ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ & ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σύστημα Cyber Range: Εγκατάσταση και πειραματισμός

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Ιωάννη Μ. Ντεμογιάννη

Επιβλέπων: Δρ. Κωνσταντίνος Μαλιάτσος

Μέλη εξεταστικής επιτροπής:

Δρ. Μαρία Καρύδα

Δρ. Κωνσταντίνος Λαμπρινουδάκης

Σάμος, Μάρτιος 2023

Πρόλογος και ευχαριστίες

Η εκπόνηση της παρούσας διπλωματικής εργασίας πραγματοποιήθηκε στο πλαίσιο του Προγράμματος Μεταπτυχιακών Σπουδών στην *Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων* του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου.

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντά μου, Επίκουρο Καθηγητή Δρ. Κωνσταντίνο Μαλιάτσο για την εμπιστοσύνη που μου έδειξε. Η υποστήριξη και η διαθεσιμότητά του κατά τη διάρκεια εκπόνησης της εργασίας, αλλά και η καθοδήγησή και συμβουλές του αποτέλεσαν σπουδαία βοήθεια για την ολοκλήρωσή της.

Θα ήθελα επίσης να ευχαριστήσω την οικογένεια και τους φίλους μου, για την αμέριστη αγάπη και κατανόησή τους, που παρά το γεγονός ότι τους αφιέρωσα λιγότερο χρόνο κατά τη διάρκεια των σπουδών μου, η υποστήριξή τους ήταν ένθερμη και με βοήθησαν να ολοκληρώσω το εγχείρημά μου αυτό.

© 2023
του
Ιωάννη Μ. Ντεμογιάννη
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Λάθε βιώσας

Επίκουρος

***Λάθε** : Επικ. Αντί έλαθε, γ' ενικ. αορ. β ΄ του λανθάνω.*

Λανθάνω και λήθω : στους περισσότερους ενεργ. χρόνους , διαφεύγω της προσοχής κάποιου, παραμένω άγνωστος, αόρατος, απαρατήρητος.

***Βιώσας** : - βίωσις, - έως , ή (βιόω) τρόπος ζωής σε Κ.Δ.*

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

In the present thesis the concept of cyber ranges is studied along with their usage in training purposes for cybersecurity topics. The increased skill demand in the cybersecurity job market combined with the rise of complex and highly specialized cyber attacks, poses the need for proper tooling for cyber security professionals and researchers which can be used for training purposes. This will allow them to keep up with the state of the art techniques and methodologies. A solution to this issue, can be Cyber Ranges, since they offer a complete platform solution for training against complex cyber attack scenarios and can support simulations of complex infrastructure.

A literature review with the most common cyber ranges is presented and extended comparison studies are cited. The basic types of cyber ranges are presented among with their architecture, the benefits from using them, especially for education.

Within the scope of the thesis was an implementation of an open-source CR, KYPO Lite. The architecture of KYPO Cyber Range Platform, and its component structure as well as the related terminology is presented. Moreover, the creation of a training scenario is presented by using the platform. Finally, the usage of Infrastructure as Code in complex CR environments is discussed.

Keywords: Cyber Range, cyber range training, cyber range assessment, simulation environments, KYPO CRP, KYPO CRP Lite, cybersecurity training, threat intelligence, security automation and orchestration, ansible, terraform, google cloud platform

Περίληψη

Η παρούσα εργασία μελετά την έννοια των cyber ranges (πεδία δοκιμών κυβερνοασφάλειας) και τη χρήση τους στην παροχή εκπαίδευσης για θέματα κυβερνοασφάλειας. Η αυξημένη σε απαιτήσεις γνώσεων αγορά εργασίας της κυβερνοασφάλειας σε συνδυασμό με την έξαρση πολύπλοκων και εξειδικευμένων κυβερνοεπιθέσεων, απαιτεί και κατάλληλα εργαλεία με τα οποία οι εκάστοτε ερευνητές ή μηχανικοί ασφάλειας θα μπορούν να εκπαιδευτούν για να ανταπεξέλθουν. Μία λύση στο πρόβλημα αυτό, μπορούν να παρέχουν τα Cyber Ranges, καθώς παρέχουν λύσεις υπό τη μορφή πλατφόρμας, που επιτρέπουν την εκπαίδευση απέναντι σε πολύπλοκα σενάρια επιθέσεων ακόμη σε πολύπλοκες υπολογιστικές υποδομές.

Μελετώνται τα είδη Cyber Ranges διαθέσιμα στη βιβλιογραφία και παρατίθενται διαθέσιμες εκτενέστερες συγκριτικές μελέτες. Περιγράφονται τα βασικά είδη cyber ranges, η αρχιτεκτονική τους, τα οφέλη τους και οι λόγοι που τα κάνουν ελκυστικά για θέματα εκπαίδευσης.

Στα πλαίσια της εργασίας επιλέχθηκε η υλοποίηση ενός ανοιχτού κώδικα CR, του KYPO Lite. Περιγράφεται η αρχιτεκτονική υλοποίησης KYPO Cyber Range Platform, και ο τρόπος με τον οποίο ορίζονται τα επιμέρους στοιχεία της πλατφόρμας CR, όπως και η σχετική του ορολογία. Επιπλέον, περιγράφεται η δημιουργία ενός εκπαιδευτικού σεναρίου μέσα στην πλατφόρμα. Τέλος αναδεικνύεται η σημασία χρήσης τεχνολογιών Infrastructure as Code για πολύπλοκα περιβάλλοντα CR.

Keywords: Cyber Range, cyber range training, cyber range assessment, simulation environments, KYPO CRP, KYPO CRP Lite, cybersecurity training, threat intelligence, security automation and orchestration, ansible, terraform, google cloud platform

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας Περιεχομένων

Πρόλογος και ευχαριστίες 2

Abstract 5

Περίληψη 6

Πίνακας Περιεχομένων 8

Λίστα Πινάκων 10

Λίστα Εικόνων 11

Ακρωνύμια 14

1. Εισαγωγή 16

2. Cyber Ranges (πεδία δοκιμών κυβερνοασφάλειας) 19

2.1 Οφέλη της εκπαίδευσης σε Cyber Ranges και πεδία εφαρμογής 24

2.2 Είδη Cyber Ranges 27

2.3 Αρχιτεκτονικός σχεδιασμός Cyber Ranges 30

2.4 Αρχιτεκτονικές CR και Test-beds 32

3. Kypo Cyber Range (CRP) 39

3.1 Αρχιτεκτονικός σχεδιασμός KYPO CRP 40

3.2 Εξομοιωμένο εικονικό περιβάλλον (emulated virtual environment) στο KYPO 43

3.3 KYPO Sandbox definition 43

3.4 KYPO Topology Definition 44

3.5 KYPO Topology Instance 47

3.6 KYPO Topology Instance Management 48

3.7 KYPO Sandbox Provisioning και Sandbox Access 48

4. Εκπαίδευση με χρήση του KYPO CRP και περιγραφή ορολογίας 54

4.1 Δημιουργία εκπαιδευτικού σεναρίου σε KYPO 58

4.2 Ροή διεργασίας εκπαίδευσης - τοπική (local) υλοποίηση 61

5. Συζήτηση – συμπεράσματα 67

6. Αναφορές 69

7. Παράρτημα.....76

a. Εγκατάσταση KYPO Lite σε GCP.....76

b. Στιγμιότυπα από το dashboard του GCP για το project kypo-lite23.....81

c. Προβλήματα εγκατάστασης στην περίπτωση χρήσης του Openstack και KYPO σε VMware ή Azure περιβάλλον.....82

Λίστα Πινάκων

Πίνακας 1: Συνοπτικός πίνακας με σχετικές εργασίες στη βιβλιογραφία και σύγκριση βασικών χαρακτηριστικών Cyber Ranges [26].....22

Λίστα Εικόνων

Εικόνα 1: Βασικό περιβάλλον CR (Cyber Range)[22].....24
Εικόνα 2: Infosec Wheel, περιγράφει τις αλληλοεπιδράσεις μεταξύ των "ομάδων" και των ρόλων που σχηματίζονται για διασφάλιση και διαχείριση της ασφάλειας πληροφοριακών συστημάτων [61].....25
Εικόνα 3: Physical CR [22] 28
Εικόνα 4: Τρόπος ταξινόμησης των test beds σύμφωνα με τους Ukwandu et al., όπου ως κριτήριο χρησιμοποιούνται τα μοντέλα λετουργίας, ο τύπος τους, ο τρόπος και η φύση των εκπαιδευτικών σεναρίων που επεξεργάζονται και οι δυνατότητες ανάλυσης. [30] 30
Εικόνα 5: Τρόπος ταξινόμησης Cyber Ranges σύμφωνα με τα χαρακτηριστικά που χρησιμοποιήθηκαν από τους Ukwandu et al., μεταξύ άλλων, διαχωρίζουν τα cyber ranges βάσει το είδους τους (physical, simulation, κλπ) του επιστημονικού ή εμπορικού πεδίου εφαρμογής, το είδος της εκπαίδευσης που παρέχουν και του δυναμικού ή στατικού τους χαρακτήρα. [30] 29
Εικόνα 6: Αρχιτεκτονικά στοιχεία ενός CR (Cyber Range)[22] 31
Εικόνα 7: Περιγραφή των στοιχείων ενός Test-bed [30].....32
Εικόνα 8: Αρχιτεκτονικός σχεδιασμός ενός Cyber Range [30].....33
Εικόνα 9: Περιγραφή αρχιτεκτονικής εικονοποίησης (Virtualization) [30].....33
Εικόνα 10: OpenNebula αρχιτεκτονική [22] 34
Εικόνα 11: Προσομοίωση RTDS (Real Time Digital Simulator) [22].....35
Εικόνα 12: Υβριδική αρχιτεκτονική Cyber Range [30].....36
Εικόνα 13: Απεικόνιση ενός βασικού μοντέλου περιγραφής των στοιχείων ενός Cyber Range κατά Yamin et al., όπου λαμβάνονται 5 κύριοι τύποι στοιχείων υπόψη, η διαχείριση, το color teaming, scoring, το σενάριο και το monitoring του περιβάλλοντος CR.[32].....36
Εικόνα 14: Αναβαθμισμένος τρόπος ταξινόμησης των Cyber Ranges σύμφωνα με τους Yamin et al. με τη διαφορά ότι λαμβάνεται υπόψη το περιβάλλον υλοποίησης και οι εκπαιδευτικές ιδιότητες του συστήματος, αλλά και εκτενέστερα στοιχεία στα επιμέρους κύρια κριτήρια.[32] 37
Εικόνα 15 Αρχιτεκτονικός σχεδιασμός ΚΥΡΟ CRP 42
Εικόνα 16: Απεικόνιση του Topology Instance Definition [71].....45
Εικόνα 17: Περιγραφή ενός pool υπολογιστικών στοιχείων, όπου διακρίνεται η συσχέτιση και το επίπεδο του sandbox definition, του sandbox και πως συγκροτούν ένα pool.[68] 45

Εικόνα 18: Παράδειγμα κώδικα σε yaml, όπου περιγράφει τη δημιουργία ενός sandbox, με τα δομικά στοιχεία του και τις πληροφορίες απαραίτητες στην πλατφόρμα OpenStack.....46
Εικόνα 19: Απεικόνιση της δομής ενός KYPO Topology Instance, όπου ιακρίνεται η βασική υποδομή που απαιτεί το KYPO, το διαχειριστικό επίπεδο και ο ορισμός που περιγράφει την αλληλεπίδραση των instances.....47
Εικόνα 20: Block κώδικα ansible σε yaml, που περιγράφει την υλοποίηση και provisioning των υπολογιστικών πόροων για τη διημιουργία ενός sandbox στο KYPO CRP. Ορίζονται διευθύνσεις IP, τα κύρια στοιχεία του KYPO, όπως kypo-proxy jump, το δίκτυο man, και οι ρυθμίσεις δικτύου και διαχείρισης.....50
Εικόνα 21: Τοπολογία βασικής υποδομής KYPO CRP, αποτελείται από έναν κύριο server KYPO Head, ένα proxy, KYPO PROXY και ένα δίκτυο, KYPO base network.[72].....52
Εικόνα 22: Στοιχεία πλατφόρμας KYPO, όπου χρησιμοποιείται η αρχιτεκτονική των microservices.[73].....53
Εικόνα 23: Αρχική σελίδα (homepage) του KYPO CRP [74].....55
Εικόνα 24: Στιγμιότυπο αρχικής σελίδας ενός εκπαιδευόμενου στο KYPO.....55
Εικόνα: 25 Στιγμιότυπο (2) εκπαιδευόμενου στο KYPO.....56
Εικόνα 26: Στιγμιότυπο διαχειιστικού πάνελ του εκπαιδευτή στην πλατφόρμα KYPO.....56
Εικόνα 27: Adaptive format της εκπαίδευσης με KYPO.Δίνεται η δυνατότητα να προσαρμόζεται στο επίπεδο του εξεταζόμενου. A: το ερηματολόγιο πριν την έ έναρξη της εκπαίδευσης, PD το υπολογιστικό μοντέλο και Q, το ερωτηματολόγιο με το πέρας της εκαπίδευσης. 57
Εικόνα 28: Στιγμιότυπο στην προβολή εκπαιδευτή από σε εξέλιξη εκπαίδευση CTF εκπαίδευσης με KYPO.....57
Εικόνα 29: Training Workflow - Cloud.....59
Εικόνα 30: Ενέργειες/διεργασίες κατά την εκπαίδευση με KYPO 60
Εικόνα 31: Δημιουργία sandboxes σε local training workflow.....61
Εικόνα 32: Περιγραφή δημιουργίας σεναρίου εκπαίδευσης σε τοπική υλοποίηση[80].....63
Εικόνα 33: Γραφική αναπαράσταση "γραμμικής" εκπαίδευσης με KYPO[81].....64
Εικόνα 34: Γραφική αναπαράσταση "προσαρμοστικής" (adaptive) εκπαίδευσης με KYPO [82] 65
Εικόνα 35: Γραφική αναπαράσταση της διασύνδεσης μεταξύ σεναρίων εκπαίδευσης και sandboxes.....66
Εικόνα 36: Dashboard Google Cloud Platform, project overview.....81

Εικόνα 37: GCP CPU Utilization, σε αδρανή κατάσταση (idle), η εγκατάσταση κατάναλώνει πραγματικά περίπου το 40% των δεσμευμένων vCPU, κάτι που στο σενάριο υλοποίησής μας ήταν αναμενώμενο, καθώς φόρτος υπάρχει μόνο κατά τη διάρκειεα εκτέλεσης σεναρίων εκπαίδευσης. Είναι χαρακτηριστικό παράδειγμα overutilization, που μπορεί να οδηγήσει σε over-provisioning πόρων και κατά συνέπεια σε αυξημένο συνολικό κόστος. Προτείνεται on-demand/ad-hoc provisioning σε τέτοιες υλοποιήσεις για να αποφευχθούν τα παραπάνω προβλήματα.....81
Εικόνα 38: Εκτίμηση-Πρόβλεψη κόστους για τη χρήση των υπολογιστικών πόρων (compute-engine) και των πόρων αποθηκευτικού χώρου (storage-engine). Το κόστος χρήσης του βασικής υλοποίησης KYPO-lite, κυμαίνεται στα 12€ ημερησίως, μη λαμβάνοντας υπόψη το ενδεχόμενο υπερβολικής τηλεπικοινωνιακής κίνησης από και προς το σύστημα. 81

Ακρωνύμια

AI	Artificial Intelligence
API	API Application Programming Interface
APT	Advanced Persistent Threat
CONCORDIA	CONCORDIA Cybersecurity cOmpeteNCe fOr Research anD InnovAtion
CR	Cyber Range
CRP	CRP Cyber Range Platform
CSA	Cyber Situational Awareness
DoS	Denial of Service
EC2	Elastic Compute Cloud
ECSO	European Cyber Security Organization
GCP	Google Cloud Platform
ICT	Information Communication Technology
IoT	Internet of Things
ISMS	Information Security Management System
IT	Information Technology
KYPO	Στα Τσέχικα: Kybernetická Polygon (Cybersecurity Polygon)
MitM	Man in the Middle
NIST	Natural Institute of Standards and Technology
OCA	OpenNebula Cloud API
OCCI	Open Cloud Computing Interface
OT	Operation Technology
PHIL	Power Hardware in Loop
RaaS	Ransomware-as-a-Service
RBAC	Role Based Access Control
RDP	Remote Desktop Protocol
RTDS	Real-Time Digital Simulator
SA	Situational Awareness
SSH	Secure Shell Protocol
VM	Virtual Machine
VNC	Virtual Network Computing
WAN	Wide Area Network
YAML	Yet Another Markup Language
TB	Test Beds

1. Εισαγωγή

Τα τελευταία χρόνια οι κυβερνοεπιθέσεις έχουν εξελιχθεί τόσο, ώστε να προσφέρονται πλέον ως υπηρεσία και με πληθώρα επιλογών διαθέσιμες μετά από απλή αναζήτηση στο dark web (σκοτεινό διαδίκτυο). Οι επιθέσεις είναι εξεζητημένες και προαπαιτούν πια εξεζητημένες γνώσεις, με τις επιθέσεις να κόβονται και να ράβονται ανάλογα με τον εκάστοτε στόχο. Θα ήταν αφελές να υποθέσουμε ότι συγκεκριμένοι τομείς οικονομικής δραστηριότητας παραμένουν ασφαλείς από κυβερνοεπιθέσεις, καθώς όλο και περισσότερο, ακόμη και οι μικρότερες επιχειρήσεις μπαίνουν στο στόχαστρο κακόβουλων ενεργειών, συνήθως για επιθέσεις που αποσκοπούν σε χρηματικές αμοιβές από εκβιασμό. Αναφορές δείχνουν ότι στο σκοτεινό διαδίκτυο (dark web) κάποιος μπορεί να αγοράσει κακόβουλο λογισμικό (malware) ακόμη και σε τιμή μικρότερη των 10 δολαρίων, με το κυβερνοέγκλημα να γίνεται όλο και πιο οργανωμένο και να έχει υιοθετήσει τη χρήση κρυπτονομισμάτων [1]. Καταλήγουμε στη θλιβερή διαπίστωση στις μέρες μας ότι μιλάμε πλέον για την ύπαρξη κυβερνοεγκλήματος ως υπηρεσία (cybercrime-as-a-service). Κύριο χαρακτηριστικό τους, η χρήση εξεζητημένης και πολύπλοκης τεχνολογίας με συγκεκριμένο στόχο. Οι πιθανές ζημίες μίας επιχείρησης από μία ενδεχόμενη επίθεση είναι στο επίκεντρο κάθε εκτίμησης και ανάλυσης ρίσκου απέναντι σε κυβερνοαπειλές. Ως κύριο πρόβλημα αναδεικνύονται οι επιθέσεις εφοδιαστικής αλυσίδας και η τάση του Ransomware-as-a-Service (RaaS) [4][5], που εκτιμάται ότι θα παραμείνει σαν πρώτη επιλογή για τους επιτιθέμενους και για το 2023 [4]–[8]. Οι ειδικοί επίσης προειδοποιούν ότι στο μέλλον δυστυχώς αναμένεται να συναντήσουμε και AI-for-cybercrime-as-a-service.Το AI ήδη χρησιμοποιείται στην κατασκευή malware, αποδεδειγμένα καταφέρνει να διαπεράσει δικλείδες ασφαλείας όπως το CAPTCHA και βρίσκει πεδίο εφαρμογής στην κατασκευή deep fakes.[9], [10] Δεν είναι εφικτό να ελεγχθεί πως θα χρησιμοποιηθεί η τεχνολογία για κακόβουλη ενέργειες. Με τη συχνότητα των κυβερνοεπιθέσεων να αυξάνεται τα τελευταία χρόνια η ανάγκη για ειδικούς σε θέματα ασφάλειας καθίσταται προφανής [1], [11], [12].

Παρατηρούμε ότι η ενημέρωση και ευαισθητοποίηση σχετικά με την ασφάλεια των πληροφοριακών συστημάτων έχει φτάσει σε ένα επίπεδο ωριμότητας όπου οι περισσότερες εταιρείες έχουν στο επίκεντρο του ενδιαφέροντος τους την ανάγκη υλοποίησης ασφαλών πληροφοριακών συστημάτων και ασφαλούς περιβάλλοντος εργασίας. Η κοινή γνώμη αντιμετωπίζει όλο και περισσότερο έννοιες όπως «κυβερνοεπιθέσεις» και η εκπαίδευση μηχανικών και επιστημόνων Πληροφορικής επικεντρώνεται τα τελευταία χρόνια στην ασφάλεια των πληροφοριακών συστημάτων. Εκτιμήσεις δείχνουν ότι η αγορά της ασφάλειας πληροφοριακών συστημάτων θα αγγίξει τα 376 δις δολάρια μέχρι το 2029, με την αξία της για

το 2021 να είναι περί τα 140 δις δολάρια και το 2022 να έχει ξεπεράσει τα 155 δις δολάρια [13], [14]. Ωστόσο, οι αναλύσεις για την αγορά εργασίας των επιστημόνων Ασφάλειας πληροφοριών και συστημάτων δείχνουν ότι παρά την αυξημένη ζήτηση από εταιρείες ανεξαρτήτου αντικειμένου, η προσφορά και η διαθεσιμότητα εργατικού δυναμικού σε υψηλής εξειδίκευσης επαγγελματίες είναι μειωμένη και θα συνεχίσει να έχει καθοδική τάση.

Οι προβλέψεις για τα διαθέσιμα ταλέντα και δεξιότητες είναι ότι θα παραμείνουν σε έλλειψη και οι ανάγκες των εταιρειών θα είναι αδύνατο να καλυφθούν [15], [16]. Όπως είναι αναμενόμενο, οι εξεζητημένοι τρόποι επίθεσης απαιτούν και αντίστοιχα εξεζητημένες άμυνες. Αποδεικνύεται δυστυχώς ότι πολλές φορές μία βασική εκπαίδευση στην κυβερνοασφάλεια είναι ανεπαρκής, λόγω του συνεχώς μεταβαλλόμενου περιβάλλοντος απειλών (threat landscape)[17]. Με το γρήγορο ρυθμό που αναπτύσσονται οι τεχνικές επίθεσης και κατά συνέπεια οι τεχνικές άμυνας, η γνώση και οι μέθοδοι που παρέχονται σε κλασικές μεθόδους εκπαίδευσης είναι πολλές φορές απαρχαιωμένες. Η εργασιακή πραγματικότητα πάσχει επίσης από το ίδιο πρόβλημα. Αυτό συνεπάγεται ότι οι αποτρεπτικές ενέργειες που λαμβάνονται κινούνται με γνώμονα την αντίδραση σε ένα συγκεκριμένο πρόβλημα, με την έλλειψη ολοκληρωμένης στρατηγικής που να ενισχύει την πρόληψη να είναι συχνό φαινόμενο. Όταν υπάρχει η δυνατότητα, λύνονται ως επί τω πλείστω, μόνο καλώς γνωστά προβλήματα με γνωστές τεχνικές. Δεν προσφέρονται ευκαιρίες στην καθημερινότητα να εξετάζονται νέες τεχνικές άμυνας και επίθεσης σε κυβερνοαπειλές. Είναι λοιπόν απαραίτητο να επενδυθούν πόροι και χρόνος για την περεταίρω εξειδίκευση και εκπαίδευση πάνω σε θέματα κυβερνοασφάλειας. Το ίδιο φαινόμενο παρατηρείται και κατά την εκπαίδευση μαθητών, φοιτητών και ερευνητών ασφάλειας.

Μία λύση στο πρόβλημα αυτό μπορούν να προσφέρουν τα Cyber Ranges (CR, Πεδία Δοκιμών Ασφάλειας). Τα Cyber Ranges είναι το ανάλογο ενός στίβου μάχης ενός στρατοπέδου που χρησιμοποιείται για την εκπαίδευση και προσομοίωση συνθηκών μάχης, ή ενός πεδίου βολής. Σε ένα περιβάλλον όπου η ασφάλεια των πληροφοριακών συστημάτων είναι στο επίκεντρο, τα Cyber Ranges αποτελούν την πλατφόρμα εκπαίδευσης απέναντι σε πραγματικά σενάρια και προσομοιώσεις βασισμένες σε πραγματικές υποδομές και αρχιτεκτονικές. Επιπλέον, λύνουν το πρόβλημα των δοκιμών ρεαλιστικών σεναρίων εκπαίδευσης σε πραγματικές υποδομές, όπου η διακοπή υπηρεσιών και μη διαθεσιμότητα των υπηρεσιών δεν μπορεί να ανεχθεί. Παρέχοντας εικονικά περιβάλλοντα που μπορούν να κλιμακωθούν ανάλογα με την αντίστοιχη ευελιξία.

