Deception Traps

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst
Κωδικός Ρόλου Εργασίας	PR-CDA-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA)
Κατηγορία	Protect and Defend (PR)
Εργασίες	Χρήση εργαλείων με σκοπό τον εντοπισμό, ανάλυση και εξουδετέρωση μιας απειλής πριν αυτή επηρεάσει την υποδομή του υπό παρακολούθηση οργανισμού. (T0088, T0259).
Γνώσεις	Ο εκπαιδευόμενος αποκτά γνώσεις σχετικές με την ανίχνευση και ανάλυση κινδύνων πριν αυτοί αποτελέσουν απειλή για τον οργανισμό. (K0001, K0013, K0040, K0046, K0049, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0110, K0112, K0160, K0161, K0192, K0318).
Δεξιότητες	Εξειδίκευση στον τρόπο λειτουργίας των συστημάτων ασφαλείας ενός οργανισμού και στον τρόπο που μια αλλαγή στα συστήματα αυτά μπορεί να επηρεάσουν τον οργανισμό. (S0027, S0036).
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0115, K0174, K0453

Σενάριο 15 (SOC15) - SIEM

Οι εκπαιδευόμενοι αναλυτές περιστατικών ασφάλειας, εμβαθύνουν στο εργαλείο το οποίο είναι ικανό να συλλέγει καταγραφές από συστήματα εντός της υποδομής ενός οργανισμού, να συσχετίζει τις παραπάνω καταγραφές και να δημιουργεί ειδοποιήσεις όταν αναγνωρίζει κάποια απειλή. Παράλληλα οι αναλυτές εκπαιδεύονται στο να αναγνωρίζουν τότε αυτές οι ειδοποιήσεις αποτελούν ψευδώς αναγνωρισμένα περιστατικά ασφάλειας και τότε αυτές αφορούν πραγματικό περιστατικό ασφάλειας. **Τρόπος Υλοποίησης** Εικονική Μηχανή με εγκατεστημένο το IBM QRadar και ενσωματωμένη άδεια για 2500 καταγραφές το δευτερόλεπτο.

Πίνακας 4.11: Σενάριο 15: SOC15 SIEM

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst
Κωδικός Ρόλου Εργασίας	PR-CDA-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA)
Κατηγορία	Protect and Defend (PR)
Εργασίες	Χρήση εργαλείων με σκοπό την παρακολούθηση και ανάλυση καταγραφών ασφάλειας από διαφορετικές πηγές καθώς επίσης και επιβεβαίωση των ειδοποιήσεων ως περιστατικά ασφάλειας. (T0023, T0088, T0155, T0164, T0166, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0293, T0294, T0295, T0297, T0299, T0310, T0332, T0469, T0470, T0504).
Γνώσεις	Γενικότερες γνώσεις γύρω από τα διαφορετικά Λειτουργικά Συστήματα, Δικτύωση, Ανάλυση Ιομορφικού Λογισμικού και ανίχνευση απειλών στο δίκτυο ενός Οργανισμού κάνοντας χρήση των καταγραφών ασφάλειας. (K0001, K0013, K0040, K0046, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0107, K0110, K0142, K0143, K0160, K0161, K0177, K0192, K0301, K0318, K0332).
Δεξιότητες	Απόκτηση δεξιοτήτων αναγνώρισης περιστατικών ασφάλειας που παράγονται από την συσχέτιση καταγραφών. (S0027, S0036, S0063, S0078).
Ικανότητες	-
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0100, K0145, K0310, K0343, K0493, K0612, S0092, A0001

Σενάριο 16 (SOC16) - Kali Linux

Οι συμμετέχοντες αποκτούν γνώση σχετική με τα πιο κοινά εργαλεία που οι επιτιθέμενοι χρησιμοποιούν, ποιος είναι ο σκοπός του εκάστοτε εργαλείου και πως μπορεί μέσω των κατα-

γραφών ασφάλειας να αναγνωριστεί η χρήση τους. **Τρόπος Υλοποίησης** Φορητός Υπολογιστής με εγκατεστημένο το Kali Linux Distribution.