Η έννοια ωστόσο των cyber ranges, έχει μεταβληθεί τα τελευταία έτη και τείνει να προσαρμόζεται όλο και περισσότερο στο συχνά μεταβαλλόμενο περιβάλλον της ασφάλειας πληροφοριών. Συγχέεται ή χρησιμοποιείται συχνά με τον ορισμό test beds, ωστόσο τα test beds είναι συνήθως συστήματα που δεν διαθέτουν όλα τα δυναμικά χαρακτηριστικά ενός CR. Δημόσιοι και ιδιωτικοί οργανισμοί αναπόφευκτα προσάρμοσαν και ερμήνευσαν τα cyber ranges κατά το δοκούν. Δύο γενικοί ορισμοί/προσδιορισμοί επικρατούν για το χαρακτηρισμό των cyber ranges; ο πρώτος είναι ότι το cyber range είναι ένα *περιβάλλον προσομοίωσης*, και ο δεύτερος εστιάζει στο ότι είναι μία *πλατφόρμα*.

Η παρούσα εργασία αναφέρεται στις ανάγκες και προβλήματα που καλύπτονται, και τις ευκαιρίες που μπορούν να προκύψουν από μία πλατφόρμα cyber range. Περιγράφονται οι αρχιτεκτονικές και οι κυριότερες δομές στα πεδία δοκιμών κυβερνοασφάλειας που συναντώνται στη βιβλιογραφία. Μελετάται η περίπτωση cyber range του KYPO Cyber Range Platform [18], ανοιχτού κώδικα υπό την άδεια MIT, αναλύονται τα σημαντικότερα δομικά στοιχεία του και οι δυνατότητές του, και υλοποιείται μία εγκατάσταση του KYPO Lite σε περιβάλλον Google Cloud Platform (GCP) με χρήση εργαλείων Infrastructure as Code, όπως Terraform Ansible και Vagrant [19]–[22].

2. Cyber Ranges (πεδία δοκιμών κυβερνοασφάλειας)

Η άποψη ότι τα cyber ranges είναι περιβάλλοντα προσομοίωσης προέρχεται από το γεγονός ότι παραδοσιακά, προσέφεραν ένα περιβάλλον προσομοίωσης για ΤΠΕ και ΙΤ με μεγάλο εύρος χρήσης. Η αντίληψη αυτή προσδίδει στατικό χαρακτήρα στα cyber ranges και συνήθως αναφέρεται μόνο σε συγκεκριμένο σύνολο προδιαγραφών και περιπτώσεων και προϋποθέτει ένα μη-συχνά μεταβαλλόμενο περιβάλλον που για να δημιουργηθεί απαιτεί σημαντικό χρόνο και προσπάθεια.

Το «ρεύμα» που περιγράφει τα cyber ranges ως πλατφόρμα, συνήθως τα ορίζει ως ένα σύνολο τεχνολογιών που χρησιμοποιούνται ως βάση για την ανάπτυξη 'άλλων εφαρμογών, διεργασιών ή τεχνολογιών'. Στα στενή έννοια των cyber ranges, μία πλατφόρμα μπορεί να είναι ένα σύνολο τεχνολογιών που χρησιμοποιούνται για τη δημιουργία και τη χρήση ενός περιβάλλοντος προσομοίωσης. Από τη στιγμή που το cyber range έχει ειδικό σκοπό, πρέπει να προσφέρει επιπλέον δυνατότητες και να προσφέρει εξειδικευμένες λειτουργίες στον τελικό χρήστη.

Χαρακτηριστικά, ο NIST (Natural Institute of Standards and Technology) ορίζει τα cyber ranges ως διαδραστικές, προσομοιωμένες αναπαραστάσεις ενός τοπικού (local) δικτύου, των συστημάτων και των εφαρμογών ενός οργανισμού, που είναι συνδεδεμένα σε ένα προσομοιωμένο περιβάλλον επιπέδου διαδικτύου (internet). Παρέχουν ασφαλή, νόμιμα περιβάλλοντα για να αποκτηθούν πρακτικές δεξιότητες κυβερνοασφάλειας και ασφαλή περιβάλλοντα για την ανάπτυξη προϊόντων και την εκτίμηση της κατάστασης της κυβερνοασφάλειας. Ένα Cyber Range μπορεί να περιλαμβάνει πραγματικό υλικό και λογισμικό ή μπορεί να είναι ένας συνδυασμός φυσικών και εικονικών στοιχείων. Τα πεδία (ranges) μπορεί να είναι διαλειτουργικά με άλλα cyber ranges. Το επίπεδο διαδικτύου του περιβάλλοντος ενός πεδίου, περιλαμβάνει όχι μόνο προσομοιωμένη τηλεπικοινωνιακή κίνηση αλλά και αντιγράφει υπηρεσίες δικτύου όπως ιστοσελίδες, προγράμματα περιήγησης και ηλεκτρονικό ταχυδρομείο, κατά τις απαιτήσεις του πελάτη [23], [24].

Ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ECSO-European Cyber Security Organization) αναδεικνύει το γεγονός ότι ο εκάστοτε ορισμός που αποδίδεται, βασίζεται καθαρά στις παραμέτρους και την οπτική/αντίληψη του περιβάλλοντος προσομοίωσης που χρησιμοποιείται [25]. Άλλωστε, τα περισσότερα cyber ranges της αγοράς, προσφέρουν πολλά περισσότερα από ένα απλό περιβάλλον προσομοίωσης που αντικατοπτρίζει το αρχικό, και εξάλλου, τα πεδία (ranges) αυτά θα πρέπει να προσφέρουν περισσότερες επιλογές για να

εξυπηρετούν τις ανάγκες της έρευνας και μελέτης σεναρίων. Βάσει των παραπάνω, ο ECSO ορίζει ένα cyber range ως:

Μία πλατφόρμα για την ανάπτυξη, παροχή και χρήση διαδραστικών περιβαλλόντων προσομοίωσης. Ένα περιβάλλον προσομοίωσης είναι μία αναπαράσταση των τεχνολογιών πληροφορικής (ICT), των διεργασιών (OT) ενός οργανισμού, τις εφαρμογές και τις υποδομές, περιλαμβανομένου των προσομοιώσεων των επιθέσεων, των χρηστών και των ενεργειών τους και ό,τι άλλες διαδικτυακές, δημόσιες ή τρίτες υπηρεσίες από τις οποίες μπορεί να εξαρτάται το προσομοιωμένο περιβάλλον. Ένα Cyber Range περιλαμβάνει το συνδυασμό βασικών/κύριων τεχνολογιών για την πραγματοποίηση και χρήση του περιβάλλοντος προσομοίωσης και των επιπλέον στοιχείων του, που είναι επιθυμητά ή απαραίτητα για την επίτευξη συγκεκριμένων σεναρίων cyber ranges [25].

Στο έργο των Pandey και Ahmad [26] ωστόσο γίνεται ιδιαίτερη μνεία για το επίπεδο ωριμότητας ενός ISMS (Information Security Management System) για ένα οργανισμό, το οποίο είναι άμεσα συνυφασμένο με το επίπεδο της CSA (Cyber Situational Awareness) της επιχείρησης. Η CSA είναι μία μεθοδολογία που χρησιμοποιείται στο να αντικρούσει εξεζητημένες κυβερνοεπιθέσεις και την εκμετάλλευση υπαρχόντων αδυναμιών σε πληροφοριακά συστήματα. Σε επίπεδο ακαδημαϊκό, στρατιωτικό και εμπορικών εφαρμογών και υλοποιήσεων η CSA θεωρείται καινοτόμος μέθοδος για την αντιμετώπιση κυβερνοεπιθέσεων [27]. Η μεθοδολογία προσπαθεί να αξιοποιήσει 4 βασικά στοιχεία που προέρχονται από την SA - Situational Awareness. Τα στοιχεία αυτά επικεντρώνονται στην αντίληψη του περιβάλλοντος, την κατανόησή του και την πρόβλεψη της εξέλιξης των στοιχείων του [27]–[31]. Κατά συνέπεια, η CSA, ορίζει:

- την ευκολία με την οποία ένας οργανισμός μπορεί να αντιληφθεί τη θέση του στο επιχειρησιακό περιβάλλον και τη θέση του απέναντι σε εξωγενείς παράγοντες,
- την κατανόηση των αιτιών, των επιπτώσεων και των συνεπειών των εξωτερικών επιρροών στα συστήματα, αναλύοντας τις αλλαγές στο περιβάλλον στο πέρας του χρόνου
- την ικανότητα πρόβλεψης των πιθανών εξελίξεων από την τρέχουσα κατάσταση σε μελλοντικές καταστάσεις
- την ικανότητα επίλυση του προβλήματος και την ανάκτηση από τυχόν ζημίες στο σύστημα.

Όπως και το ίδιο το Διαδίκτυο, έτσι και τα πεδία δοκιμών κυβερνοασφάλειας, βρίσκουν εφαρμογές και υποστήριξη σε στρατιωτικές εφαρμογές. Κρατικοί και στρατιωτικοί οργανισμοί

έχουν διεκπεραιώσει πολλές έρευνες σχετικά με τα Cyber Ranges, και έχουν προτείνει λύσεις και υλοποιήσεις. Υλοποιήσεις και έρευνες από τα Υπουργεία Άμυνας των ΗΠΑ και της Αυστραλίας, αλλά και πρωτοβουλείες στα πλαίσια του ΝΑΤΟ, είναι χαρακτηριστικά παραδείγματα στη βιβλιογραφία [32], [33]. Επιπλέον πάρα πολλές είναι και οι κατοχυρωμένες εμπορικές λύσεις και παραδείγματα. Τα τελευταία χρόνια πραγματοποιούνται συνεχώς μελέτες για τις εφαρμογές και υλοποιήσεις των Cyber Ranges και τα χαρακτηριστικά τους. Παραπέμπουμε για περισσότερες λεπτομέρειες και συγκρίσεις στην εργασία των Ukwundu et al. [34] όπου παρουσιάζεται εκτενής μελέτη και σύγκριση των Cyber Ranges και Test-beds για την πενταετία 2015-2020 και συνοψίζει τα κύρια χαρακτηριστικά τους κατηγοριοποιημένα βάσει του σκοπού χρήσης, των τεχνολογιών που χρησιμοποιούνται το είδος του περιβάλλοντος δοκιμών και τις πειραματικές μεθόδους που υλοποιούνται. Επιπλέον εργασίες που ασχολούνται με την ανασκόπηση στο πεδίο των cyber ranges συναντάται στους Chaskos [35], Yamin et al [36] , Leitner et al [37], Chouliaras et al. [38].

Στον **Πίνακα 1** βλέπουμε τη σύνοψη των χαρακτηριστικώνΑκολουθεί πίνακας με ταξινομημένα τα Cyber Ranges της βιβλιογραφίας σύμφωνα με τα παρακάτω κριτήρια: αν βρίσκουν εφαρμογή στρατιωτικές και αμυντικές υλοποιήσεις (MDI), αν έχουν ακαδημαϊκή χρήση (Aca), εμπορική και εταιρική χρήση (EC), αν παρέχουν υπηρεσίες ως πάροχοι (SP), αν είναι ανοιχτού κώδικα (OS), αν χρησιμοποιούνται από την εκτελεστική εξουσία (LE), από κρατικους μηχανισμούς (Gvt), τον τύπο υλοποίησης (Deploy), την περιοχή εξειδίκευσης (Specialty), τον τύπο του CR (Type), τις ομάδες κυβερνοασφάλειας που υποστηρίζει (Team), το είδος του περιβάλλοντος δοκιμών (TE) και τις πειραματικές μεθόδους που χρησιμοποιούν (ME).

Λόγω του πεδίου εφαρμογής που πολύ συχνά είναι στρατιωτικές υλοποιήσεις, ή εμπορικές εφαρμογές για παροχή υπηρεσιών εκπαίδευσης, τα περισσότερα πεδία δοκιμών κυβερνοασφάλειας (cyber ranges) είναι ξεκάθαρο, ότι τα τελευταία χρόνια όλο και λιγότερες λύσεις ανοιχτού κώδικα γίνονται διαθέσιμες προς το κοινό. Ωστόσο μία σχετικά πρόσφατη λύση το KYPO CRP [18] προσφέρεται από το Πανεπιστήμιο του Μάσαρικ (Masaryk University) της Τσεχίας ενώ στην ανάπτυξή στοιχείων του συνεργάστηκε και με την Κρατικό Οργανισμό Κυβερνοασφάλειας της Τσεχίας. Η πλατφόρμα αναπτύσσεται από το 2013, ενώ από το 2020 αναδείχθηκε μέσω του ευρωπαϊκού προγράμματος CONCORDIA H2020 και διάφορων επιδοτούμενων προγραμμάτων του Υπουργείου Εσωτερικών της Δημοκρατίας της Τσεχίας [39]. Πρόσφατα άρχισε να προσφέρεται ως λογισμικό ανοιχτού κώδικα, υπό την άδεια MIT [40] και από αποθετήριο λογισμικού του Πανεπιστημίου του Μάσαρικ [41], [42]. Το

λογισμικό, KYPO CRP Lite [43], θα χρησιμοποιηθεί στην παρούσα εργασία για μια υλοποίηση και μελέτη των στοιχείων του και την κατασκευή σεναρίων προσομοίωσης κυβερνοεπιθέσεων.

Πίνακας 1: Συνοπτικός πίνακας με σχετικές εργασίες στη βιβλιογραφία και σύγκριση βασικών χαρακτηριστικών Cyber Ranges [34], [38]

Categories	Ref	MDI	Aca	EC	SP	OS	LE	Govt	Deploy	Specialty	Type	Team	TE	ME
KYPO CR	[18], [44]	N	Y	N	N	Y	N	N	C, VPN,	S, SB,E, EM, ST,CSE; Training,	Prv	B,Gn,Gy,P, R,W,Yl	VM, Hybrid ,SB	E,S,S B
NCR	[24] [25] [45]	Y	N	N	N	N	N	Y	C, VPN	ST, NS	Fed	R, B, Gy	VM	E
Virginia CR	[45], [46]	N	Y	N	N	N	N	N	C	ST	Pub, Prv	R, B	VM	N
Michigan CR	[45]	N	Y	N	N	N	Y	N	C, VPN	ST, AS, CSE	Pub, Prv	R, B	VM, SB	N
Pinecone CR	[45]	N	N	Y	N	N	N	N	N	N	N	N	N	N
IBM X-Force	[45]	N	N	Y	N	N	N	N	C	N	Prv	R, B	VM, SB	N
Cyberbit CR	[45]	N	N	N	Y	N	N	N	N	N	N	N	N	N
Arizona CWR	[45]	N	N	N	N	Y	N	N	N	CSE	N	N	N	N
CRATE	[45], [47]	Y	N	N	N	N	N	N	C, VPN	N	Fed	R, B	VM	N
Cisco CR	[45]	N	Y	Y	N	N	N	N	C, VPN	N	Pub, Prv	R, B, Gn	VM	N
NATO CR	[45], [48]	N	Y	N	N	N	N	N	C, VPN	N	Fed	R, B, G, W, Y	VM, SB	N
DoD CR	[33], [45]	Y	N	N	N	N	N	N	C, VPN	N	Fed	R, B	VM, SB	N
Raytheon CR	[45]	N	N	Y	N	N	N	N	C, VPN	N	Fed	R, B	N	N
Baltimore CR	[45]	N	N	Y	N	N	N	Y	C, VPN	N	Pub, Prv	R, B	N	N
Florida CR	[45]	Y	Y	N	N	N	N	Y	C	PT, EH, NS, SS	Fed, Pub, Prv	R, B	N	N
CRUD	[45]	N	Y	N	N	N	N	N	N	N	N	R, B, P	VM	N
Regent CR	[45]	Y	Y	Y	N	N	N	N	N	RA, M, TV, DF	N	N	N	N
Wayne CR	[45]	N	Y	Y	N	N	N	N	C	EH, CTF, PT, EH	N	N	SB	N
Arkansas CR	[45]	N	Y	N	N	N	N	N	C	PT	N	N	VM	N
Georgia CR	[45]	N	N	Y	N	N	N	Y	N	N	N	N	N	N
SIMTEX	[32]	Y	N	N	N	N	N	Y	N	CSE	Pub	N	N	S
CAAJED	[32], [49]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
SAST	[32], [50]i	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
StealthNet	[32], [51]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
SECUSIM	[32]	N	Y	N	N	N	N	N	N	CSE	Pub	N	N	S
RINSE	[32], [52]	N	Y	N	N	N	N	N	N	CSE	Pub	N	N	S
NetENGINE	[32], [53]	N	Y	N	N	N	N	N	N	CSE	Prv	N	N	S
ARENA	[32], [54]	N	Y	N	N	N	N	N	N	CSE	Pub	N	N	S
OPNET-based	[32]	N	N	N	N	N	N	N	N	NA	Pub	N	N	N
LARIAT	[32], [55]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
VCSTC	[32]	N	Y	N	N	N	N	Y	N	CSE	Pub	N	N	S
Breaking Point	[32]	N	N	Y	N	N	N	N	N	Training	Prv	N	N	S

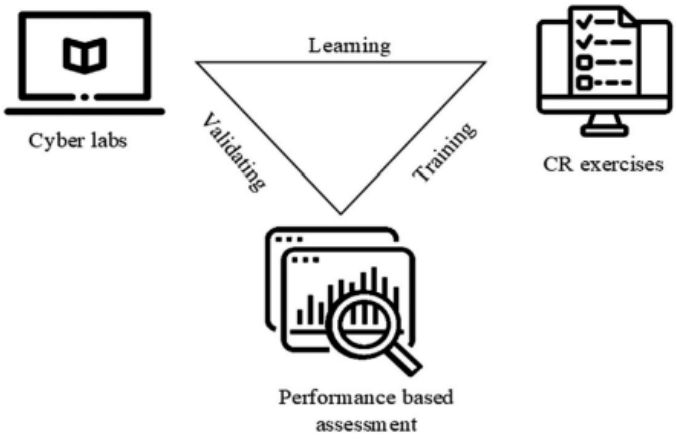
Categories	Ref	MDI	Aca	EC	SP	OS	LE	Govt	Deploy	Specialty	Type	Team	TE	ME
Exata	[32]	Y	N	Y	N	N	N	N	N	Training	Prv	N	N	S
PlanetLab	[32]	N	N	N	N	N	N	N	N	Training, CSE	Fed, Pub	N	N	O
X-Bone	[32]	N	N	N	N	N	N	N	N	CSE	Prv	N	N	O
JIOR	[32]	Y	N	N	N	N	N	Y	N	CSE, Training	Fed	N	N	E
INL	[32], [56]	Y	N	N	N	N	N	Y	N	CSE, Training	Fed	N	N	E
Emulab	[32], [57]	N	Y	N	N	N	N	N	N	CSE, Research	Fed	N	N	E
DETER	[32]	N	Y	N	N	N	N	N	N	CSE, Research	Fed	N	N	E
Virtualised CR	[32], [58]	N	Y	N	N	N	N	N	N	CSE, Research	Fed	N	N	E
Reassure	[32]	N	Y	N	N	N	N	N	N	Research	Pub	N	N	E
Northrop G	[32]	Y	N	Y	N	N	N	N	N	CSE, Training	Prv	N	N	E
Counter HC	[32]	N	N	Y	N	N	N	N	N	Training, CSE	Prv	N	N	NA
Detica	[32]	N	N	Y	N	N	N	N	N	Training	Prv	N	N	N
ATC	[32]	N	N	Y	N	N	N	N	N	Training	Prv	N	N	LS
Testbed@ TWISC	[36], [59]	N	Y	N	N	N	N	N	C	Research, ST	Prv	N	SB	E
INSALATA	[36], [60]	N	N	N	N	Y	N	N	C	NS, Research	Prv	N	Hybrid	E
CyberVan	[36], [61]	Y	N	N	N	N	N	N	C	ST, NT	Pub	N	Hybrid	S
SoftGrid	[36], [62]	Y	N	N	N	Y	N	N	C	ST, NT, AS	Prv	N	H	E

Υπόμνημα Πίνακα 1

Aca: Academic or Research	H: Hardware	RA: Ransomware Attacks
AS: Attack Simulation	LE: Law Enforcement	S: Simulation
B: Blue	M: Monitoring	SB: Sandbox
C: Cloud	MDI: Military, Defense and Intelligence	SP: Service Provider
CSE: Cyber- Security Exercise	ME: Methods of Experimentation	SS: System Security
CTF: Catch-The-Flag	N: No/ Not Available	ST: Security/ Software Testing
DF: Digital Forensic	NS: Network Security	TE: Testing Environment
E: Emulation	O: Overlay	TV: Threat and Vulnerability
EC: Enterprise and Commercial	OS: Open Source	VCN: Virtual Clone Network
EH: Ethical hacking	P: Purple	VM: Virtual Machine
Fed: Federated	Prv: Private	VPN: Virtual Private Network
Gn: Green	PT: Penetration Testing	W: White
Govt: Government	Pub: Public	Y: Yellow
Gy: Grey	R: Red	Y: Yes/ Available

2.1 Οφέλη της εκπαίδευσης σε Cyber Ranges και πεδία εφαρμογής

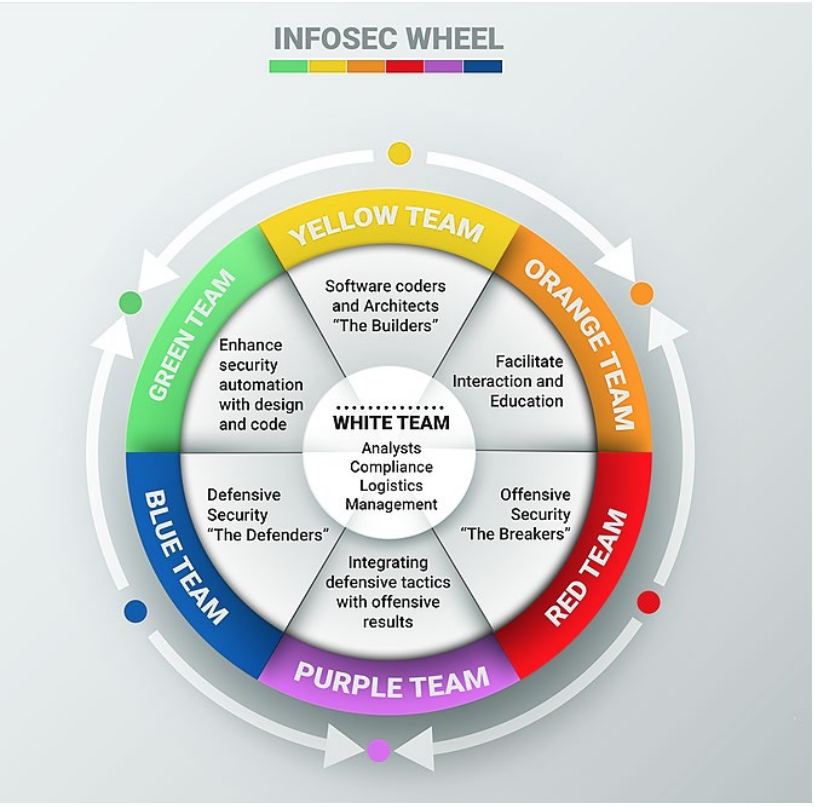
Τα cyber ranges χρησιμοποιούνται από πολλά διαφορετικά είδη οργανισμών και χρηστών, με κυριότερο σκοπό την εκπαίδευση. Χρησιμοποιούνται από φοιτητές είτε ακαδημαϊκά είτε σε ατομικά επίπεδο, για να εφαρμοστούν οι γνώσεις τους και να εμβαθύνουν στον τομέα της ασφάλειας πληροφοριών. Μία κοινή χρήση είναι η προετοιμασία για εξετάσεις πιστοποιήσεων. Εκπαιδευτικοί μπορούν να τα χρησιμοποιήσουν πέραν της κλασικής διδασκαλίας, για να εκπαιδεύσουν, να εξετάσουν και να αξιολογήσουν μαθητές. Επιπλέον, μπορεί να χρησιμοποιηθούν σε διάφορα ερευνητικά έργα, για εφαρμογή πειραμάτων σε ασφαλή περιβάλλοντα. Μπορούν να χρησιμοποιηθούν από επαγγελματίες και οργανισμούς για την αξιολόγηση του επιπέδου γνώσεων σε θέματα κυβερνοασφάλειας, τις δοκιμές υλοποιήσεων νέου λογισμικού, όπως και για την εκπαίδευση και βελτίωση τους. Με την πρακτική άσκηση να είναι σε πρώτο πλάνο, τα προσόντα των ομάδων κυβερνοασφάλειας ή των διάφορων ειδικοτήτων σε έναν οργανισμό μπορούν να εξασκηθούν δοκιμάζοντας διάφορα σενάρια επιθέσεων.



Εικόνα 1: Βασικό περιβάλλον CR (Cyber Range)[26]

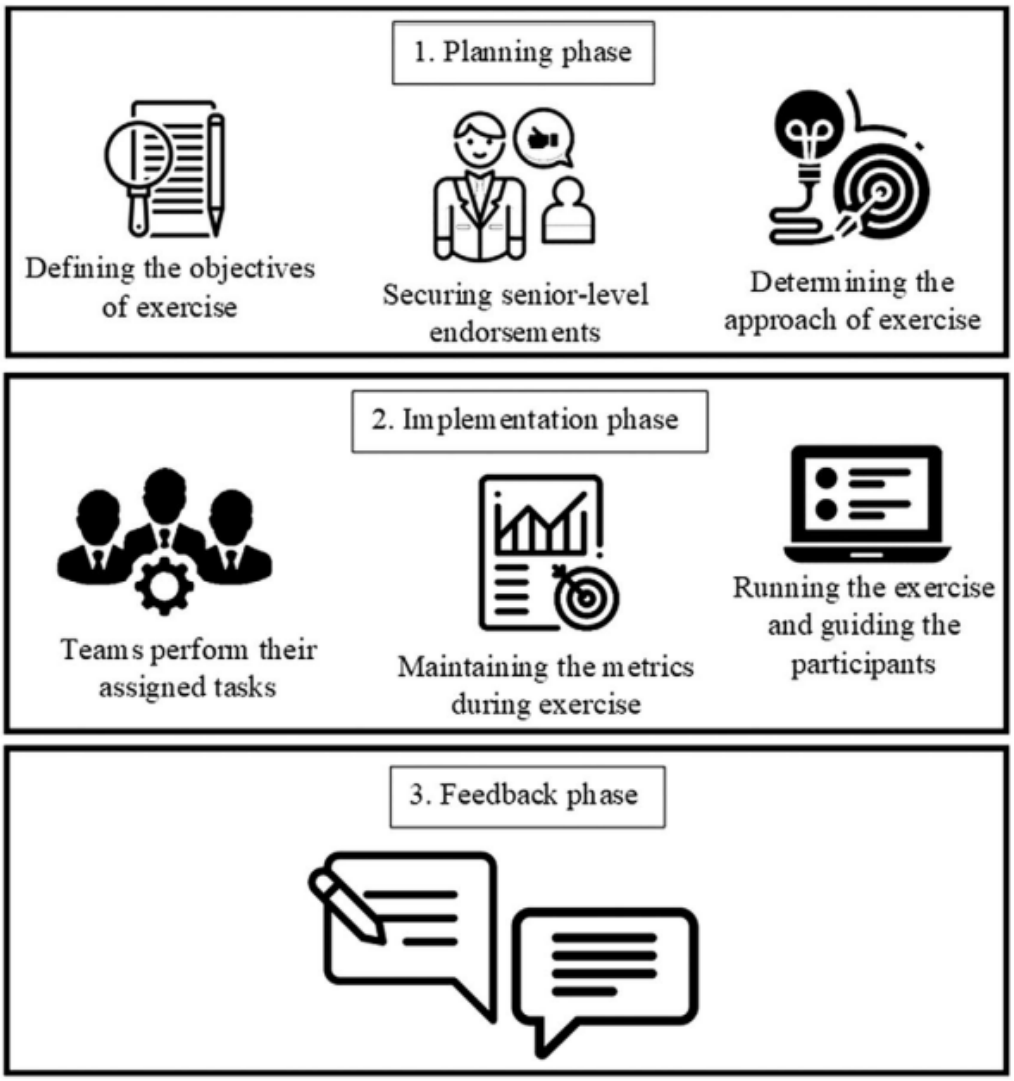
Στο χώρο της κυβερνοασφάλειας χρησιμοποιούνται συχνά ορισμοί που περιγράφουν ομάδες και είδος ενεργειών βάσει χρωμάτων για να περιγράψουν το ρόλο ή το σκοπό μιας εξειδικευμένης ομάδας που είτε ασχολείται με την επίθεσή την άμυνα ενός Πληροφοριακού Συστήματος (ΠΣ) ομάδων. Οι πιο γνωστοί ορισμοί που χρησιμοποιούνται είναι το Red Teaming και το Blue Teaming. Η "κόκκινη" ομάδα είναι η ομάδα που είναι υπεύθυνη να παίξει το ρόλο του επιτιθέμενου στο σύστημα στην προσπάθεια να ανακαλυφθούν οι ευπάθειες του συστήματος και να ελέγξουν την πραγματική κατάσταση των δικλείδων ασφαλείας του ΠΣ.

Συνήθως οι Red Teams εκτελούν καμπάνιες social engineering, penetration testing, και χρησιμοποιούν τρόπους ενεργής επίθεσης (με χρήση κώδικα, ή άλλων μέσων). Κατ-αντιστοιχία οι "μπλε" ομάδες έχουν αμυντικό ρόλο και είναι υπεύθυνοι για να ενισχύσουν την περιμετρική, και όχι μόνο, ασφάλεια με υλοποιήσεις όπως συστήματα ανίχνευσης διείσδυσης (IDS) και συστήματα αποτροπής διείσδυσης στο δίκτυο (IPS). Είναι επίσης υπεύθυνοι για την εφαρμογή τεχνικών hardening στα συστήματα απέναντι σε γνωστές ευπάθειες με χρήση καλών πρακτικών. Σε σύγχρονες υλοποιήσεις, αυτοί οι ρόλοι αλληλοκαλύπτονται σε εταιρικά περιβάλλοντα και οργανισμούς, καθώς αναδεικνύεται η ανάγκη για εξειδικευμένες γνώσεις τόσο επίθεσης όσο και άμυνας απέναντι σε κυβερνοαπειλές, με αποτέλεσμα να ορίζονται και "μωβ" ομάδες (Purple Team)[63]–[65]. Επιπλέον, η κίτρινη ομάδα έχει πιο ελεύθερο ρόλο, συνεισφέροντας στο ρεαλισμό των εκάστοτε σεναρίων προσομοίωσης, ενώ η λευκή ομάδα, είναι υπεύθυνη για την προετοιμασία και διαχείριση του σεναρίου της άσκησης. Κατ΄ επέκταση, μπορούμε να σχηματίσουμε συνδυασμούς χρωμάτων-ομάδων χρησιμοποιώντας ως βάση τα βασικά χρώματα (μπλε, κόκκινο, κίτρινο) και να δημιουργήσουμε "ενδιάμεσες" ομάδες. Μιλάμε πλέον για "πράσινες" ομάδες, "πορτοκαλί" ομάδες ενώ χρησιμοποιούμε και τον ορισμό της "λευκής" ομάδας.



Εικόνα 2: Infosec Wheel, περιγράφει τις αλληλοεπιδράσεις μεταξύ των "ομάδων" και των ρόλων που σχηματίζονται για διασφάλιση και διαχείριση της ασφάλειας πληροφοριακών συστημάτων [66]

Η ανάγκη για τη χρήση και διαχωρισμό σε ομάδες σε μία άσκηση κυβερνοασφάλειας βασίζεται κυρίως στο γεγονός ότι κατά το σχεδιασμό της, διακρίνονται τρεις φάσεις σύμφωνα με τους Wilhelmson et al. [67] όπως αυτές περιγράφονται στην Εικόνα 3, και συνοψίζονται στη φάση του προγραμματισμού, της υλοποίησης και της ανατροφοδότησης πληροφοριών (feedback) σχετικών με την άσκηση. Κατά την πρώτη φάση ο οργανισμός που επιλέγει μία άσκηση κυβερνοασφάλειας θα πρέπει να είναι σε θέση να ορίσει τους στόχους και τα οφέλη της άσκησης και να ακολουθήσει κατάλληλη προσέγγιση. Πολύ σημαντικό είναι και η εξασφάλιση των πόρων σε χρόνο και χρήμα. Δεν πρέπει να ξεχνάμε ότι όλες οι ασκήσεις πρέπει να είναι σε συνάρτηση με το ενδιαφέρον του οργανισμού και να συνάδει με τις λειτουργίες του επιχειρησιακού μοντέλου του.



Εικόνα 3: Φάσεις κατά τη διάρκεια ζωής μίας άσκησης κυβερνοασφάλειας [26].

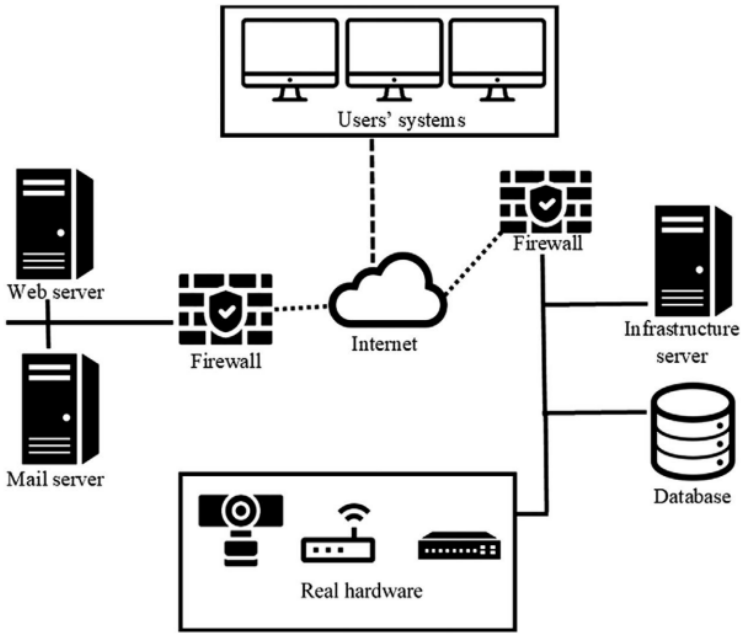
Ένα από τα μεγαλύτερα πλεονεκτήματα της εκπαίδευσης σε cyber ranges, είναι η πρακτική εμπειρία που αποκτάται πάνω στα διάφορα σενάρια κυβερνοαπειλών. Για αναλυτές ασφάλειας και μηχανικούς ασφαλείας τα CRs προσφέρουν ένα περιβάλλον όπου μπορεί να ενισχυθεί η συλλογική διατμηματική συνεργασία και να βελτιωθεί η επικοινωνία μεταξύ των ομάδων. Το γεγονός αυτό σε ένα γρήγορα μεταβαλλόμενο επιχειρησιακό περιβάλλον βασισμένο σε DevSecOps πρακτικές και Agile μεθοδολογίες βοηθά στη μείωση των silos και την ενίσχυση της διαφάνειας (transparency) . Επιπλέον μπορούν να μελετηθούν με ευκολία νέες περιπτώσεις χρήσης που προσαρμόζονται αντίστοιχα στα νέα σενάρια κυβερνοαπειλών. Η ταχύτητα με την οποία προσαρμόζονται τα σενάρια λόγω της ευελιξίας των CRs, προσφέρει τη δυνατότητα να εξετάζονται σενάρια πραγματικών περιπτώσεων. Όλα τα σενάρια που μελετώνται σε ένα CR, υλοποιούνται σε ελεγχόμενα περιβάλλοντα όπου πολύπλοκες αρχιτεκτονικές χρησιμοποιούνται ως αναφορά ή και σενάριο. Η πολυπλοκότητα αυτή δίνει τη δυνατότητα στις ομάδες να προετοιμάζονται, να υλοποιούν και να εξετάζουν επαρκείς στρατηγικές ασφάλειας για τις υποδομές ενός οργανισμού. Οι νέες τεχνικές και η έρευνα επωφελούνται καθώς το περιβάλλον του CR είναι ασφαλές και με μικρό κόστος. Επιπλέον χαρακτηρίζονται από μικρό ρίσκο όταν υλοποιούνται νέες τεχνολογίες ή επεμβατικές δοκιμές στα ελεγχόμενα περιβάλλοντα, με μικρό ρίσκο για τα παραγωγικά περιβάλλοντα. Πολύ σημαντικός είναι και ο ρόλος των CR στην ανάπτυξη της κουλτούρας κυβερνοασφάλειας καθώς μέσω της διαρκούς εκπαίδευσης, μπορεί να αναδείξει τα ταλέντα και να προσφέρει περισσότερη κατανόηση των κυβερνοαπειλών κατά την πρακτική ανάλυση και εξέταση σεναρίων απειλών. Ένα CR Μπορεί επίσης να αναδείξει τα προβλήματα ή τις ελλείψεις σε γνώσεις σε θέματα κυβερνοασφάλειας στα άμεσα, και όχι μόνο, συσχετιζόμενα τμήματα ενός οργανισμού και να δώσει ένα ακόμη εργαλείο αξιολόγησης προσωπικού ή πιθανών υποψηφίων για μία θέση και να χρησιμοποιηθεί ως μέθοδος αξιολόγησης σε διαδικασία συνέντευξης. Μπορούν να αντιγράψουν πραγματικές επιθέσεις APT, και να βοηθήσουν να αξιολογηθεί η αμυντική ετοιμότητα του οργανισμού,

2.2 Είδη Cyber Ranges

Μπορούμε να διακρίνουμε τρία βασικά είδη Cyber Ranges:

- **Physical CR** που δημιουργούν ένα πρωτότυπο οποιουδήποτε φυσικού δικτύου ή επεξεργαστικών υποδομών (routers,switches, firewals, servers, κ.ά.)
- Τα **Virtual CR** (εικονικά). Αυτό το είδος CR προσφέρει μία προσομοίωση ολόκληρης της υπολογιστικής υποδομής με τη βοήθεια των τεχνολογιών εικονοποίησης (virtualization)

- **Hybrid CR**, ως αναμενόμενο τα φυσικά και εικονικά CRs συνδυασμένα, υλοποιούνται και χρησιμοποιούνται κατ' απαίτηση, διασφαλίζοντας οικονομία πόρων. Συναντώνται και ως *cyber-physical* ranges.



Εικόνα 4: Physical CR [26]

Ένας ακόμη συνηθισμένος τρόπος διαχωρισμού και ταξινόμησης είναι εκτός από το είδος του της τεχνολογίας στην οποία βασίζονται, να ταξινομούνται ανάλογα με το περιβάλλον που χρησιμοποιούνται.

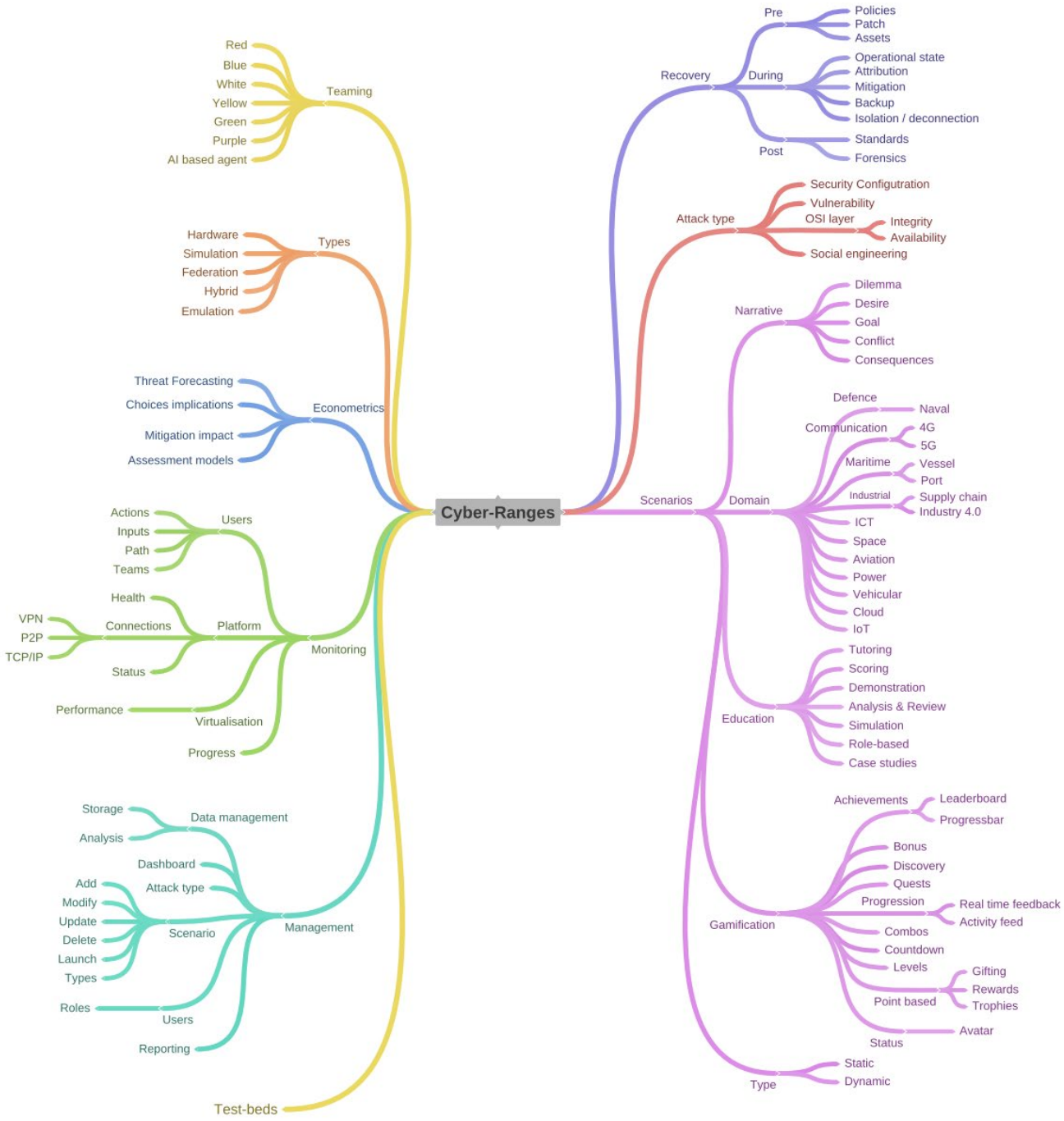
Στη βιβλιογραφία διακρίνουμε επίσης ότι διαχωρίζονται τα cyber ranges με τα test beds, λόγω του εκάστοτε τρόπου εφαρμογής τους και του σκοπού εκπαιδευτικής χρήσης τους. Η διαφοροποίηση αυτή υφίσταται για να αναδείξει κυρίως το γεγονός ότι τα CRs χρησιμοποιούνται σε περιβάλλοντα IT, ενώ τα test beds σε περιβάλλοντα OT (Operational Technology). Επιπλέον, γίνεται πιο ξεκάθαρο ότι τα CR αποσκοπούν σε τελικούς χρήστες με γενική γνώση της αρχιτεκτονικής προσομοίωσης, ενώ τα test-beds συχνά απαιτούν εξειδικευμένη γνώση στο επιστημονικό πεδίο. Οι Pandey και Ahmad διαχωρίζουν τα CR σε ακαδημαϊκά ή στρατιωτικά [26]. Για την κατασκευή του κορμού ενός CR, απαιτείται η δημιουργία ενός σεναρίου που θα πρέπει να περιέχει τα παρακάτω στοιχεία [34].

i. Ένα αφήγημα, που επιτρέπει στον χρήστη να εξελίσσεται
ii. Το πεδίο εφαρμογής, που μπορεί να ορίζεται ευρέως ή σε κλειστό πεδίο (π.χ. cyber training ή military cyber training)

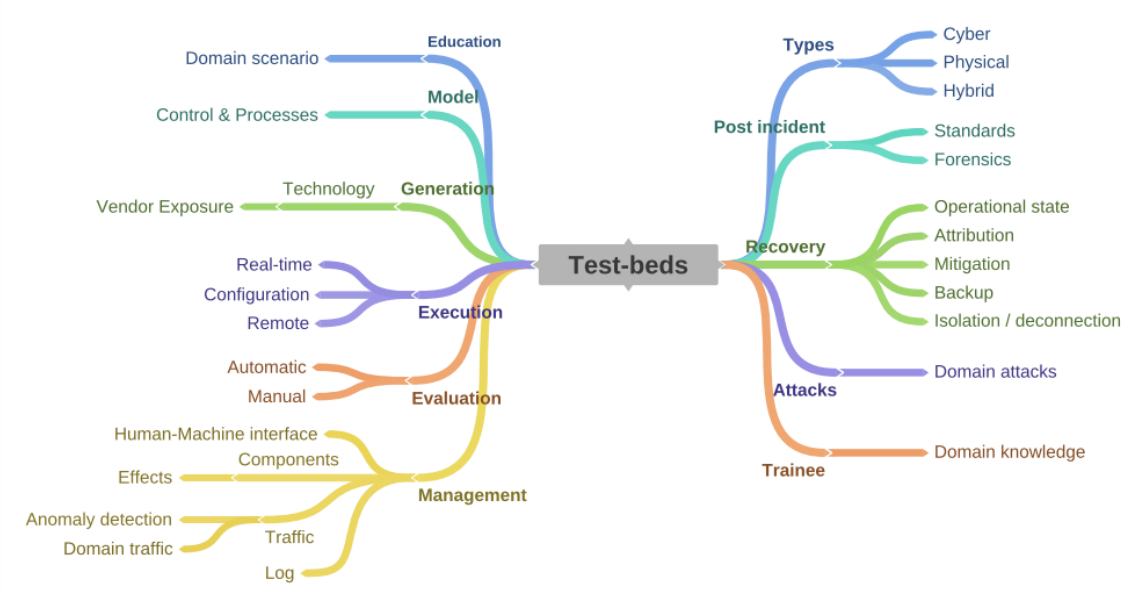
iii. Να υπάρχει σύνδεση μεταξύ των μηχανισμών εκπαίδευσης και των μηχανισμών της πλατφόρμας κατά τη διάρκεια του σεναρίου (ενημέρωση προόδου, βαθμολογίας, συλλογή δεδομένων, κτλ)

iv. Οι μηχανισμοί αυτοί εξαρτώνται επιπλέον στο παίγνιο (gamification)[68] [69], [70]

v. Ένα δυναμικό ή στατικό σενάριο.



Εικόνα 5: Τρόπος ταξινόμησης Cyber Ranges σύμφωνα με τα χαρακτηριστικά που χρησιμοποιήθηκαν από τους Ukwandu et al., μεταξύ άλλων, διαχωρίζουν τα cyber ranges βάσει το είδους τους (physical, simulation, κλπ) του επιστημονικού ή εμπορικού πεδίου εφαρμογής, το είδος της εκπαίδευσης που παρέχουν και του δυναμικού ή στατικού τους χαρακτήρα. [34]



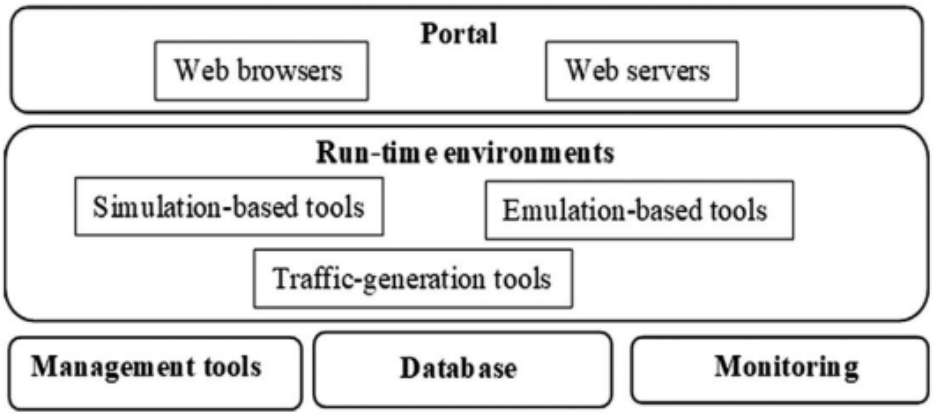
Εικόνα 6: Τρόπος ταξινόμησης των test beds σύμφωνα με τους Ukwandu et al., όπου ως κριτήριο χρησιμοποιούνται τα μοντέλα λετουργίας, ο τύπος τους, ο τρόπος και η φύση των εκπαιδευτικών σεναρίων που επεξεργάζονται και οι δυνατότητες ανάλυσης. [34]

2.3 Αρχιτεκτονικός σχεδιασμός Cyber Ranges

Στόχος των CR είναι να παρέχουν ασφαλή και κατανοητά περιβάλλοντα, όπου θα μπορούν να αναλυθούν πολιτικές (policies) και προϊόντα πέρα από τις κυβερνοαπειλές και ευπάθειες. Όπως προαναφέρθηκε, τα CR έχουν ως κύριο σκοπό την εκπαίδευση, και πρέπει να διασφαλίζουν βασικές λειτουργίες για την εκπλήρωσή ενός σεναρίου εκπαίδευσης (προσομοίωση κυβερνοαπειλών, εκπαίδευση προσωπικού, δοκιμές προϊόντων). Η πιο συνήθης αρχιτεκτονική που συναντάται στα συστήματα CR, είναι αυτή που φαίνεται στην Εικόνα 7 και περιλαμβάνει τα εξής στοιχεία:

- **Portal**: (Πύλη εισόδου) που χρησιμοποιεί στοιχεία διεπαφής χρήστη και front-end τεχνολογία.