Πίνακας 4.12: Σενάριο 16: SOC16 Kali Linux

Όνομα Ρόλου Εργασίας	Cyber Defense Analyst, Vulnerability Assessment Analyst
Κωδικός Ρόλου Εργασίας	PR-CDA-001, PR-VAM-001
Πεδίο Εξειδίκευσης	Cybersecurity Defense Analysis (CDA)
Κατηγορία	Protect and Defend (PR)
Εργασίες	Ορισμός και κατανόηση των Εργαλείων Enumeration που υπάρχουν στο Kali Linux, αναγνώριση και εφαρμογή αντίμετρων σε περίπτωση χρήσης Εργαλείων Enumeration. (T0295).
Γνώσεις	Ενίσχυση της γνώσης σχετικά με τα Λειτουργικά Συστήματα Unix, τις μεθοδολογίες επίθεσης σε έναν Οργανισμό και των τρόπων που σκέφτεται και δρα ο επιτιθέμενος. (K0005, K0013, K0059, K0060, K0070, K0106, K0110, K0111, K0116, K0160, K0161, K0177, K0192, K0290, K0300, K0301, K0318, K0332, K0339, K0342, K0624).
Δεξιότητες	Απόκτηση δεξιοτήτων ώστε οι εκπαιδευόμενοι να είναι σε θέση να κατανοήσουν την μεθοδολογία ενός επιτιθέμενου καθώς επίσης και τα εργαλεία που μπορεί να χρησιμοποιήσει. (S0057, S0078, S0156, S0167).
Ικανότητες	Ενίσχυση της ικανότητας του εκπαιδευόμενου να αναγνωρίζει καινούριες τεχνικές επίθεσης σε έναν Οργανισμό όπως επίσης να είναι σε θέση να αναγνωρίσει πως ο επιτιθέμενος μπορεί να εκμεταλλευτεί ευπάθειες στα συστήματα του Οργανισμού. (A0015, A0159).
Προαπαιτούμενα	-
Επιπλέον KSAs που καλύπτονται	K0009, K0115, K0119, K0129, K0131, K0187, K0189, K0234, K0296, K0310, K0314, K0362, K0392, K0480, K0481, K0493, K0536, K0634, A0055, A0107

Κεφάλαιο 5

Συμπεράσματα

Έχοντας παρουσιάσει τις τεχνικές προδιαγραφές του σχεδιασμού των σεναρίων, σε αυτό το κεφάλαιο περιγράφονται τα αποτελέσματα της αξιολόγησης και τα συμπεράσματα ολοκληρώνοντας την εργασία.

Ο τρόπος που θα υπολογιστεί η αποτελεσματικότητα των σεναρίων είναι με την χρήση εξίσωσης η οποία σαν αριθμητή θα έχει τον αριθμό των Εργασιών (T), Γνώσεων (K), Δεξιοτήτων (S) που καλύπτονται στα σενάρια ανά ρόλο εργασίας και σαν παρανομαστή το σύνολο των TKS που αναφέρονται στο NICE για τον αντίστοιχο ρόλο εργασίας με αναγωγή στα 100 για να είναι πιο εύκολη η κατανόηση του. Η αξιολόγηση μπορεί να χρησιμοποιηθεί για να εντοπίσει ελλείποντα στοιχεία στα σενάρια και να παρέχει προτάσεις για ενημερώσεις ή επεκτάσεις, προκειμένου να βελτιωθεί η αποτελεσματικότητά τους στη διδασκαλία των εννοιών της κυβερνοασφάλειας. Στον πίνακα 5.1 αποτυπώνονται συνοπτικά τα αποτελέσματα για κάθε έναν από τους ρόλους.

Ρόλος Εργασίας	Εργασίες	Γνώσεις	Δεξιότητες
PR-CDA-001	67.7%	64.3%	73.3%
OM-ADM-001	55.6%	44.8%	78.6%
OM-NET-001	72.7%	30.8%	54.5%
PR-INF-001	33.3%	54.2%	44.4%
PR-VAM-001	0%	45.7%	50%

Πίνακας 5.1: Αντιστοίχιση της κάλυψης της πλατφόρμας κυβερνοάμυνας με το πλαίσιο NICE για τους πιο σχετικούς ρόλους εργασίας.

Παρατηρούμε πως το περιβάλλον που δημιουργήθηκε καλύπτει επαρκώς τους Εργασιακούς Ρόλους PR-CDA-001 και OM-ADM-001. Για παράδειγμα, ο Εργασιακός Ρόλος PR-CDA-001 καλύπτεται από 7 σενάρια (SOC01, SOC02, SOC05, SOC13-SOC16). Οι συνολικές Εργασίες (T) που καλύπτονται από αυτά τα 7 σενάρια περιλαμβάνουν 23 Εργασίες (T) από τις συνολικά 34 που απαιτεί ο Εργασιακός Ρόλος PR-CDA-001, και συνεπώς η κάλυψη φτάνει το 67,64%. Από την άλλη πλευρά, προκύπτει πως δεν υπάρχει η απαραίτητη κάλυψη για τον Εργασιακό Ρόλο PR-VAM-001.