- **Run-time environments**: τα περιβάλλοντα που υποστηρίζουν την εκτέλεση των εργαλείων προσομοίωσης και σεναρίων. Υποστηρίζουν επίσης και την δημιουργία τεχνητής τηλεπικοινωνιακής κίνησης σε πραγματικό χρόνο.
- **Management**: (Διαχείριση) είναι το στοιχείο όπου γίνεται η διαχείριση των διεργασιών, και αυτό μεταφράζεται σε δέσμευση απαραίτητων υπολογιστικών πόρων, διαχείριση ομάδων, και ανάθεση εργασιών ενός CSE (CSEEEE)
- **Database**: (Βάση Δεδομένων) χρησιμοποιείται για την αποθήκευση διαφορετικών σεναρίων εκπαίδευσης, στατιστικά δεδομένα των ολοκληρωμένων ασκήσεων, αποθήκευση αρχείων καταγραφής (logs), κλπ.
- **Monitoring**: (Παρακολούθηση) υποστηρίζει τα συστήματα παρακολούθησης των CSEs, την έρευνα για κυβερνοεπιθέσεις και κυβερνοαπειλές, όπως και δοκιμές ασφάλειας σε προϊόντα.



Εικόνα 7: Αρχιτεκτονικά στοιχεία ενός CR (Cyber Range)[26]

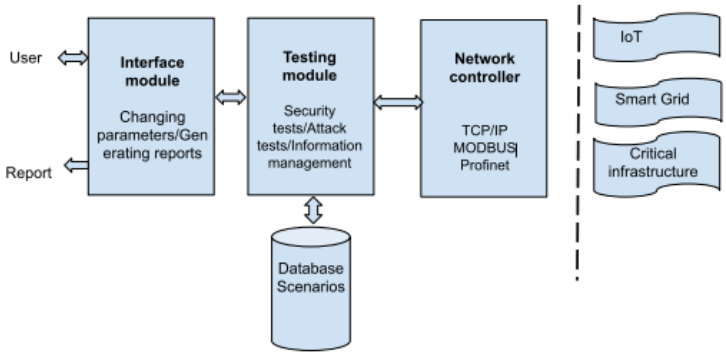
Πιο συγκεκριμένα το **portal** είναι υπεύθυνο για τη διασφάλιση της επικοινωνίας μεταξύ ενός CR, των χρηστών του και του περιβάλλοντος προσομοίωσης. Άμεσα συσχετισμένοι χρήστες με το portal είναι οι CSE admins, τα μέλη της White Team (Λευκή Ομάδα), ερευνητές ασφάλειας, διαχειριστές των test beds, εκπαιδευτές. Τα περισσότερα portal είναι συνήθως web-based, σε τεχνολογίες όπως nginx ή Apache web servers, όπου ο διακομιστής ελέγχει την κίνηση και πραγματοποιεί διαχείριση χρηστών, αλλά και διαχειρίζεται το σύνολο των αιτημάτων και απαντήσεων (requests-responses).

2.4 Αρχιτεκτονικές CR και Test-beds

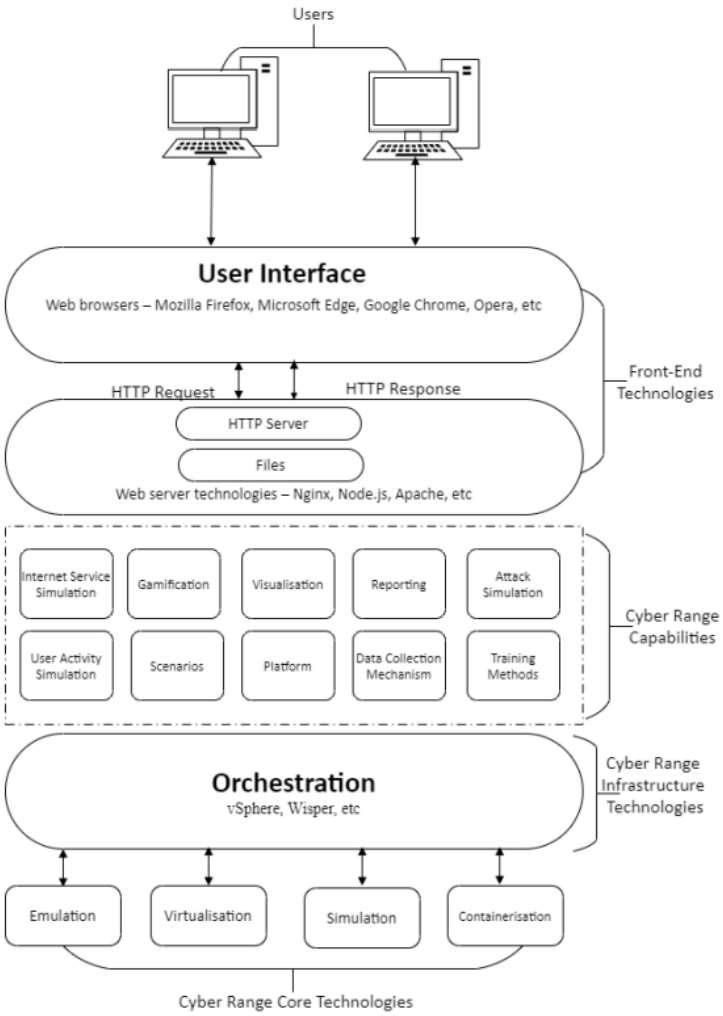
Ακολουθεί η περιγραφή των σημαντικότερων αρχιτεκτονικών που συναντώνται στη βιβλιογραφία και στις πιο διαδεδομένες λύσεις για CR και Test-beds.

Τα περιβάλλοντα εκτέλεσης (**Run-time environments**) μπορεί να συνδυάζουν πολλά και πολύπλοκα περιβάλλοντα για να εκτελέσουν και να προσφέρουν επιτυχώς ένα σενάριο εκπαίδευσης. Παρακάτω παρουσιάζονται οι πιο γνωστές και διαδεδομένες τεχνικές και αρχιτεκτονικές για την υλοποίηση cyber ranges ή test-beds.

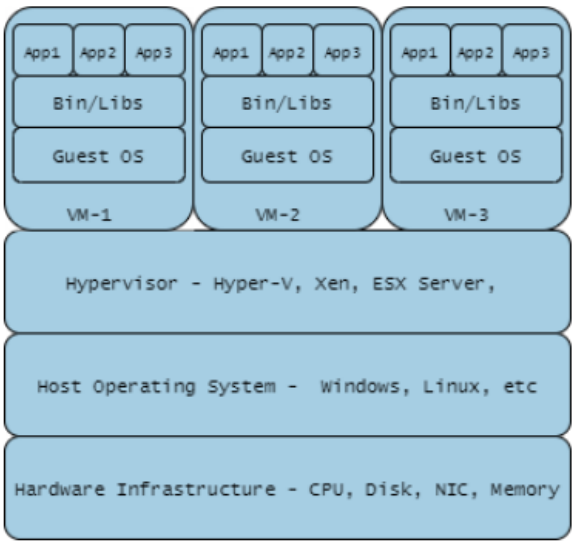
Οι πλατφόρμες εικονοποίησης όπως το VMWare είναι από αυτές που χρησιμοποιούνται συχνότερα. Ειδικότερα μία αρχιτεκτονική βασισμένη σε VMWare μπορεί να παρέχει τα εξής χαρακτηριστικά: Μπορεί να εγκατασταθεί απευθείας πάνω σε υλικό (π.χ. ESXi), παρέχει επίπεδα virtualization μεταξύ Λειτουργικού συστήματος και υλικού, και προσφέρει τη δυνατότητα να δημιουργηθούν ασφαλή συστήματα με πόρους που είναι διαχωρισμένοι σε λογικό επίπεδο. Αρκετά CRs επιλέγουν να βασίζουν την υλοποίησή τους σε πλατφόρμα VMware, καθώς ενδείκνυται για περιβάλλοντα με ποικίλα λογισμικά, και ακόμη περισσότερο σε περιβάλλοντα με απαιτήσεις στην απομόνωση (isolation) και διαχείριση των πόρων κάνοντας χρήση των δεσμεύεσεων (reservations), των ορίων (limits), και των διαμοιραζόμενων πόρων (shares).



Εικόνα 8: Περιγραφή των στοιχείων ενός Test-bed [34]

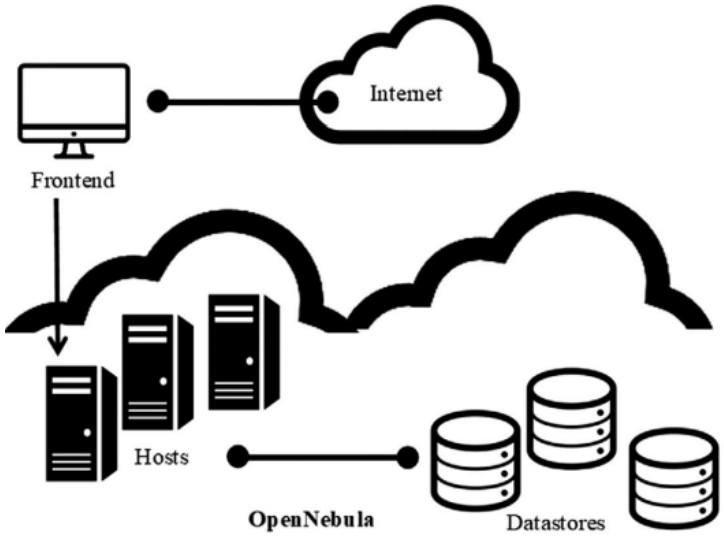


Εικόνα 9: Αρχιτεκτονικός σχεδιασμός ενός Cyber Range [34]



Εικόνα 10: Περιγραφή αρχιτεκτονικής εικονοποίησης (Virtualization) [34]

Μία άλλη τεχνολογία είναι το virtualization που προσφέρεται από το OpenNebula. Η αρχιτεκτονική είναι πιο απλή σε σχέση με το VMware, και μπορεί να περιγραφεί από 9 στοιχεία: *το front end, το host, το cluster, το image repository, sunstone (admin web-interface), OCCI και OCA*. Άξιο αναφοράς είναι το γεγονός ότι χρησιμοποιείται η RBAC (Role Based Access Control) αρχή για την διαχείριση χρηστών στο σύστημα και ότι οι υπηρεσίες OCCI, EC2 services επιτρέπουν τη διαχείριση υπολογιστικής νέφους με διαφορετικές διεπαφές. Τα στοιχεία αυτά είναι και τα υπεύθυνα για την παρακολούθηση, έλεγχο και πρόσβαση των αποθηκευτικών μέσων.

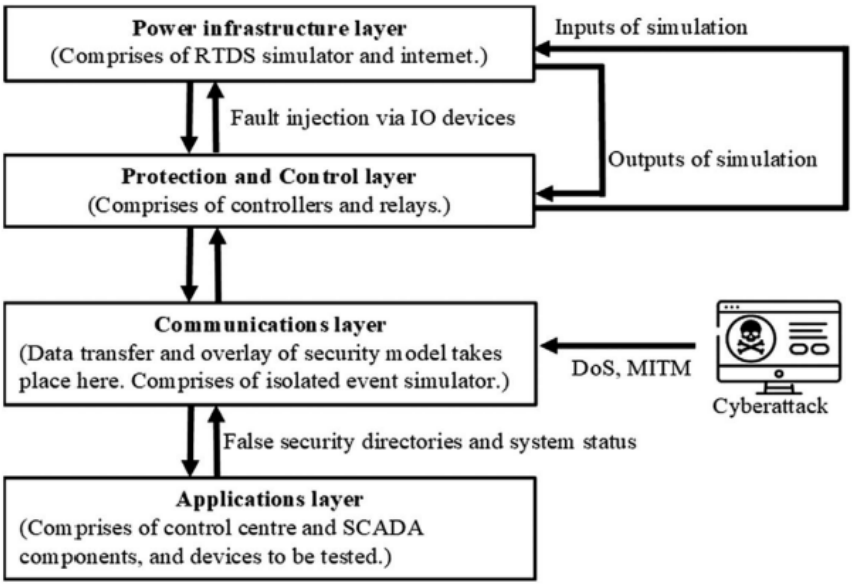


Εικόνα 11: OpenNebula αρχιτεκτονική [26]

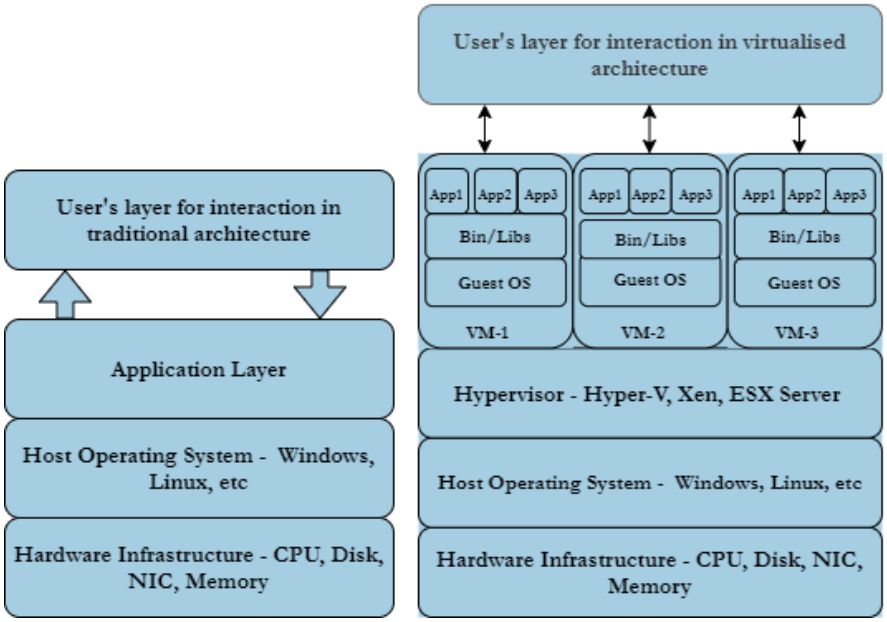
Το OpenNebula προσφέρει κλιμακώμενα (scalable) περιβάλλοντα, την πλατφόρμα Elastic παρέχοντας δυνατότητες SIEM (Security Information and Event Management) και δυνατότητα ανάλυσης των δεδομένων του περιβάλλοντος προσομοίωσης ενώ λόγω του διαμοιρασμού πόρων μεταξύ διαφορετικών φυσικών πόρων, ελαχιστοποιείται το ρίσκο παύσης λειτουργίας του συστήματος, και προσφέρει βελτιστοποίηση για της χρήσης των πόρων με την εικονοποίηση.

Βλέπουμε επίσης ότι στη βιβλιογραφία χρησιμοποιούνται εδώ και αρκετά χρόνια τεχνικές και αρχιτεκτονικές που διασφαλίζουν τη λειτουργία τέτοιων πολύπλοκων συστημάτων προσομοίωσης. Αρχιτεκτονικές που μετράνε ήδη 30 χρόνια συναντώνται σε περιβάλλοντα προσομοίωσης κυρίως υλικού (hardware) που εφαρμόζονται κυρίως σε συστήματα ενέργειας, συστήματα αυτόματης διανομής, συστήματα κλειστού βρόχου και συστήματα υψηλής τάσης. Οι RTDS (Real-Time Digital Simulator/Ψηφιακοί Προσομοιωτές

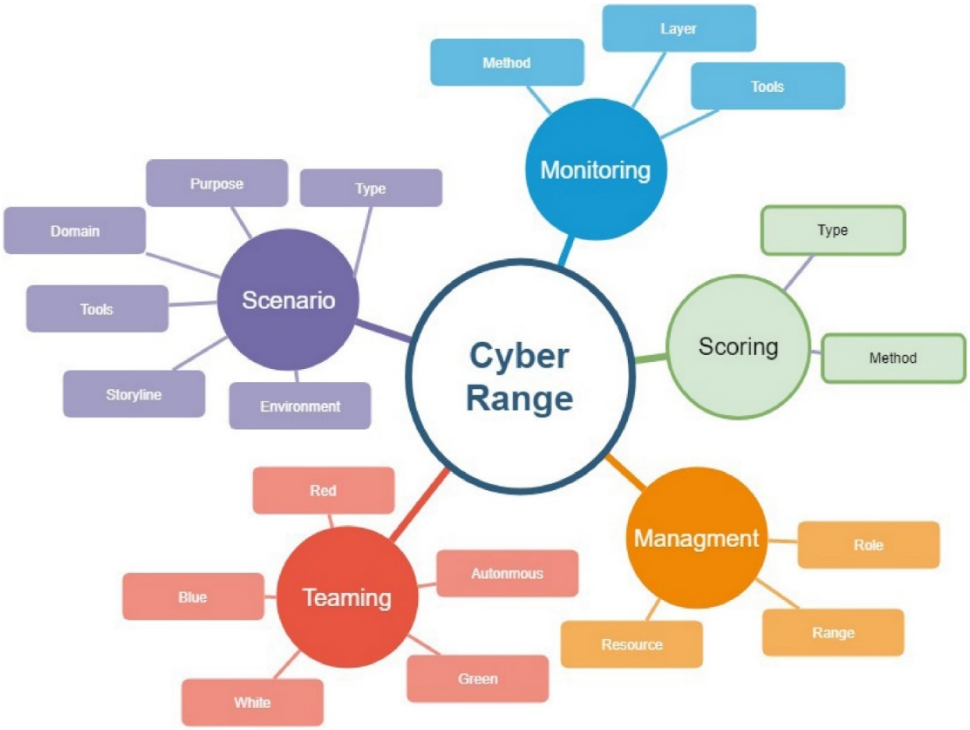
Πραγματικού Χρόνου) είναι ικανοί να προσομοιώσουν υποδομές ενεργειακών συστημάτων βασισμένοι σε αρχιτεκτονική παράλληλης επεξεργασίας [71]. Το κόστος τους είναι σημαντικά μικρότερο σε σύγκριση με τον αναλογικό προσομοιωτή. Με τα χρόνια η αρχιτεκτονική αυτή εξελίχθηκε και προσαρμόστηκε στις ανάγκες των βιομηχανικών κυρίως IoT συσκευών [72]–[74]. Σε πραγματικές συνθήκες προσφέρουν μία πλατφόρμα δοκιμών (test-bed) για την προσομοίωση κυβερνοεπιθέσεων σε ενεργειακές υποδομές. Είναι σε θέση να προσομοιώσουν DoS (Denial of Service) και MitM (Man in the Middle) επιθέσεις, ανάλυση σφαλμάτων υλικού ή κρυπτογραφική ανάλυση. Στην Εικόνα 12, παρουσιάονται αυτές οι αλληλεπιδράσεις. σΣτα θετικά συγκαταλέγεται το γεγονός ότι προσφέρει πολύ γρήγορα αποτελέσματα για ερευνητικούς και εκπαιδευτικούς σκοπούς, καθότι μπορεί να δώσει γρήγορα και άμεσα αποτελέσματα και οι δοκιμές μπορούν να ελεγχθούν και να πιστοποιηθούν από τους χρήστες, βοηθώντας στην οικονομία χρόνου. Στα σενάρια μελέτης PHIL (Power Hardware In Loop) ή HIL (Hardware In Loop), δίνεται η δυνατότητα σύνδεση και μελέτης του πραγματικού υλικού σε χρήση, δίνοντας δυνατότητες μηχανικών δοκιμών ή συμπεριφοριακής ανάλυσης υπό φόρτο καθώς και άλλα σενάρια. Είναι συστήματα που μπορούν εύκολα να αναπτυχθούν, να κλιμακωθούν και να παρέχουν άμεση ανταλλαγή δεδομένων μέσω διάφορων πρωτοκόλλων επικοινωνίας (MODBUS, TCP/UDP, IEC 61850-9-2).



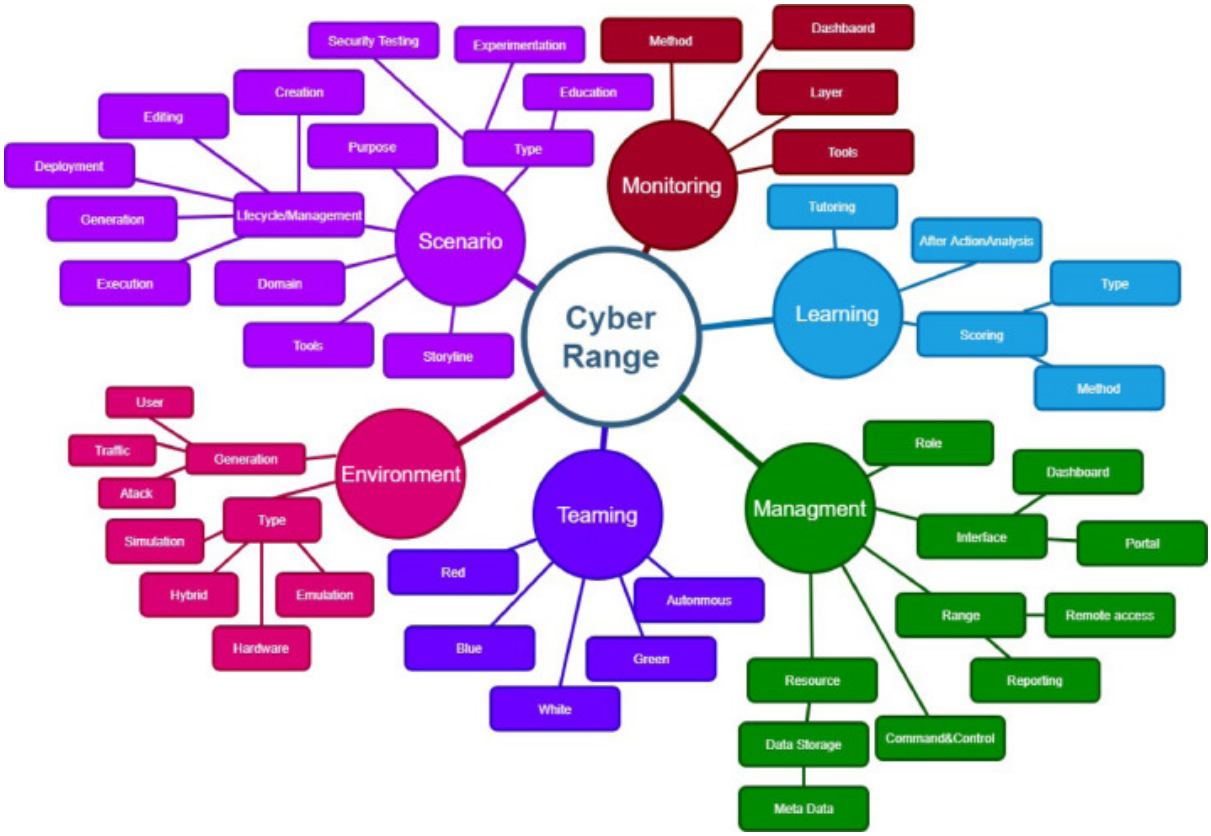
Εικόνα 12: Προσομοίωση RTDS (Real Time Digital Simulator) [26]



Εικόνα 13: Υβριδική αρχιτεκτονική Cyber Range [34]

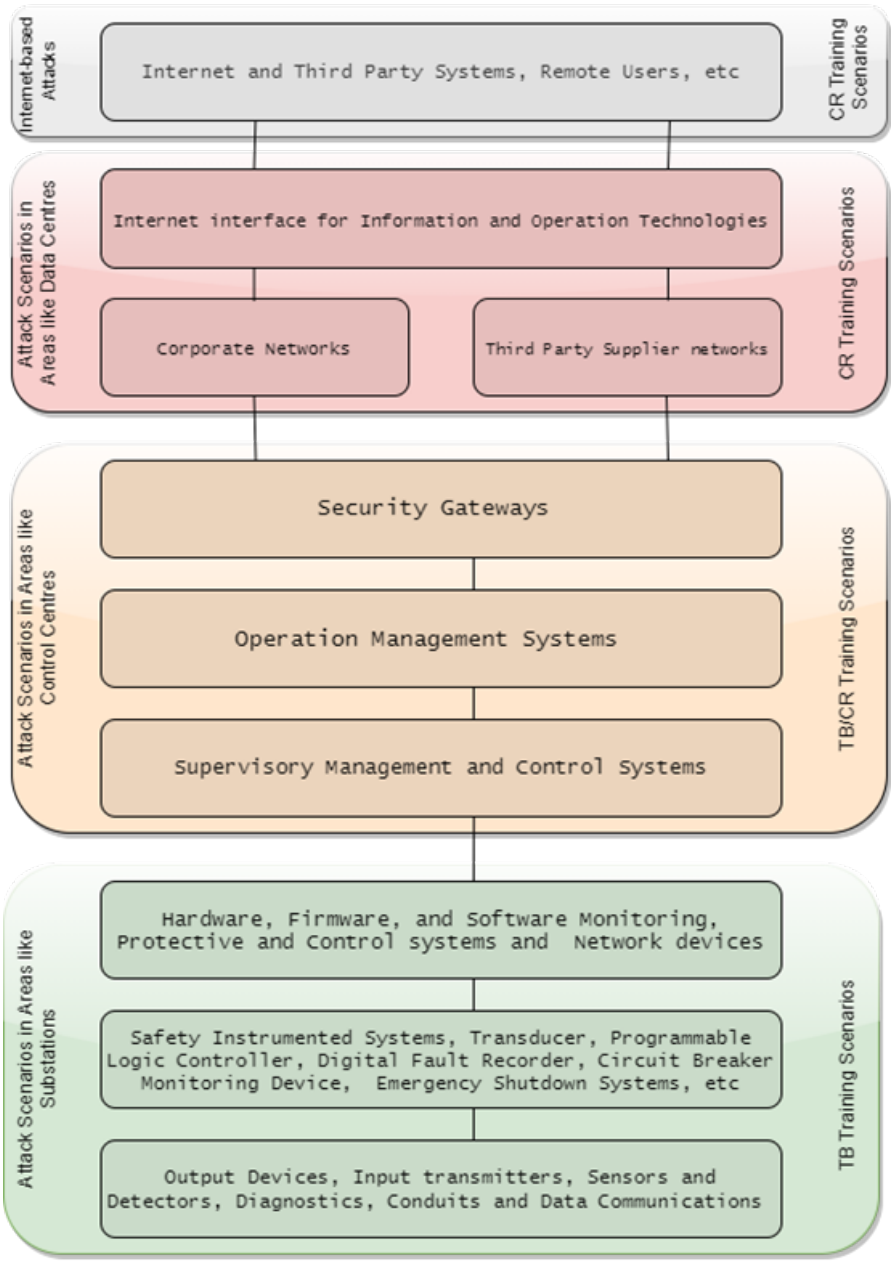


Εικόνα 14: Απεικόνιση ενός βασικού μοντέλου περιγραφής των στοιχείων ενός Cyber Range κατά Yamin et al., όπου λαμβάνονται 5 κύριοι τύποι στοιχείων υπόψη, η διαχείριση, το color teaming, scoring, το σενάριο και το monitoring του περιβάλλοντος CR.[36]



Εικόνα 15: Αναβαθμισμένος τρόπος ταξινόμησης των Cyber Ranges σύμφωνα με τους Yamin et al. με τη διαφορά ότι λαμβάνεται υπόψη το περιβάλλον υλοποίησης και οι εκπαιδευτικές ιδιότητες του συστήματος, αλλά και εκτενέστερα στοιχεία στα επιμέρους κύρια κριτήρια.[36]

Στην Εικόνα 13 απεικονίζεται ένα υβριδικό CR, το οποίο έχει όμως πολλές ομοιότητες με μία κλασική αρχιτεκτονική Virtualization. Αυτό επιτρέπει στα CR να υλοποιούνται πάνω σε γνωστές τεχνικές και τεχνολογίες, επιτρέποντας δε την εύκολη παραμετροποίηση ήδη καλώς γνωστών αρχιτεκτονικών για σκοπούς που εστιάζουν στην εκπαίδευση μέσω των CR. Σε αυτή την περ΄ριπτωση είναι αρκετό να υλοποιηθεί μόνο η διεπαφή με την υποδομή και τα απαραίτητα στοιχεία του CR που επιτρέπουν τη διάδραση “μαθητή” και πλατφόρμας. Στις Εικόνες 14 και 15, οι Yamin et al. παραθέτουν έναν απλό και έναν αναβαθμισμένο τρόπο ταξινόμησης των CRs, αντίστοιχα. Στη δεύτερη περίπτωση είναι έντονο το γεγονός ότι στο κάθε βασικό στοιχείο που ορίζουν στην εργασία τους ως κριτήριο, επιτρέπει στην ταξινόμηση μεγαλύτερο βάθος και λεπτομέρεια. Χαρακτηριστικά, λαμβάνονται υπόψη λεπτομέρειες σε επίπεδο metadata, διεπαφών τρόπου σύνδεσης στην πλατφόρμα, αλλά και το είδος του περιβάλλοντος που χρησιμοποιείται για την εκτέλεση του σεναρίου. Τέλος, στην Εικόνα 16, αναπαρίστανται διάφορες επιθέσεις κατηγοριοποιημένες, η αλληλεπίδραση μεταξύ των στοιχείων του CR ή ενός test bed.



Εικόνα 16: Σενάρια επιθέσεων σε συνάρτηση με ένα CR ή TB και στο επίπεδο το οποίο λαμβάνουν χώρα[34]

3. Kypo Cyber Range (CRP)

Η πλατφόρμα KYPO Cyber Range Platform (KYPO CRP) [42] αναπτύσσεται από το Πανεπιστήμιο Masaryk από το 2013. Το KYPO CRP βασίζεται εξ ολοκλήρου σε σύγχρονες προσεγγίσεις, όπως τα containers, το infrastructure as a Code (IaC), οι microservices και το λογισμικό ανοικτού κώδικα, συμπεριλαμβανομένης της τεχνολογίας παρόχου cloud – OpenStack [75]. Με γνώμονα τις πρακτικές εφαρμογές, το KYPO αναπτύχθηκε με έμφαση στην ικανότητα επαναχρησιμοποίησης (reproducibility), την επεκτασιμότητα, την αυτοματοποίηση και τη διαλειτουργικότητα ενός περιβάλλοντος προσομοίωσης, ώστε να ελαχιστοποιηθούν κατά το μέγιστο οι χειροκίνητες ενέργειες και να καταστούν οι εκπαιδεύσεις στον κυβερνοχώρο προσιτές και οικονομικά αποδοτικές. Ο πηγαίος κώδικας του KYPO CRP προσφέρεται μέσω Gitlab [41] υπό την άδεια MIT. Παρόλα αυτά το KYPO προσφέρεται και με επαγγελματική υποστήριξη για την εγκατάσταση και υλοποίηση μίας αρχιτεκτονικής, για όποια εταιρεία ή άτομο ενδιαφέρεται. Η υλοποίηση της πλατφόρμας KYPO, βασίζεται στις αρχές του Infrastructure as Code (IaC) [22], κάνοντας χρήση τεχνολογιών όπως το Terraform, Ansible, Vagrant και OpenStack. Επιτρέπεται έτσι στον τελικό χρήστη να υλοποιεί ολόκληρα περιβάλλοντα σε μερικά λεπτά από το μηδέν. Όλοι οι στόχοι του KYPO για τον χαρακτήρα της πλατφόρμας υλοποιούνται με χρήση αυτών των τεχνολογιών. Ελαχιστοποιείται ο παράγοντας του ανθρώπινου σφάλματος, προσφέρει ταχύτατες υλοποιήσεις με χρήση αυτοματισμών, τα περιβάλλοντα χαρακτηρίζονται από συνοχή, όποτε αυτά να υλοποιηθούν, μηδενίζεται η διαφορά στην παραμετροποίηση από εκτέλεση σε εκτέλεση, και μειώνεται δραστικά το κόστος. Όλες αυτές οι αρχές, συντελούν στην υιοθέτηση ασφαλών τακτικών και υλοποίηση ασφαλούς περιβάλλοντος. Επιπλέον προσφέρουν διαφάνεια στον τρόπο παραμετροποίησης του περιβάλλοντας και συνήθως ο "κώδικας" είναι αυτοεπεξηγηματικός. Ωστόσο, μπορεί να κρύβουν παγίδες καθώς η τεχνολογική εξειδίκευση είναι εκτεταμένη. Κάθε από τις επιμέρους τεχνολογίες που χρησιμοποιεί το KYPO, απαιτεί βαθιά γνώση για να κατανοηθεί το περιβάλλον υλοποίησης. Ωστόσο απλοποιεί κατά πολύ το στάδιο της υλοποίησης, καθώς οι ενέργειες που απαιτούνται από τον διαχειριστή, είναι σε πολύ υψηλό επίπεδο και προαπαιτούν βασικές γνώσεις. Στην περίπτωση του KYPO-Lite που μπορεί να χρησιμοποιηθεί για να μελετηθούν οι βασικές αρχές του KYPO και να δημιουργηθεί ένα γρήγορο περιβάλλον KYPO, απαιτείται εκτέλεση ελάχιστων εντολών και εντός 40 περίπου λεπτών, η πλατφόρμα είναι έτοιμη για δοκιμές και σενάρια. Παρατηρείται ωστόσο ότι σε πιο

πολύπλοκα περιβάλλοντα, το KYPO παραμένει απαιτητικό σε υπολογιστικούς πόρους για να δουλέψει σε μεγάλη κλίμακα.

Η πλατφόρμα του KYPO CRP επικεντρώνεται σε δύο περιπτώσεις χρήσης:

1. Σε **Εξομοιωμένο εικονικό περιβάλλον (emulated virtual environment)**: τη δημιουργία και παροχή ενός περιβάλλοντος για την εξομοίωση υπολογιστικών υποδομών σε ελεγχόμενο περιβάλλον για την επίτευξη υψηλής ευελιξίας, επεκτασιμότητας, απομόνωσης και φορητότητας. Η πλατφόρμα επιτρέπει τη δημιουργία εικονικών δικτύων με ένα πλήρες λειτουργικό σύστημα και συσκευές δικτύου που προσομοιώνουν συστήματα του πραγματικού κόσμου.
2. **Εκπαιδεύσεις (Trainings)**: Εκτέλεση ταυτόχρονων εκπαιδευτικών συνεδριών ως παιχνίδια κυβερνοασφάλειας που συμπληρώνονται από αξιολόγηση των συμμετεχόντων. Το KYPO CRP επιτρέπει στους εκπαιδευτές να δημιουργούν εκπαιδευτικά σενάρια και στους εκπαιδευόμενους να συμμετέχουν στις συνεδρίες στο προσομοιωμένο εικονικό περιβάλλον που παρέχεται από το KYPO CRP. Οι εκπαιδευτές μπορούν εύκολα να δημιουργήσουν πολλαπλές εκφάνσεις (instances) της ίδιας εκπαίδευσης και του ίδιου εικονικού περιβάλλοντος για δεκάδες ή εκατοντάδες συμμετέχοντες μέσω της διεπαφής web και να παρακολουθούν την πρόοδό των εκπαιδευόμενων στον πίνακα ελέγχου.

Επιπλέον, το KYPO CRP παρέχει τη δυνατότητα διαχείρισης χρηστών. Αυτή η δυνατότητα αποτελεί ουσιαστικό μέρος της πλατφόρμας, διότι επιτρέπει να περιορίζεται η μη εξουσιοδοτημένη πρόσβαση στις στα εκπαιδευτικά σενάρια και τα εξομοιωμένα εικονικά περιβάλλοντα. Το KYPO χρησιμοποιεί συγκεκριμένη ορολογία για να περιγράψει τις λειτουργίες και τα στοιχεία που αποτελούν το περιβάλλον του και ακολουθεί σχετική περιγραφή.

3.1 Αρχιτεκτονικός σχεδιασμός KYPO CRP

Αποθετήρια Git

Τα αποθετήρια Git χρησιμοποιούνται για την αποθήκευση δημιουργημένων sandbox definitions που μπορούν να χρησιμοποιηθούν σε περιβάλλον cloud, σε τοπικό περιβάλλον ή και στις δύο περιπτώσεις. Και στις δύο περιπτώσεις, φορτώνονται από τη συγκεκριμένη μικρουπηρεσία (microservice) της πύλης KYPO, ώστε να μπορούν αργότερα να

χρησιμοποιηθούν για τη δημιουργία στιγμιοτύπων sandbox στο σύννεφο ή για την εμφάνιση της τοπολογίας των τοπικών sandbox. Η πρόσβαση στο Git ρυθμίζεται κατά την εγκατάσταση του KYPO CRP.

Χρήστες

Οι χρήστες έχουν διαφορετικούς ρόλους με διαφορετικά πεδία εργασίας εντός του KYPO CRP. Μπορούν να δημιουργούν και να διαχειρίζονται εκπαιδεύσεις, να διαχειρίζονται άλλους χρήστες μέσω των ορισμών sandboxes και είναι επίσης υπεύθυνοι για το σχεδιασμό των sandboxes. Οι χρήστες μπορούν να έχουν πρόσβαση στα μηχανήματα στα sandboxes του cloud χρησιμοποιώντας τον client Spice [76], την πύλη απομακρυσμένης επιφάνειας εργασίας Apache Guacamole [77] ή απευθείας μέσω SSH [78]. Από την άλλη πλευρά, οι χρήστες μπορούν να έχουν πρόσβαση στα τοπικά sandboxes απευθείας χρησιμοποιώντας τη συγκεκριμένη εντολή vagrant [19], [79].

Πύλη KYPO

Αποτελεί μια γραφική διεπαφή χρήστη για την απλή αλληλεπίδραση των χρηστών με το KYPO CRP, την εύκολη πρόσβαση στα cloud sandboxes και στις άλλες λειτουργίες. Αντιπροσωπεύει τον διαμεσολαβητή μεταξύ των χρηστών και των μικρουπηρεσιών που εκτελούνται στο παρασκήνιο. Για πιο λεπτομερείς πληροφορίες σχετικά με τις μικρουπηρεσίες, ανατρέξτε στην ενότητα Στοιχεία πλατφόρμας.

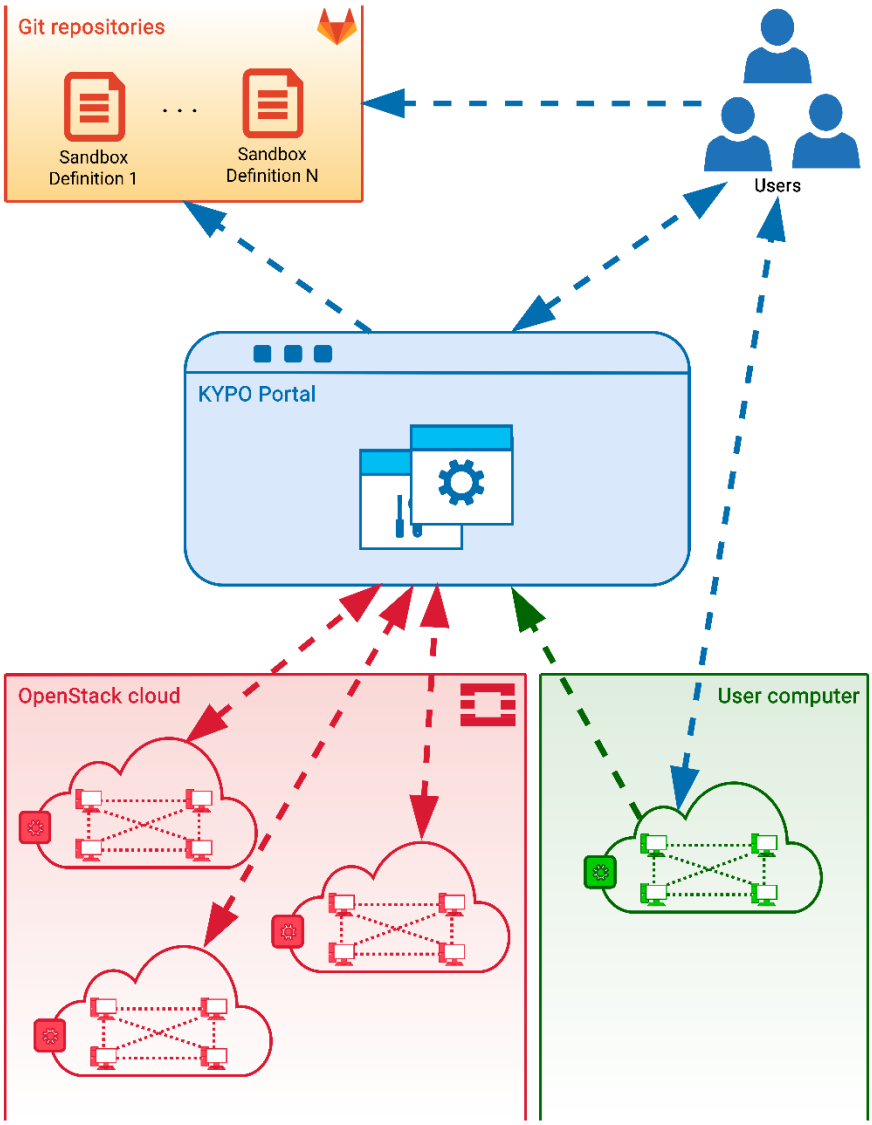
Cloud

Η μηχανή του περιβάλλοντος KYPO CRP βασίζεται κυρίως στην πλατφόρμα νέφους OpenStack [75]. Ελέγχει μεγάλες δεξαμενές υπολογιστικών, αποθηκευτικών και δικτυακών πόρων που διαχειρίζεται μέσω APIs ή ενός ταμπλό. Αναπτύσσεται κυρίως ως υποδομή ως υπηρεσία (Infrastructure as a Service – IaaS) σε δημόσια και ιδιωτικά νέφη, όπου διατίθενται εικονικοί διακομιστές και άλλοι πόροι στους χρήστες.

Local

Ως εναλλακτική λύση για τα sandboxes του cloud, τα τοπικά sandboxes μπορούν να δημιουργηθούν στον υπολογιστή του χρήστη χρησιμοποιώντας VirtualBox [80] και Vagrant [79]. Αυτό εξοικονομεί πόρους του νέφους και επιτρέπει τη δημιουργία εκπαιδεύσεων με μεγάλο αριθμό χρηστών με μικρές μόνο διαφορές. Απαιτεί αλληλεπίδραση του χρήστη ο οποίος πρέπει να κλωνοποιήσει το αποθετήριο ορισμού του sandbox και να εκτελέσει μια

εντολή για τη δημιουργία ενός sandbox. Επίσης, ο υπολογιστής του χρήστη πρέπει να πληροί τις απαιτήσεις υλικού και εικονικοποίησης.



Εικόνα 17 Αρχιτεκτονικός σχεδιασμός KYPO CRP[81]

Επισκόπηση

Πριν από την έναρξη μιας εκπαιδευτικής διαδρομής, πρέπει να εκτελεστούν διάφορα βήματα. Αυτά τα βήματα δεν εκτελούνται απαραίτητα από έναν μόνο χρήστη και συνήθως κατανέμονται σε διάφορους χρήστες με ρόλο εκπαιδευτή. Ολόκληρη η ροή εργασιών για τη δημιουργία εκπαίδευσης εξαρτάται από τον τύπο των χρησιμοποιούμενων sandboxes (cloud ή τοπικά). Σε γενικές γραμμές, η ροή εργασίας χωρίζεται σε δύο μέρη, καθώς περιλαμβάνει και τη δημιουργία των sandboxes.

3.2 Εξομοιωμένο εικονικό περιβάλλον (emulated virtual environment) στο KYPO

Όταν δημιουργούμε και χρησιμοποιούμε ένα εξομοιωμένο εικονικό περιβάλλον, χρησιμοποιείται η ακόλουθη ορολογία:

- ***Sandbox***: Πρόκειται για ένα απομονωμένο περιβάλλον δοκιμών με εικονικά δίκτυα που επιτρέπουν στους χρήστες να συνδέονται στα virtual machines (VM) και να επικοινωνούν με το υπόλοιπο δίκτυο, το host, και άλλα VM. Στα VMs, ο χρήστης μπορεί να εκτελεί προγράμματα, να χρησιμοποιεί υπηρεσίες δικτύου ή να παρακολουθεί την κυκλοφορία του δικτύου. Όλα αυτά χωρίς να επηρεάζεται η εξωτερική υποδομή. Διακρίνονται δύο τύποι *sandboxes*:
  - **Cloud** – το sandbox εκτελείται εντός του cloud και είναι προσβάσιμο από απόσταση.
  - **Local** – το sandbox δημιουργείται τοπικά στον υπολογιστή του χρήστη χρησιμοποιώντας το *Vagrant* [79], [82](ένα εργαλείο που επιτρέπει τη δημιουργία και διαχείριση περιβάλλοντος VM με μία απλή διεργασία/workflow και αυτοματισμό) μαζί με το εργαλείο εικονικοποίησης *VirtualBox*.

3.3 KYPO Sandbox definition

Sandbox Definition: Είναι ο Ορισμός της εσωτερικής δομής των sandboxes (δίκτυα και hosts) και της παραμετροποίησης των hosts από τον χρήστη. Αποτελείται από δύο μέρη: Τον ορισμό της τοπολογίας (Topology Definition) και την Παροχή Sandbox (Sandbox Provisioning).
Είναι μία δομή φακέλου αποθηκευμένη ως αποθετήριο κώδικα που διαχειρίζεται από το ίδιο το KYPO τοπικά και ορίζει την τοπολογία και παροχή πόρων για τους κόμβους του sandbox. Όταν υλοποιηθεί (deploy) στο cloud ένα topology.yaml, λέγεται πλέον topology instance [83].

```
sandbox-definition/
├── topology.yml
├── variables.yml
└── provisioning/
    └── playbook.yml
└── preconfig/
```

- **variables.yml**: είναι ένα αρχείο παραμετροποίησης με όλα τα απαραίτητα και προαιρετικά στοιχεία για τη δημιουργία μεταβλητών APG [84], που χρησιμοποιούνται

για τη δημιουργία ποικίλων απαντήσεων για τα sandboxes που συμμετέχουν στο pool. Είναι απαραίτητες για τις σενάρια εκπαιδευσης APG.

- **Provisioning**: μία δομή φακέλου για αρχεία yaml, ενός sandbox provisioning που επιτρέπει την παραμετροποίηση μίας Topology instance. Μόλις παραχθεί, ονομάζεται sandbox.
- **Preconfig** (μόνο για local sandbox definition): περιλαμβάνει αρχεία για τη βασική παραμτεροποίηση των συσκευών που δημιουργήθηκαν (π.χ. παραμετροποίηση δικτύου)

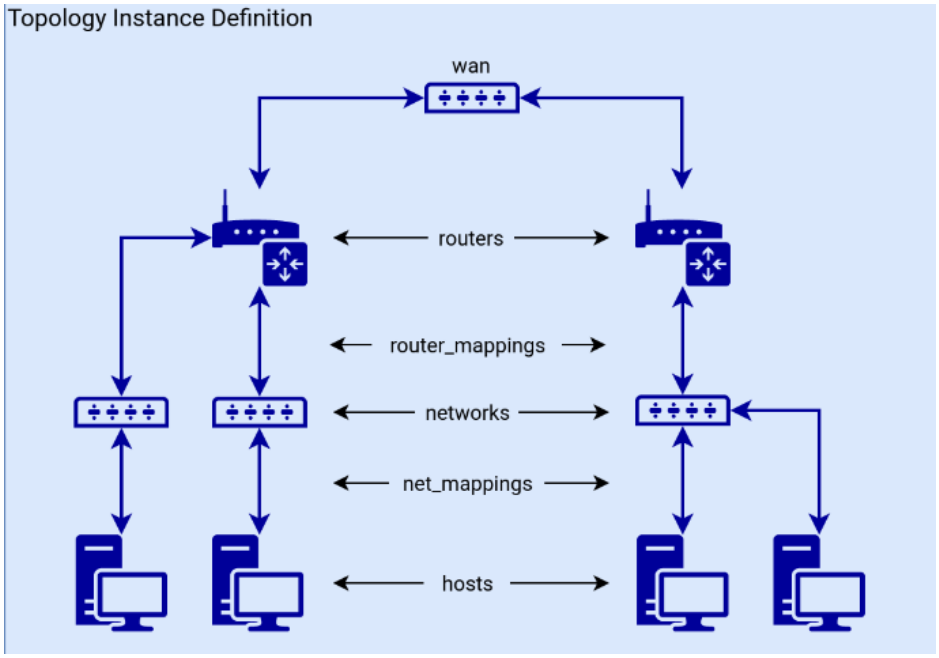
3.4 KYPO Topology Definition

Το αρχείο με τον ορισμό της δομής του sandbox (hosts, routers, networks, κλπ) αποτελείται από διάφορα χαρακτηριστικά (attributes) ου περιγράφονται σε αρχεία yaml. Περιγράφονται τα ονόματα των hosts, το είδος του openstack flavor [85] , το είδος του image, πληροφορίες για τους χρήστες και διαχειριστές, τα πρωτόκολλα σε χρήση και πληροφορίες σχετικές με τη δέσμευση πόρων, όπως χωρητικότητα δίσκων. Επιπλέον τα στοιχεία δικτύου, όπως η λίστα των routers, περιγράφεται κατά παρόμοιο τρόπο.