Καταλήγουμε στο συμπέρασμα ότι η ενημέρωση των σεναρίων και η ενσωμάτωση των ελλειπόντων TKS είναι απαραίτητη για την πλήρη κάλυψη των παραπάνω Εργασιακών Ρόλων. Για παράδειγμα, θα μπορούσε να συμπεριληφθούν περισσότερες Εργασίες (T) σχετικά με τη διαχείριση απειλών και ευπαθειών (ενδεικτικά οι T0178, T0292, T0526), την αφαίρεση κακόβουλου λογισμικού (ενδεικτικά η T0296), την ανάλυση δικτύου (ενδεικτικά οι T0043, T0298), την αναφορά και τη μείωση κινδύνων (ενδεικτικά οι T0178, T0548). Τα παραπάνω μπορούν να ενσωματωθούν εύκολα με την προσθήκη επιχειρησιακών διαδικασιών και μη τεχνικών εργασιών. Ωστόσο, οι Εργασίες (T) που είναι δύσκολο να ενσωματωθούν στην πλατφόρμα αφορούν αυτές που απαιτούν εργασία σε φυσικό εξοπλισμό. Για παράδειγμα, στον Ρόλο Εργασίας OM-ADM-001, οι εργασίες που απαιτούν φυσικό εξοπλισμό περιλαμβάνουν τις εργασίες T0514—Διάγνωση ελαττωματικού υλικού συστήματος/διακομιστή και T0515—Επισκευή ελαττωματικού υλικού συστήματος/διακομιστή.

Συνοψίζοντας, η πλήρης κάλυψη των Εργασιακών Ρόλων είναι μια πρόκληση· ωστόσο, με την ενσωμάτωση των ανθρώπινων στοιχείων και την ενημέρωση των σεναρίων χρησιμοποιώντας τα ελλείποντα TKS, η πλατφόρμα κυβερνοάμυνας θα μπορούσε να προσφέρει μια πιο ολοκληρωμένη και ρεαλιστική προσομοίωση, καλύπτοντας ένα ευρύτερο φάσμα δεικτών ικανότητας. Σε αυτό το πλαίσιο, το πλαίσιο NICE έχει αποδειχθεί χρήσιμο για τον εντοπισμό κενών ή ελλείψεων.

Βιβλιογραφία

- [1] Tejaswini C Herath, Hemantha SB Herath, and David Cullum. “An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks”. In: *Information Systems Frontiers* 25.2 (2023), pp. 681–721.
- [2] R Petersen et al. “National initiative for cybersecurity education (NICE) cybersecurity workforce framework”. In: *NIST Spec. Publ.* 800 (2020), p. 181.
- [3] Jan Vykopal et al. “Scalable learning environments for teaching cybersecurity hands-on”. In: *2021 IEEE Frontiers in Education Conference (FIE)*. IEEE. 2021, pp. 1–9.
- [4] Jan Vykopal, Valdemar Švábenský, and Ee-Chien Chang. “Benefits and pitfalls of using capture the flag games in university courses”. In: *Proceedings of the 51st ACM Technical symposium on computer science education*. 2020, pp. 752–758.
- [5] Nestoras Chouliaras et al. “Cyber ranges and testbeds for education, training, and research”. In: *Applied Sciences* 11.4 (2021), p. 1809.
- [6] Enrico Russo, Gabriele Costa, and Alessandro Armando. “Scenario design and validation for next generation cyber ranges”. In: *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*. IEEE. 2018, pp. 1–4.
- [7] Jan Vykopal et al. “Lessons learned from complex hands-on defence exercises in a cyber range”. In: *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE. 2017, pp. 1–8.
- [8] Manfred Vielberth et al. “A digital twin-based cyber range for SOC analysts”. In: *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer. 2021, pp. 293–311.