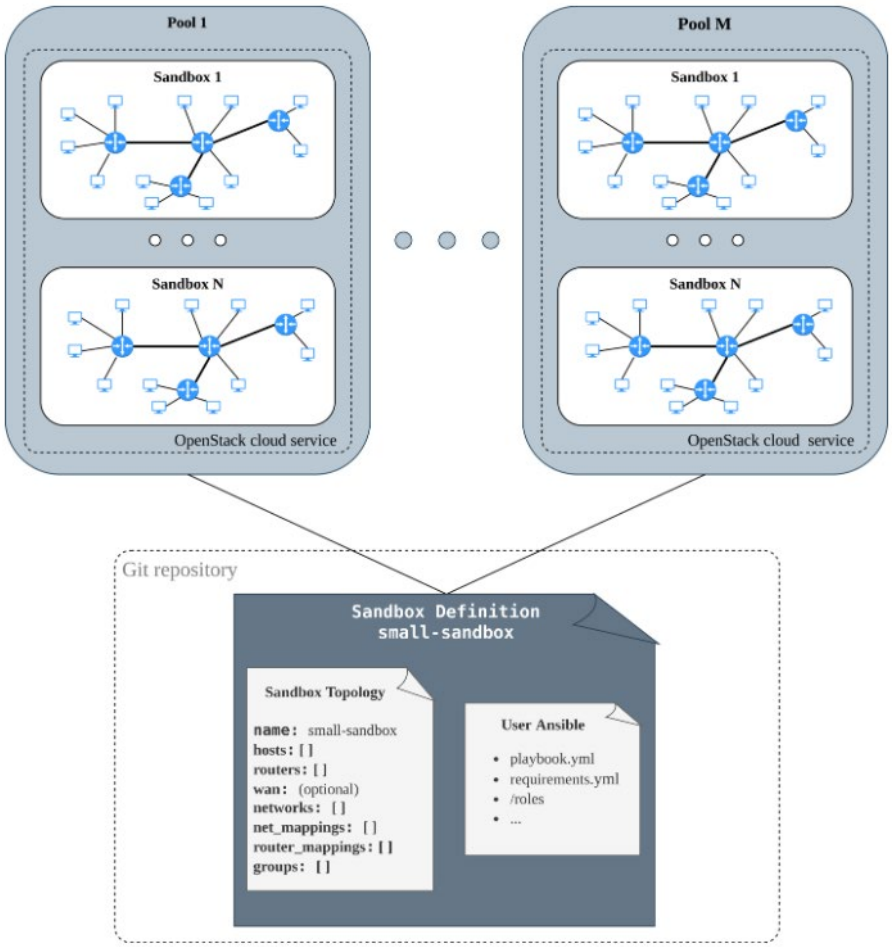
Pool : Αποτελεί μια ομάδα cloud sandboxes που δημιουργείται με βάση το ίδιο sandbox definition. Πριν από τη δημιουργία cloud sandboxes, είναι απαραίτητο να δημιουργηθεί το σύστημα τις λεγόμενες δεξαμενές (pools). Τα pools είναι ομάδες sandboxes που δημιουργούνται με βάση τον ίδιο sandbox definition. Πριν από τη δημιουργία της δεξαμενής (pool) καθορίζεται το (sandbox) definition. Μετά τη δημιουργία του pool, είναι δυνατόν να ξεκινήσει η κατανομή των sandboxes, η οποία χωρίζεται σε τρεις φάσεις:

1. **Sandbox Allocation**: Δημιουργία sandbox (εικονικές μηχανές) μέσα στο cloud.
2. **Sandbox networking**: Δικτύωση των VMs και διανομή κλειδιών χρήστη στις μηχανές. Η φάση αυτή εκτελείται αυτόματα και δεν αποτελεί ευθύνη του χρήστη.
3. **Sandbox Provisioning**: Προσαρμογή των VMs που προαναφέρθηκαν.

Στην Εικόνα 20, φαίνεται ο τρόπος με τον οποίο δημιουργείται ένα sandbox στο KYPO, ορίζοντας με yaml τα κύρια στοιχεία της αρχικτεκτονικής του. Ορίζεται το όνομα και τα υπολογιστικά χαρακτηριστικά του sandbox (cpu, ram, openstack flavor). Ορίζονται επιπλέον τα στοιχεία του δικτύου (routers) και η διεπαφή wan, όπως και τα network mappings με τα αντίστοιχα δικαιώματα πρόσβασης που ανατίθενται στους χρήστες.



Εικόνα 18: Απεικόνιση του Topology Instance Definition [86]



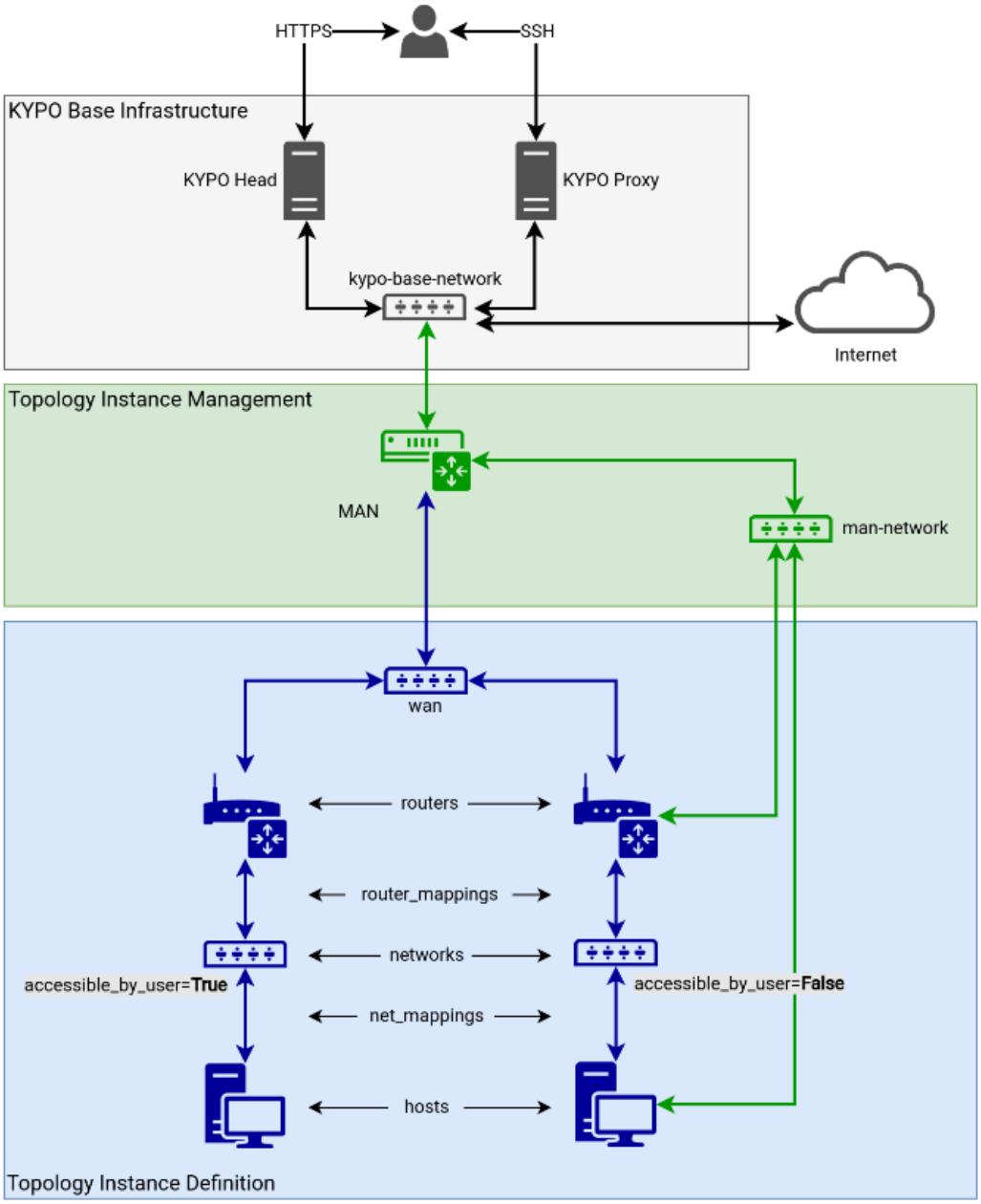
Εικόνα 19: Περιγραφή ενός pool υπολογιστικών στοιχείων, όπου διακρίνεται η συσχέτιση και το επίπεδο του sandbox definition, του sandbox και πως συγκροτούν ένα pool.[83]

```
name: small-sandbox
hosts:
  - name: server
    base_box:
      image: debian-9-x86_64
      mgmt_user: debian
    flavor: csirtmu.tiny1x2
    hidden: True
    volumes:
      - size: 16
      - size: 2
      - size: 9

  - name: home
    base_box:
      image: windows-10-0.2.0
      mgmt_user: windows
      mgmt_protocol: wirm
    flavor: csirtmu.tiny1x2

routers:
  - name: server-router
    base_box:
      image: debian-9-x86_64
      mgmt_user: debian
    flavor: csirtmu.tiny1x2

  - name: home-router
    base_box:
      image: debian-9-x86_64
      mgmt_user: debian
    flavor: csirtmu.tiny1x2

wan:
  name: internet-connection
  cidr: 100.100.100.0/24

networks:
  - name: server-switch
    cidr: 10.10.20.0/24
    accessible_by_user: False

  - name: home-switch
    cidr: 10.10.30.0/24

net_mappings:
    - host: server
      network: server-switch
      ip: 10.10.20.5β

    - host: home
      network: home-switch
      ip: 10.10.30.5

router_mappings:
    - router: server-router
      network: server-switch
      ip: 10.10.20.1

    - router: home-router
      network: home-switch
      ip: 10.10.30.1

groups:
  - name: custom-group
    nodes:
      - home
      - home-router
```

Εικόνα 20: Παράδειγμα κώδικα σε yaml, όπου περιγράφει τη δημιουργία ενός sandbox, με τα δομικά στοιχεία του και τις πληροφορίες απαραίτητες στην πλατφόρμα OpenStack.

3.5 KYPO Topology Instance

Ο terraform client του KYPO, μετατρέπει ένα topology definition (user-defined), μέσω της **Topology Instance Management** υποδομής σε terraform template, το οποίο *χρησιμοποιείται* για τη δημιουργία της εικονικής υποδομής που ονομάζεται *KYPO Topology Instance.* Το Terraform είναι ένα εργαλείο IaC, το οποίο επιτρέπει τη δημιουργία, την παραμετροποίηση υποδομών κατά αυτοματοποιημένο τρόπο, παρέχοντας versioning και επιτρέποντας επαναχρησιμοποίηση και διαμοιρασμό των παραμέτρων. Είναι εργαλείο ανοιχτού κώδικα, που μεταφράζει σε κώδικα APIs σε declarative αρχεία παραμετροποίησης [21].



Εικόνα 21: Απεικόνιση της δομής ενός KYPO Topology Instance, όπου ιακρίνεται η βασική υποδομή που απαιτεί το KYPO, το διαχειριστικό επίπεδο και ο ορισμός που περιγράφει την αλληλεπίδραση των instances.[86]

3.6 KYPO Topology Instance Management

Κάθε **Topology Instance** δημιουργείται με μία υποδομή υπεύθυνη για τη διαχείριση (management), σε λογικό επίπεδο τοποθετείται ανάμεσα στην KYPO Base Infrastructure και το Topology Instance, και αποτελείται από τα εξής:

- **MAN (Management Access Node, κόμβος πρόσβασης διαχείρισης**): Ο μοναδικός κόμβος που συνδέεται με το δίκτυο εκτός του Topology Instance. Το δίκτυο πρέπει να καθοριστεί ως base_network στη διαμόρφωση της υπηρεσίας sandbox. Το Topology Instance είναι προσβάσιμο μόνο μέσω του hypervisor του νέφους OpenStack ή του MAN.
- **man-network (management network, δίκτυο διαχείρισης)**: Όλοι οι κόμβοι του Topology Instance συνδέονται σε αυτό το δίκτυο, ώστε κάθε κόμβος να είναι προσβάσιμος από το MAN και να μπορεί να ρυθμιστεί μέσω αυτού. Το CIDR αυτού του δικτύου θα πρέπει να καθορίζεται στη διαμόρφωση. Το εύρος διευθύνσεων IP αυτού του δικτύου μπορεί να παρακαμφθεί στη διαμόρφωση της υπηρεσίας sandbox-service.

3.7 KYPO Sandbox Provisioning και Sandbox Access

Στο KYPO παρέχεται η δυνατότητα να παραμετροποιηθεί το Topology Instance, κατά τη διάρκεια του provisioning. Μπορεί να χρησιμοποιηθεί για να εγκατασταθεί το περιβάλλον, ή για δημιουργία χρηστών, εγκατάσταση πακέτων και εφαρμογών, κλπ. Χρησιμοποιείται Ansible [20], για την υλοποίηση και ακολουθούνται οι βασικές αρχές και η δομή φακέλου ενός Ansible playbook. Η Ansible είναι βασισμένη σε YAML, είναι ανοιχτού κώδικα και χρησιμοποιείται σε παραμετροποίηση συστημάτων, στην εγκατάσταση λογισμικού και στην υλοποίηση αυτοματοποιημένων ροών διεργασιών. βασίζει την διάδραση και επικοινωνία με τα συστήματα στο πρωτόκολλο ssh, κάνοντάς την ιδιαίτερα ασφαλές εργαλείο.Κύριο χαρακτηριστικό της είναι το idempotency, δηλαδή τη δυνατότητα να εκτελείται μία συγκεκριμένη ενέργεια επανειλλημένα και να παράγεται το ίδιο πάντα αποτέλεσμα στον στόχο[20], [87], [88].

```
all:
  hosts:
    home:
      ansible_host: 192.168.128.3
      ansible_user: windows
      user_network_ip: 10.10.30.5
    home-router:
      ansible_host: 192.168.128.7
      ansible_user: debian
      interfaces:
      - def_gw_ip: 100.100.100.1
        mac: 00:00:00:00:00:16
        routes: []
      ip_forward: true
      user_network_ip: 10.10.30.1
    kypo-proxy-jump:
      ansible_host: jump-host-ip
      ansible_user: debian
      user_access_mgmt_name: pool-prefix
      user_access_present: true
      user_access_user_name: stack-name
    man:
      ansible_host: 10.10.10.10
      ansible_user: kypo-man
      interfaces:
      - def_gw_ip: ''
        mac: 00:00:00:00:00:02
        routes:
        - gw: 100.100.100.2
          mask: 255.255.255.0
          net: 10.10.20.0
        - gw: 100.100.100.3
          mask: 255.255.255.0
          net: 10.10.30.0
      ip_forward: true
    server:
      ansible_host: 192.168.128.2
      ansible_user: debian
      user_network_ip: 10.10.20.5
    server-router:
      ansible_host: 192.168.128.6
      ansible_user: debian
      interfaces:
      - def_gw_ip: 100.100.100.1
        mac: 00:00:00:00:00:13
        routes: []
      ip_forward: true
      user_network_ip: 10.10.20.1
  children:
    custom-group:
      hosts:
```

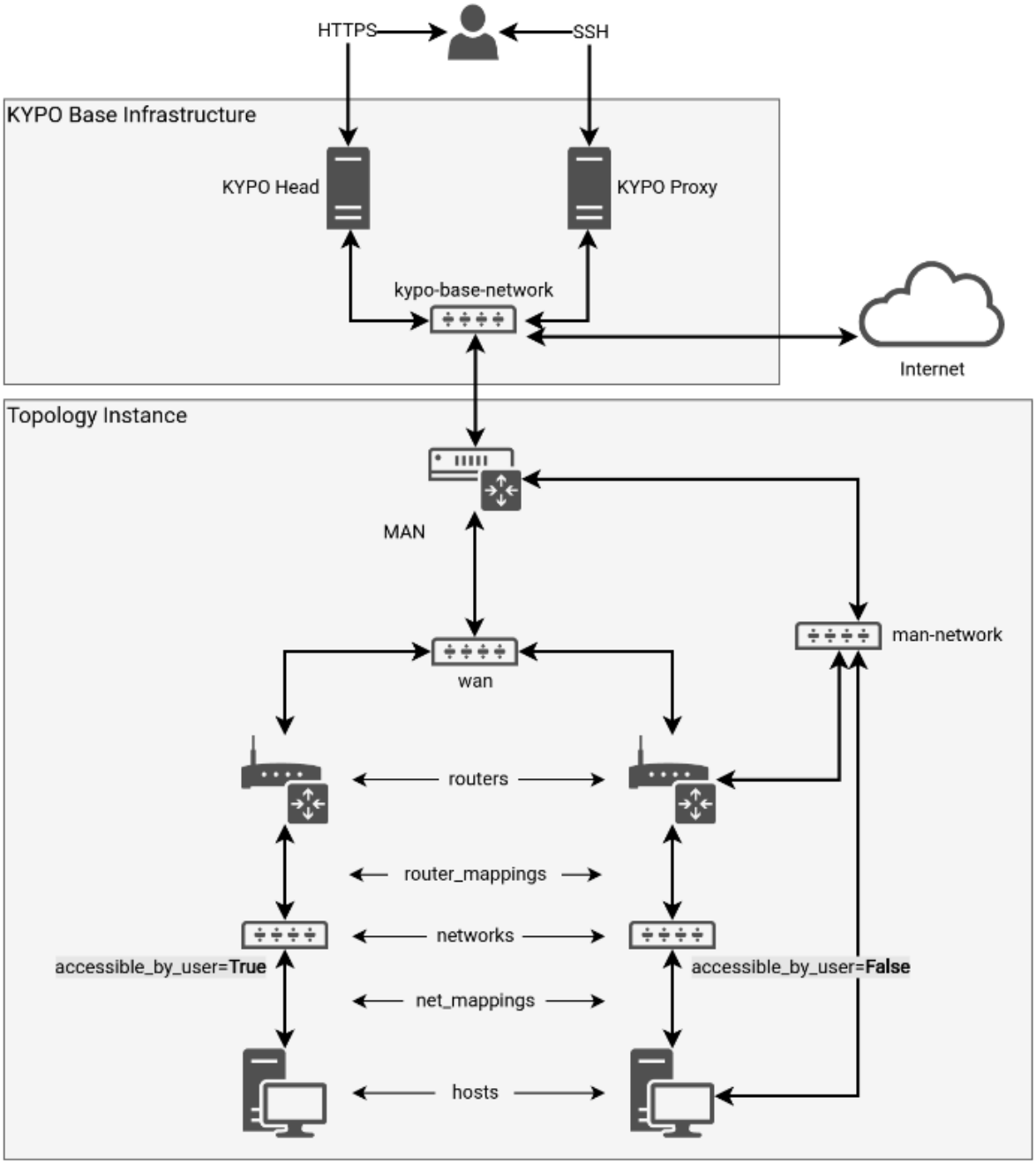
```
        home: null
        server-router: null
    hidden_hosts:
      hosts:
        server: null
    hosts:
      hosts:
        home: null
        server: null
    management:
      hosts:
        man: null
    routers:
      hosts:
        home-router: null
        server-router: null
    ssh_nodes:
      hosts:
        home-router: null
        server: null
        server-router: null
    user_accessible_nodes:
      hosts:
        home: null
        home-router: null
    winrm_nodes:
      hosts:
        home: null
      vars:
        ansible_connection: psrp
        ansible_psrp_auth: certificate
        ansible_psrp_cert_validation: ignore
        ansible_psrp_certificate_key_pem: /root/.ssh/pool_mng_key
        ansible_psrp_certificate_pem: /root/.ssh/pool_mng_cert
        ansible_psrp_proxy: socks5://localhost:12345
  vars:
    kypo_global_head_ip: 0.0.0.0
    kypo_global_openstack_stack_id: heatstack-stack-id
    kypo_global_pool_id: 1
    kypo_global_sandbox_allocation_unit_id: 1
    kypo_global_sandbox_ip: 10.10.10.10
    kypo_global_sandbox_name: stack-name
    kypo_global_ssh_public_mgmt_key: /root/.ssh/pool_mng_key.pub
    kypo_global_ssh_public_user_key: /root/.ssh/user_key.pub
```

Εικόνα 22: Block κώδικα ansible σε yaml, που περιγράφει την υλοποίηση και provisioning των υπολογιστικών πόρων για τη δημιουργία ενός sandbox στο KYPO CRP. Ορίζονται διευθύνσεις IP, τα κύρια στοιχεία του KYPO, όπως kypo-proxy jump, το δίκτυο man, και οι ρυθμίσεις δικτύου και διαχείρισης.[83]

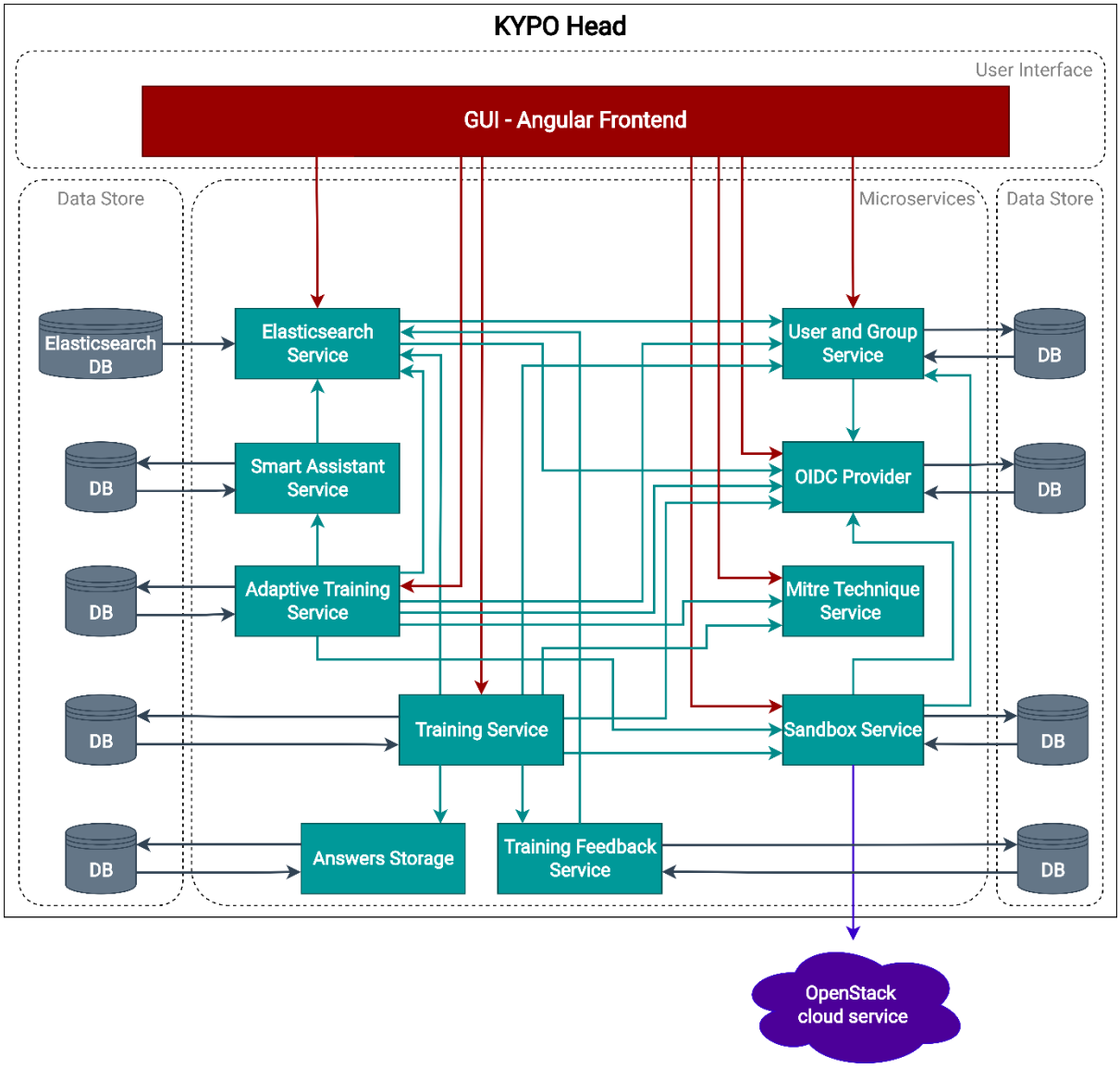
Ένα Topology instance του sandbox δημιουργείται στην πλατφόρμα cloud και συνδέεται στην βασική υποδομή του KYPO (KYPO Base Infrastructure), που αποτελείται κυρίως από 2 servers και ένα δίκτυο:

- **KYPO Head**: ο διακομιστής όπου εγκαθίσταται η πλατφόρμα KYPO.
- **KYPO Proxy**: ο διακομιστής χρησιμοποιείται μόνο για να διαχειρίζεται την πρόσβαση ssh σε όλα τα sandbox.
- **KYPO Base Network**: Το δίκτυο όπου και οι δύο διακομιστές και όλα τα sandboxes είναι συνδεδεμένα μέσω κόμβων MAN.

Η πρόσβαση μπορεί να επιτευχθεί είτε με ssh, rdp και vnc συνδέσεις, είτε με web-based (apache wuacamole, spice). Υπάρχει διαχωρισμός βάσει δικαιωμάτων πρόσβασης και διαχωρίζεται σε δύο βασικούς τύπους: management access (instructor) και user access (trainee)



Εικόνα 23: Τοπολογία βασικής υποδομής KYPO CRP, αποτελείται από έναν κύριο server KYPO Head, ένα proxy, KYPO PROXY και ένα δίκτυο, KYPO base network.[89]



Εικόνα 24: Στοιχεία πλατφόρμας KYPO, όπου χρησιμοποιείται η αρχιτεκτονική των microservices.[90]

4. Εκπαίδευση με χρήση του KYPO CRP και περιγραφή ορολογίας

Η εκπαίδευση KYPO επικεντρώνεται γύρω από ένα sandbox, όπου οι εκπαιδευόμενοι επιλύουν εργασίες που παρουσιάζονται στο KYPO GUI. Η εκπαίδευση με το KYPO μπορεί επίσης να περιλαμβάνει ερωτηματολόγια για τη συλλογή σχολίων από τους εκπαιδευόμενους ή τεστ για την αξιολόγηση των γνώσεών τους [91]. Στο πλαίσιο της εκπαίδευσης, χρησιμοποιούμε την ακόλουθη ορολογία:

Training definition: Καθορίζει το σενάριο της κατάρτισης. Με βάση τον τύπο τους, οι ορισμοί μπορούν να αποτελούνται είτε από επίπεδα είτε από φάσεις. Οι γραμμικοί ορισμοί μπορούν να περιέχουν επίπεδα κατάρτισης, επίπεδα αξιολόγησης και επίπεδα πληροφοριών. Οι προσαρμοστικοί ορισμοί μπορούν να αποτελούνται από φάσεις κατάρτισης, φάσεις ερωτηματολογίου και φάσεις πληροφοριών.

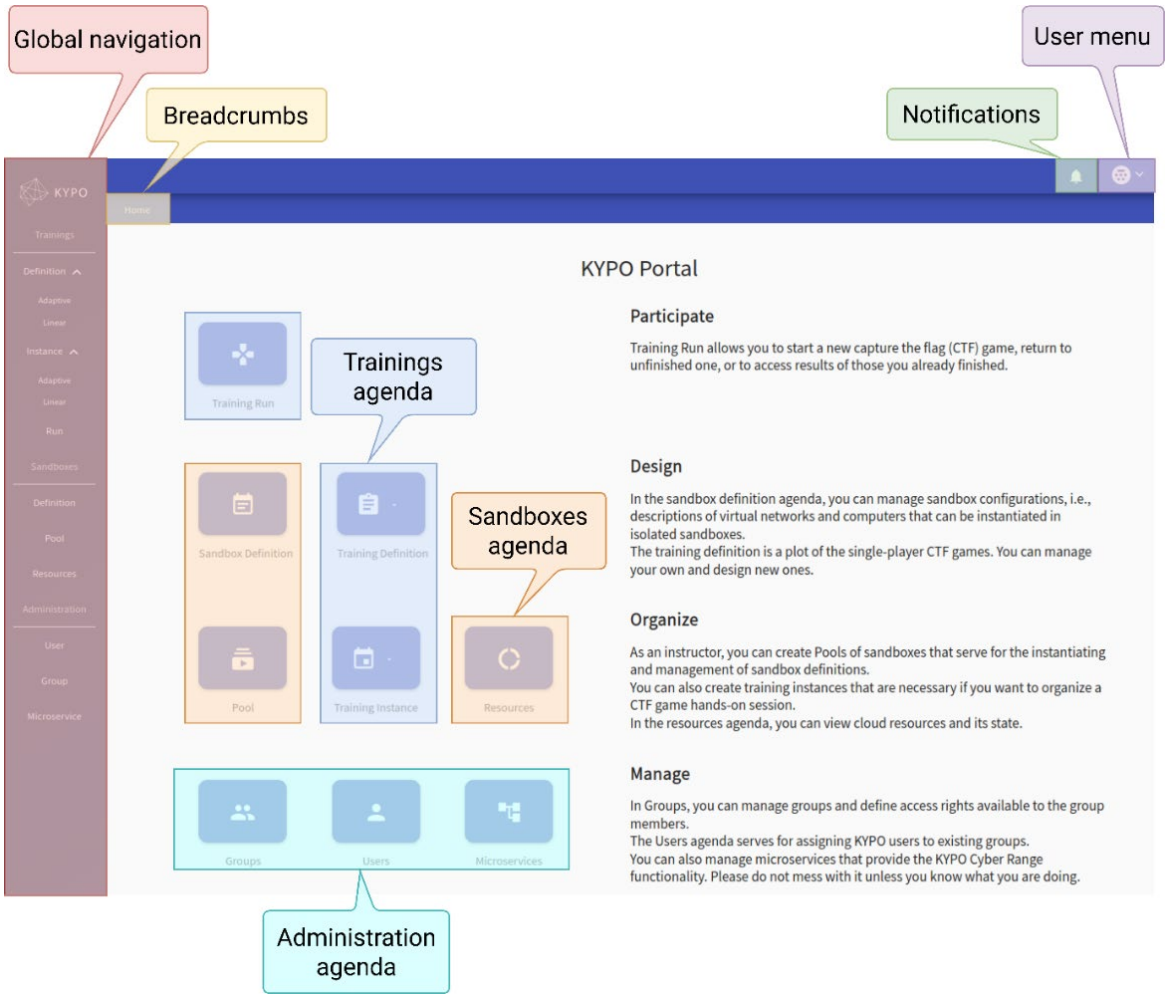
Training Example: Καθορίζει τη χρονική περίοδο κατά την οποία οι παίκτες μπορούν να έχουν πρόσβαση στην εκπαίδευση. Κάθε περίπτωση κατάρτισης ορίζεται επίσης σε ένα από τα ακόλουθα περιβάλλοντα:

Cloud Environment (περιβάλλον νέφους) (προεπιλογή) - κατά τη διάρκεια της εκπαίδευσης χρησιμοποιούνται cloud sandboxes. Πρέπει να εκχωρηθεί ένα pool από sandboxes στην περίπτωση εκπαίδευσης.

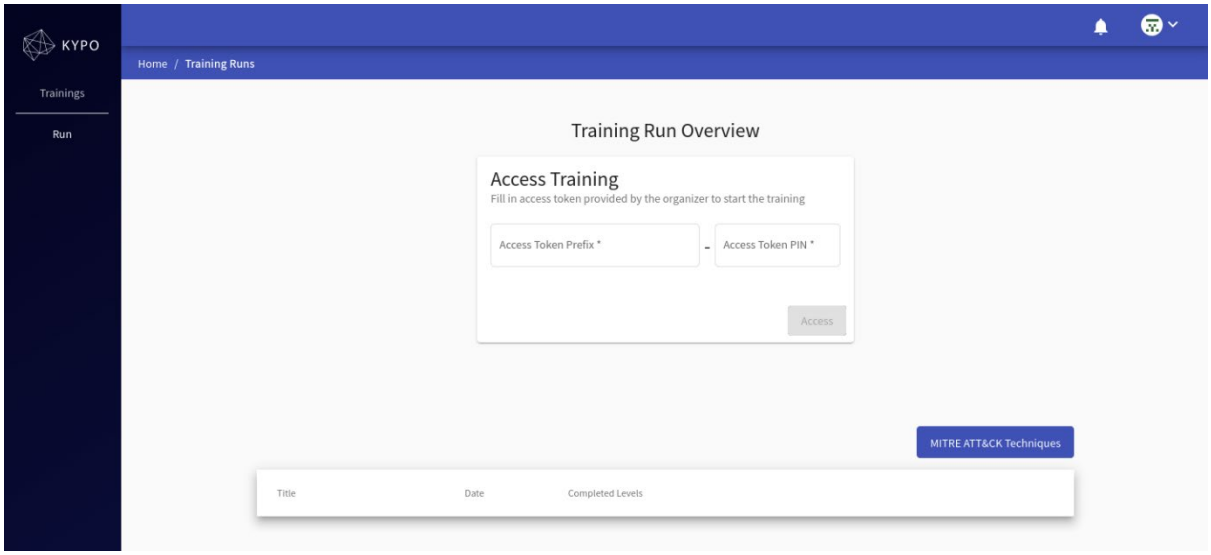
Local Environment (Τοπικό περιβάλλον)- κατά τη διάρκεια της εκπαίδευσης χρησιμοποιούνται τοπικά sandboxes. Ένας ορισμός sandbox μπορεί να εκχωρηθεί στην εκπαιδευτική περίπτωση, ώστε οι εκπαιδευόμενοι να μπορούν να ρίξουν μια ματιά στην τοπολογία.

Training Run: Είναι η μεμονωμένη εκτέλεση της εκπαίδευσης του συγκεκριμένου εκπαιδευόμενου. Κάθε εκτέλεση έχει ένα καθορισμένο sandbox από το pool ή χρησιμοποιεί το δικό του τοπικό sandbox.

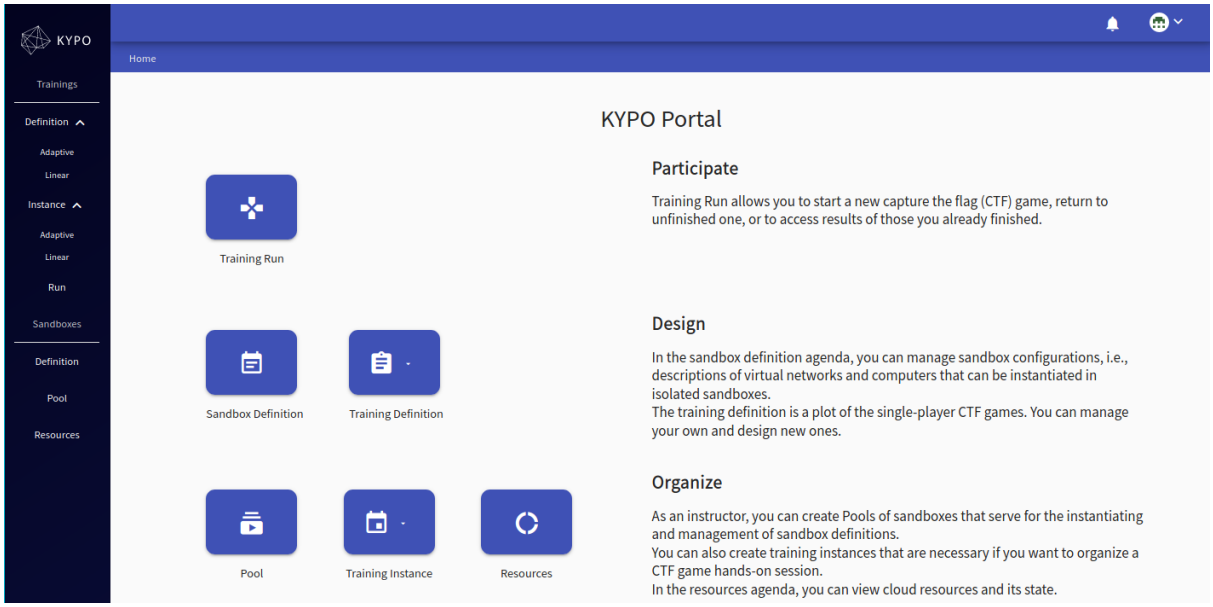
Ακολουθούν κάποια στιγμιότυπα από το γραφικό περιβάλλον του KYPO, με τα μενού περιήγησης και τα μενού χρήστη. Το περιβάλλον είναι ιδιαίτερα φιλικό προς το χρήστη και διαχωρίζει την εμφάνιση των επιλογών ανάλογα με το επίπεδο και είδος πρόσβασης (user, admin, trainee, κλπ). Οι διαθέσιμοι ορισμοί των sandbox και των trainings είναι επίσης διαθέσιμοι. Είναι σημαντικό να τονίσουμε, ότι η δημιουργία σεναρίων και προετοιμασία της υποδομής sandbox, προσφέρεται και μέσω GUI.



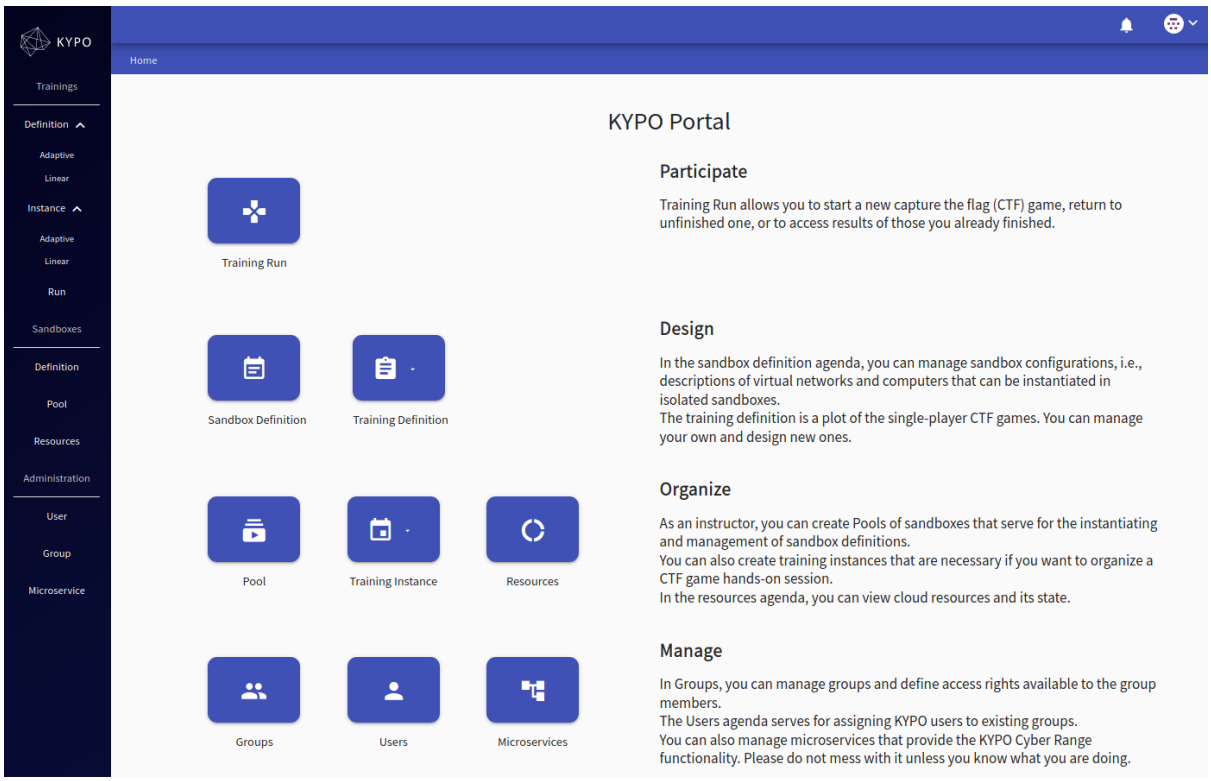
Εικόνα 25: Αρχική σελίδα (homepage) του KYPO CRP [91]



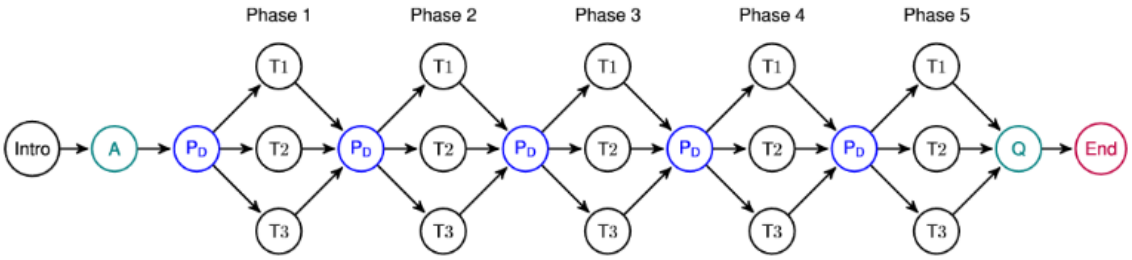
Εικόνα 26: Στιγμιότυπο αρχικής σελίδας ενός εκπαιδευόμενου στο KYPO



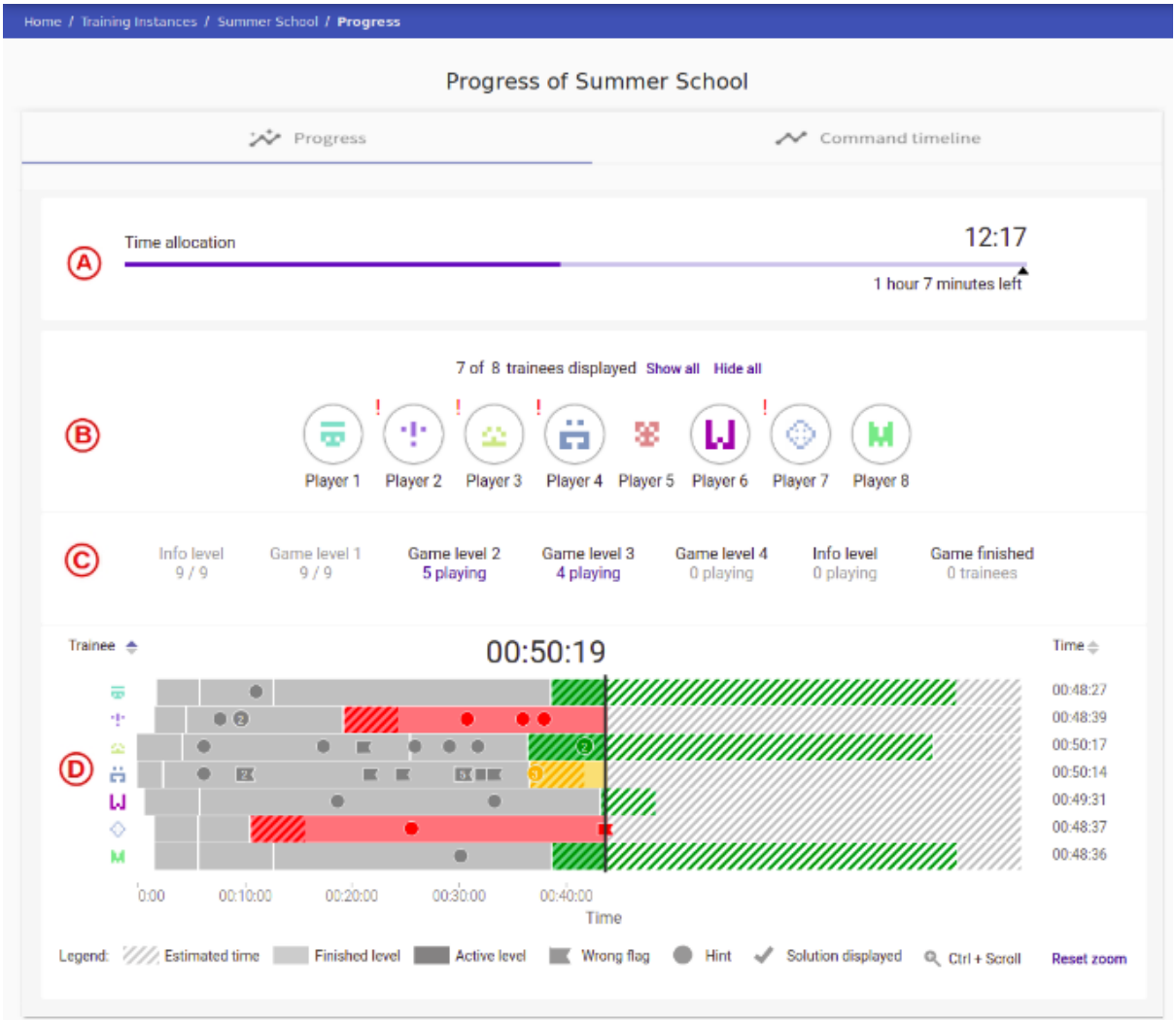
Εικόνα: 27 Στιγμιότυπο (2) εκπαιδευόμενου στο KYPO



Εικόνα 28: Στιγμιότυπο διαχειριστικού πάνελ του εκπαιδευτή στην πλατφόρμα KYPO



Εικόνα 29: Adaptive format της εκπαίδευσης με KYPO.Δίνεται η δυνατότητα να προσαρμόζεται στο επίπεδο του εξεταζόμενου. A: το ερωτηματολόγιο πριν την έ έναρξη της εκπαίδευσης, PD το υπολογιστικό μοντέλο και Q, το ερωτηματολόγιο με το πέρας της εκπαίδευσης.[92]



Εικόνα 30: Στιγμιότυπο στην προβολή εκπαιδευτή από σε εξέλιξη εκπαίδευση CTF εκπαίδευσης με KYPO

4.1 Δημιουργία εκπαιδευτικού σεναρίου σε KYPO

Ροή εργασίας εκπαίδευσης – υλοποίηση σε Cloud [93]

Δημιουργία Sandboxes

1. Ο ορισμός ενός sandbox δημιουργείται από τους εκπαιδευτές σύμφωνα με αυτή τη μορφή και αποθηκεύεται ως αποθετήριο Git.
2. Στην πύλη KYPO, δημιουργείται μια εγγραφή σχετικά με τον ορισμό του sandbox μέσω της σελίδας Sandbox Definition Overview εισάγοντας το URI του αντίστοιχου αποθετηρίου Git από το προηγούμενο βήμα.
3. Από τον ορισμό sandbox που δημιουργήθηκε στην KYPO Portal, μπορεί να δημιουργηθεί ένα pool με καθορισμένο μέγεθος ακολουθώντας τα εξής βήματα [94].
4. Τα sandboxes στο cloud κατανέμονται κάνοντας κλικ στο κουμπί κατανομής του αντίστοιχου pool. Πραγματοποιούνται αυτόματα δύο ενέργειες:
    a. Ο αντίστοιχος ορισμός sandbox κατεβαίνει από το αποθετήριο Git, αναλύεται και επεξεργάζεται.
    b. Τα sandboxes δημιουργούνται στο cloud σύμφωνα με τον sandbox definition.

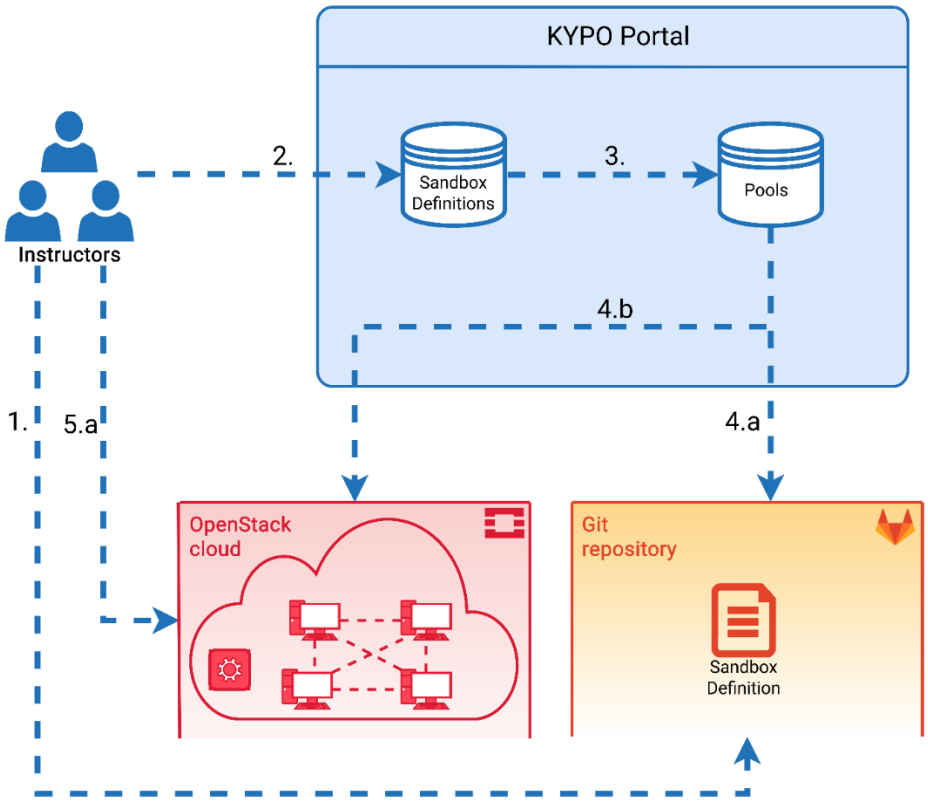
5. Τα sandboxes μπορούν να χρησιμοποιηθούν με δύο τρόπους:
    a. Ένας εκπαιδευτής μπορεί να έχει πρόσβαση σε VM εντός των sandboxes χρησιμοποιώντας SSH ή GUI και να εκτελέσει οποιεσδήποτε ενέργειες.
    b. Τα sandboxes χρησιμοποιούνται ως μέρος των εκπαιδεύσεων.