- [9] Maurice Dawson, Pedro Taveras, and Danielle Taylor. “Applying software assurance and cybersecurity NICE job tasks through secure software engineering labs”. In: *Procedia Computer Science* 164 (2019), pp. 301–312.
- [10] Jan Hajny et al. “Framework, tools and good practices for cybersecurity curricula”. In: *IEEE Access* 9 (2021), pp. 94723–94747.
- [11] Diana Burley et al. “Curriculum guidelines for post-secondary degree programs in cybersecurity”. In: *Cybersecurity Curricula 2017* (2017).
- [12] Chad M Dewey and Chad Shaffer. “Advances in information security education”. In: *2016 IEEE International Conference on Electro Information Technology (EIT)*. IEEE. 2016, pp. 0133–0138.
- [13] Razvan Beuran et al. “Integrated framework for hands-on cybersecurity training: CyTrONE”. In: *Computers & Security* 78 (2018), pp. 43–59.
- [14] Martin Shimba, Michael PJ Mahenge, and Camilius A Sanga. “Virtual labs versus hands-on labs for teaching and learning computer networking: A comparison study”. In: *International Journal of Research Studies in Educational Technology* 6.1 (2017), pp. 43–58.
- [15] Yuli Deng et al. “Personalized learning in a virtual hands-on lab platform for computer science education”. In: *2018 IEEE Frontiers in education conference (FIE)*. IEEE. 2018, pp. 1–8.
- [16] Yanyan Li and Mengjun Xie. “Platoon: A virtual platform for team-oriented cybersecurity training and exercises”. In: *Proceedings of the 17th Annual Conference on Information Technology Education*. 2016, pp. 20–25.
- [17] Yuli Deng et al. “Knowledge graph based learning guidance for cybersecurity hands-on labs”. In: *Proceedings of the ACM conference on global computing education*. 2019, pp. 194–200.
- [18] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture”. In: *Computers & Security* 88 (2020), p. 101636.
- [19] Polina Zilberman et al. “Sok: A survey of open-source threat emulators”. In: *arXiv preprint arXiv:2003.01518* (2020).

- [20] Mauro Andreolini et al. “A framework for the evaluation of trainee performance in cyber range exercises”. In: *Mobile Networks and Applications* 25.1 (2020), pp. 236–247.
- [21] JD Work. “In wolf’s clothing: Complications of threat emulation in contemporary cyber intelligence practice”. In: *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE. 2019, pp. 1–8.
- [22] Z Cliffe Schreuders et al. “Hackerbot: Attacker Chatbots for Randomised and Interactive Security Labs, Using {SecGen} and {oVirt}”. In: *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. 2018.
- [23] Tom Chothia and Chris Novakovic. “An Offline Capture The {Flag-Style} Virtual Machine and an Assessment of Its Value for Cybersecurity Education”. In: *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*. 2015.
- [24] Valdemar Švábenskỳ et al. “Cybersecurity knowledge and skills taught in capture the flag challenges”. In: *Computers & Security* 102 (2021), p. 102154.
- [25] Oliver Nock, Jonathan Starkey, and Constantinos Marios Angelopoulos. “Addressing the security gap in IoT: towards an IoT cyber range”. In: *Sensors* 20.18 (2020), p. 5439.
- [26] Sagar Rahalkar, Rahalkar, and Karkal. *Quick Start Guide to Penetration Testing*. Springer, 2019.
- [27] Eric W Burger et al. “Taxonomy model for cyber threat intelligence information exchange technologies”. In: *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*. 2014, pp. 51–60.
- [28] Raphael Hertzog, Jim O’Gorman, and Mati Aharoni. “Kali linux revealed”. In: *Mastering the Penetration Testing Distribution* (2017).
- [29] Marietheres Dietz, Manfred Vielberth, and Günther Pernul. “Integrating digital twin security simulations in the security operations center”. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 2020, pp. 1–9.
- [30] VN Harikrishnan and GT Kumar. “Advanced persistent threat analysis using Splunk”. In: *International Journal of Pure and Applied Mathematics* 118.20 (2018), pp. 3761–3768.

- [31] Bingdong Li et al. “A survey of network flow applications”. In: *Journal of Network and Computer Applications* 36.2 (2013), pp. 567–581.
- [32] Maria Stoyanova et al. “A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues”. In: *IEEE Communications Surveys & Tutorials* 22.2 (2020), pp. 1191–1221.
- [33] D Paul Joseph and Jasmine Norman. “An analysis of digital forensics in cyber security”. In: *First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018*. Springer. 2019, pp. 701–708.
- [34] Maxim Chernyshev et al. “Internet of things forensics: The need, process models, and open issues”. In: *IT professional* 20.3 (2018), pp. 40–49.
- [35] T Man et al. “A decision support system for DM algorithm selection based on module extraction”. In: *Procedia Computer Science* 186 (2021), pp. 529–537.
- [36] Rodney Petersen et al. “Workforce framework for cybersecurity (NICE framework)”. In: (2020).
- [37] Jean RS Blair et al. “Infusing principles and practices for secure computing throughout an undergraduate computer science curriculum”. In: *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education*. 2020, pp. 82–88.
- [38] Matthew Hudnall. “Educational and workforce cybersecurity frameworks: comparing, contrasting, and mapping”. In: *Computer* 52.3 (2019), pp. 18–28.