Πριν από την εκπαίδευση

Προσφέρονται διάφοροι τρόπο δημιουργίας ενός σεναρίου εκπαίδευσης:

1. Ο ορισμός εκπαίδευσης (training definition) μπορεί να δημιουργηθεί μέσω του συνδέσμου “Create Linear Training Definition” [95] ή του συνδέσμου “Create Adaptive Training Definition” [92] ανεξάρτητα από τον ορισμό του sandbox.
2. Η περίπτωση εκπαίδευσης μπορεί να δημιουργηθεί μέσω της σελίδας Create/Edit Training Instance ειδικά για τον επιλεγμένο διαθέσιμο ορισμό εκπαίδευσης. Η επιλογή “τοπικό περιβάλλον” πρέπει να είναι απενεργοποιημένη.
3. Ένα ξεκλείδωτο pool με sandboxes που έχει δημιουργηθεί για την εκπαίδευση εκχωρείται στην περίπτωση εκπαίδευσης στο δεύτερο πάνελ “Assign Pool” κατά την επεξεργασία της training instance.

4. Κάθε εκπαιδευτική περίπτωση έχει ένα διακριτικό πρόσβασης (token) το οποίο ο εκπαιδευτής παραδίδει στους εκπαιδευόμενους ώστε να μπορούν να έχουν πρόσβαση σε γραμμικές ή προσαρμοστικές εκτελέσεις εκπαίδευσης.



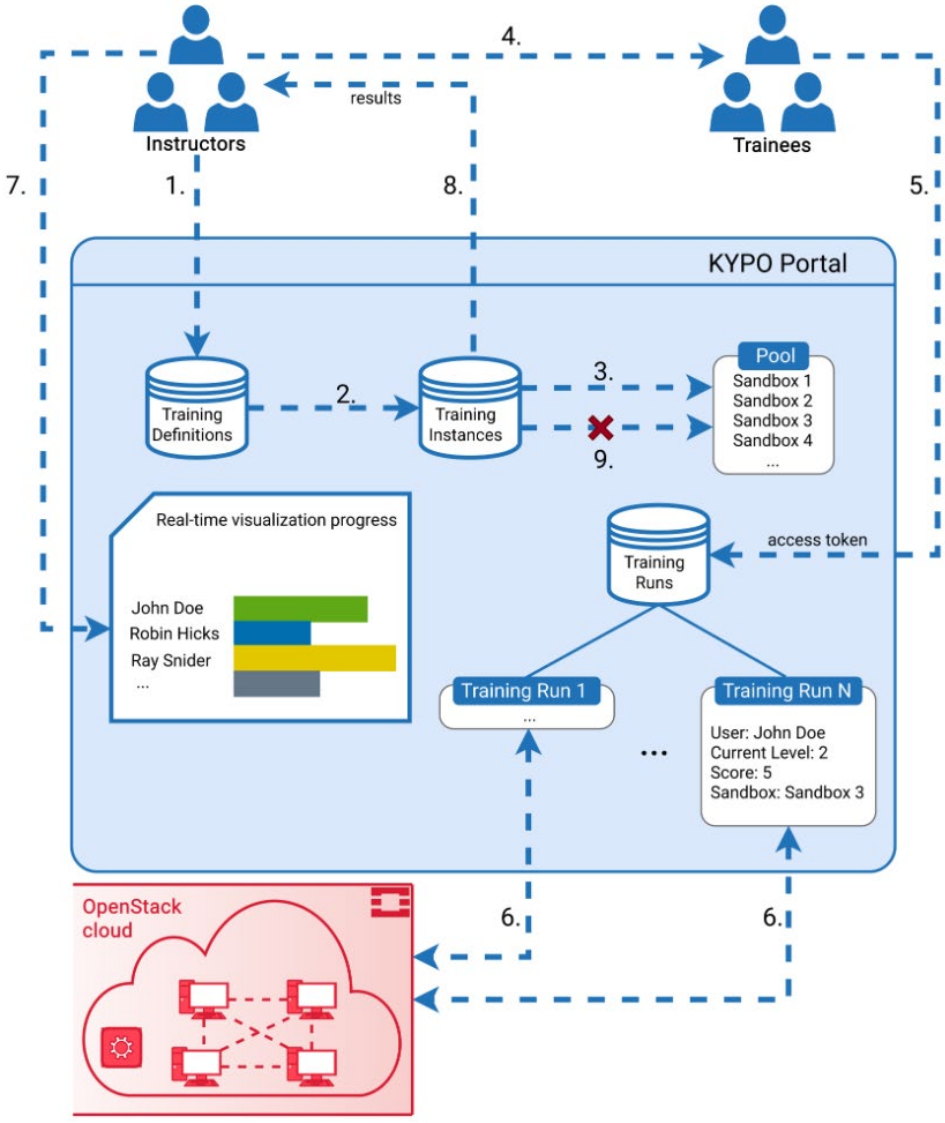
Εικόνα 31: Training Workflow - Cloud[93]

Κατά τη διάρκεια της εκπαίδευσης

5. Οι εκπαιδευόμενοι αποκτούν πρόσβαση στο *Training Run* χρησιμοποιώντας το token που έλαβαν. Οι εκπαιδευόμενοι μπορούν να συνεχίσουν τις δοκιμασίες στις οποίες είχαν πρόσβαση, εάν η training instance είναι ακόμη ενεργή.
6. Σε κάθε εκτέλεση έχει εκχωρηθεί ένα συγκεκριμένο sandbox και οι εκπαιδευόμενοι μπορούν να έχουν πρόσβαση σε VM σε αυτό το sandbox, χρησιμοποιώντας απομακρυσμένη πρόσβαση μέσω τερματικού (SSH) ή πρόσβαση μέσω Web (Apache Guacamole, Spice).
7. Ο διοργανωτής της εκπαιδευτικής περίπτωσης χρήσης μπορεί να παρακολουθεί σε πραγματικό χρόνο την πρόοδο των εκπαιδευομένων και να βλέπει τα αποτελέσματα της γραμμικής εκτέλεσης της εκπαίδευσής τους κατά τη διάρκεια της εκπαίδευσης.

Μετά την εκπαίδευση

8. Όταν ολοκληρωθεί η περίπτωση εκπαίδευσης, τα αποτελέσματα είναι διαθέσιμα και έτοιμα για περαιτέρω αξιολόγηση.
9. Η δεσμευμένη pool αποδεσμεύεται από την εκπαιδευτική περίπτωση χρήσης και διαγράφεται χρησιμοποιώντας το κουμπί διαγραφής στη σελίδα Pool για να απελευθερωθούν πόροι στο cloud. Η αντίστοιχη εκπαιδευτική περίπτωση χρήσης μπορεί να διαγραφεί χρησιμοποιώντας το κουμπί διαγραφής στη σελίδα Training Instances Overview.

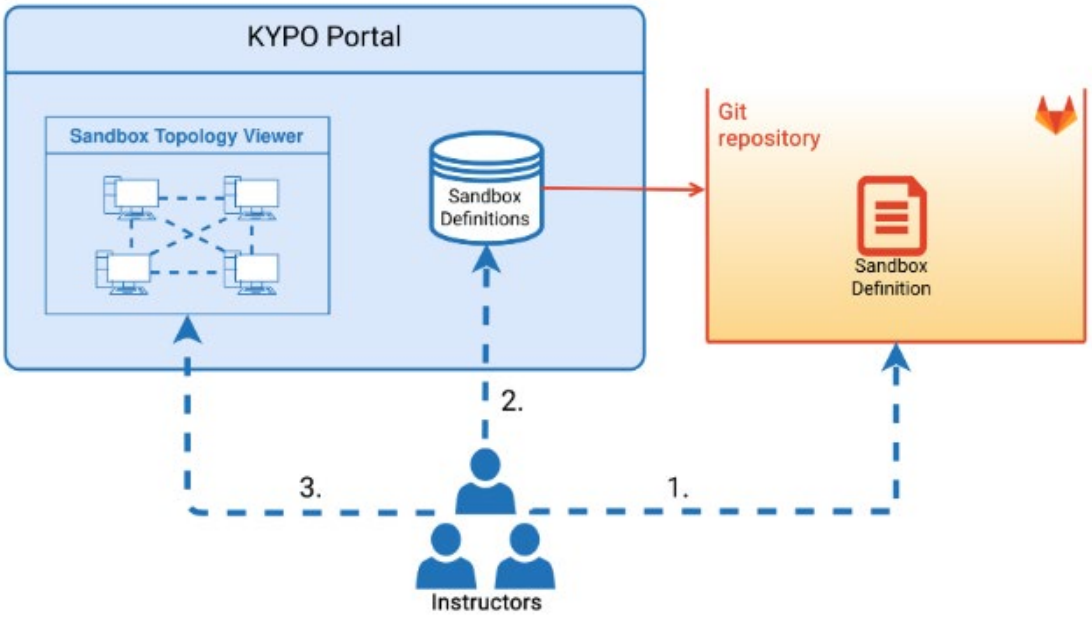


Εικόνα 32: Ενέργειες/διεργασίες κατά την εκπαίδευση με KYPO[93]

4.2 Ροή διεργασίας εκπαίδευσης - τοπική (local) υλοποίηση

Δημιουργία Sandboxes [96]

1. Ο ορισμός ενός sandbox (sandbox definition) δημιουργείται με τη χρήση του Cyber Sandbox Creator και αποθηκεύεται σε ένα αποθετήριο Git [97].
2. Στο portal του KYPO, δημιουργείται μια εγγραφή σχετικά με τον ορισμό του sandbox μέσω του συνδέσμου "*Sandbox Definition Overview"* (Επισκόπηση ορισμού sandbox) εισάγοντας το URI του αντίστοιχου αποθετηρίου Git από το προηγούμενο βήμα.
3. Ένας εκπαιδευτής μπορεί να δει και να ελέγξει την τοπολογία του ορισμού sandbox μέσω του portal του KYPO.



Εικόνα 33: Δημιουργία sandboxes σε local training workflow [96]

Δημιουργία εκπαίδευσης

Πριν από την εκπαίδευση

1. Ο ορισμός εκπαίδευσης (training definition) μπορεί να δημιουργηθεί μέσω του συνδέσμου "Create Linear Training Definition" [95] ή του συνδέσμου "Create Adaptive Training Definition" [92] ανεξάρτητα από τον ορισμό του sandbox.

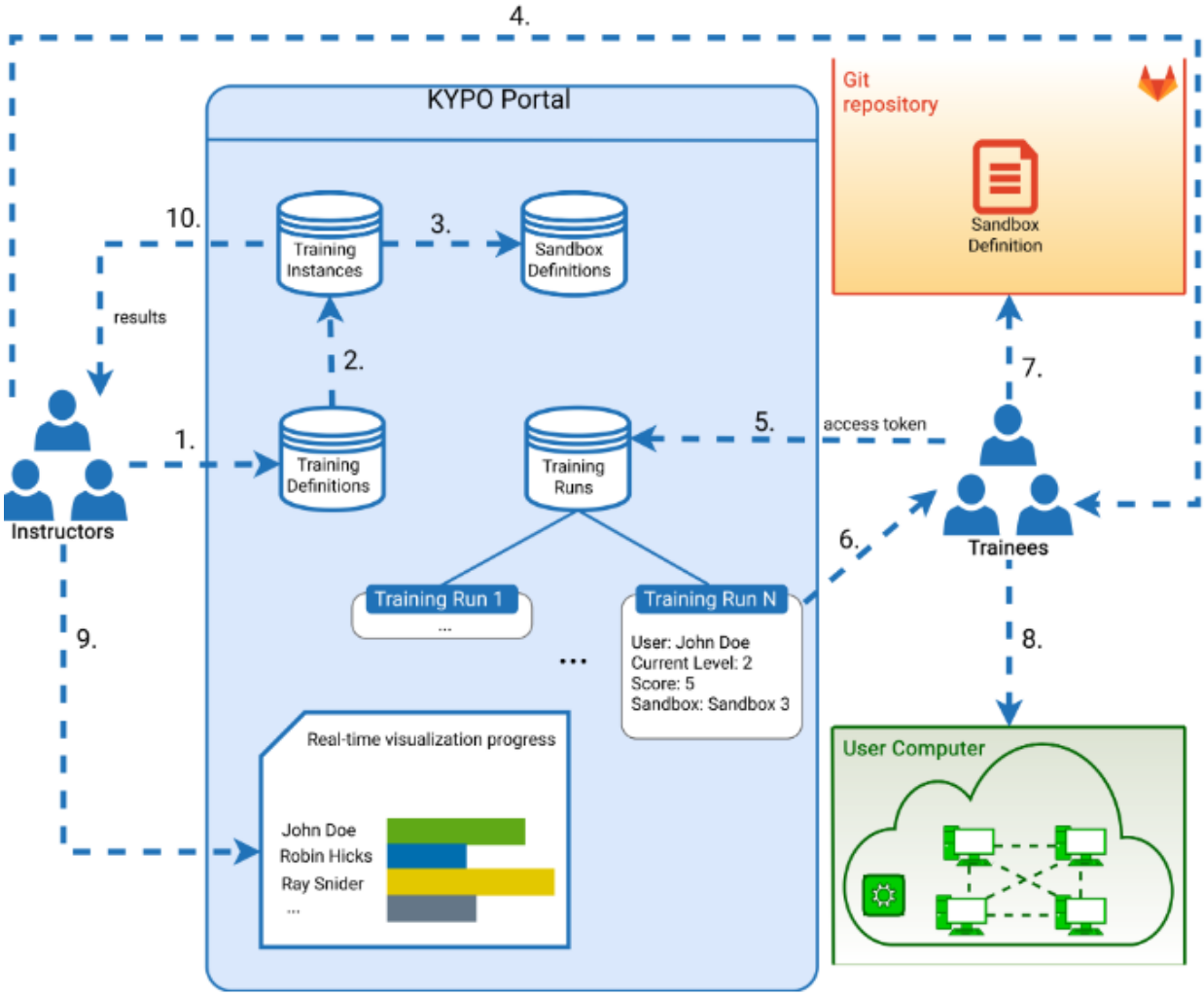
2. Το στιγμιότυπο εκπαίδευσης μπορεί να δημιουργηθεί μέσω της σελίδας Create/Edit Training Instance ειδικά για τον επιλεγμένο διαθέσιμο ορισμό εκπαίδευσης. Η επιλογή "τοπικό περιβάλλον" πρέπει να είναι ενεργοποιημένη.
3. Ένα sandbox definition που έχει δημιουργηθεί για την εκπαίδευση εκχωρείται στο στιγμιότυπο εκπαίδευσης (training instance) στο δεύτερο πάνελ "Assign Sandbox Definition" [95] κατά την επεξεργασία της περίπτωσης εκπαίδευσης.
4. Κάθε εκπαιδευτικό στιγμιότυπο έχει ένα μερικώς δημιουργημένο διακριτικό πρόσβασης (token) το οποίο ο εκπαιδευτής παραδίδει στους εκπαιδευόμενους ώστε να μπορούν να έχουν πρόσβαση σε γραμμικές ή προσαρμοστικές εκτελέσεις εκπαίδευσης.

Κατά τη διάρκεια της εκπαίδευσης

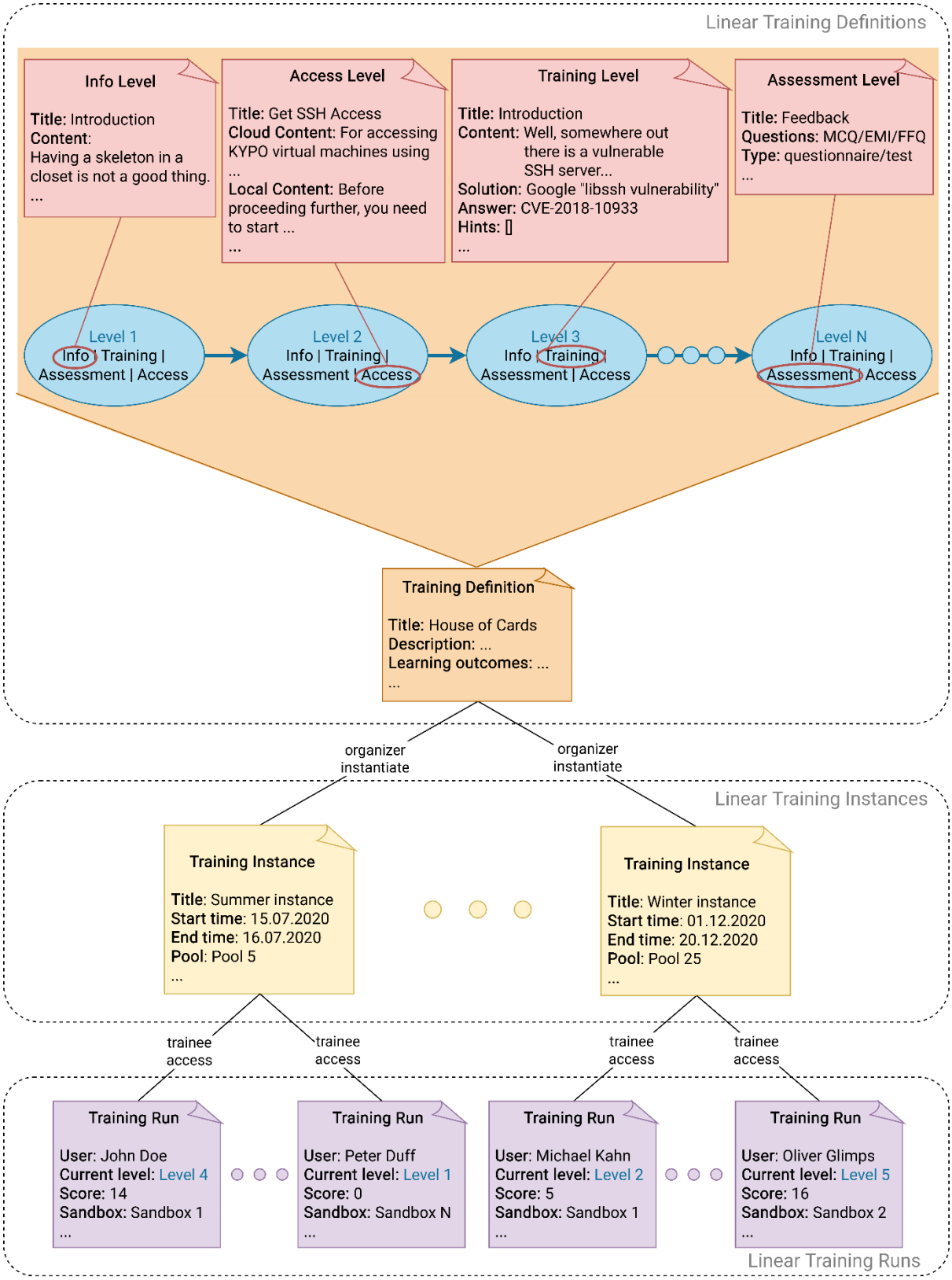
5. Οι εκπαιδευόμενοι αποκτούν πρόσβαση στην Trainin Run χρησιμοποιώντας το ληφθέν access token. Οι εκπαιδευόμενοι μπορούν να συνεχίσουν τις εκπαιδεύσεις στις οποίες έχουν πρόσβαση, εάν η εκπαιδευτική περίπτωση είναι ακόμη ενεργή.
6. Κάθε Trainin Run θα πρέπει να έχει ένα καθορισμένο ειδικό επίπεδο πρόσβασης και στάδιο, το οποίο θα πρέπει να περιέχει μια διεύθυνση URL για το αποθετήριο Git του του sandbox definition και οδηγίες για τον τρόπο κατασκευής ενός sandbox τοπικά.
7. Οι χρήστες εκτελούν την εντολή που παρέχεται στο επίπεδο πρόσβασης/στάδιο για να εκτελέσουν το τοπικό sandbox και περιμένουν μέχρι να κατασκευαστεί επιτυχώς και να είναι έτοιμο.
8. Οι χρήστες μπορούν να έχουν πρόσβαση σε μηχανήματα εντός του τοπικού sandbox χρησιμοποιώντας την κονσόλα ή την πρόσβαση SSH.
9. Ο διοργανωτής της εκπαιδευτικής περίπτωσης μπορεί να παρακολουθεί σε πραγματικό χρόνο την πρόοδο των εκπαιδευόμενων και να βλέπει τα αποτελέσματα της γραμμικής εκτέλεσης της εκπαίδευσής τους κατά τη διάρκεια της εκπαίδευσης.

Μετά την εκπαίδευση

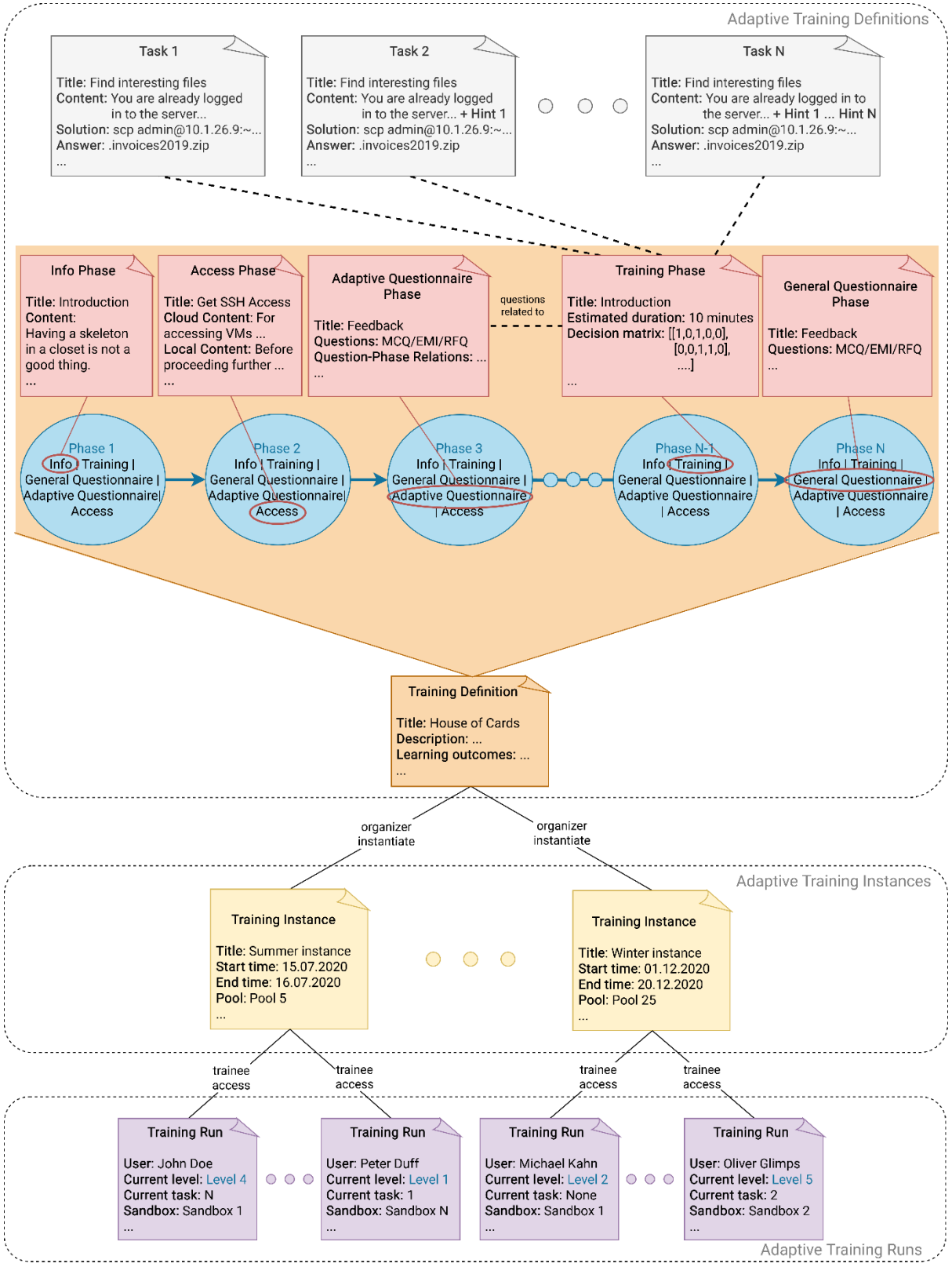
Όταν ολοκληρωθεί η περίπτωση κατάρτισης, τα αποτελέσματα είναι διαθέσιμα και έτοιμα για περαιτέρω αξιολόγηση.



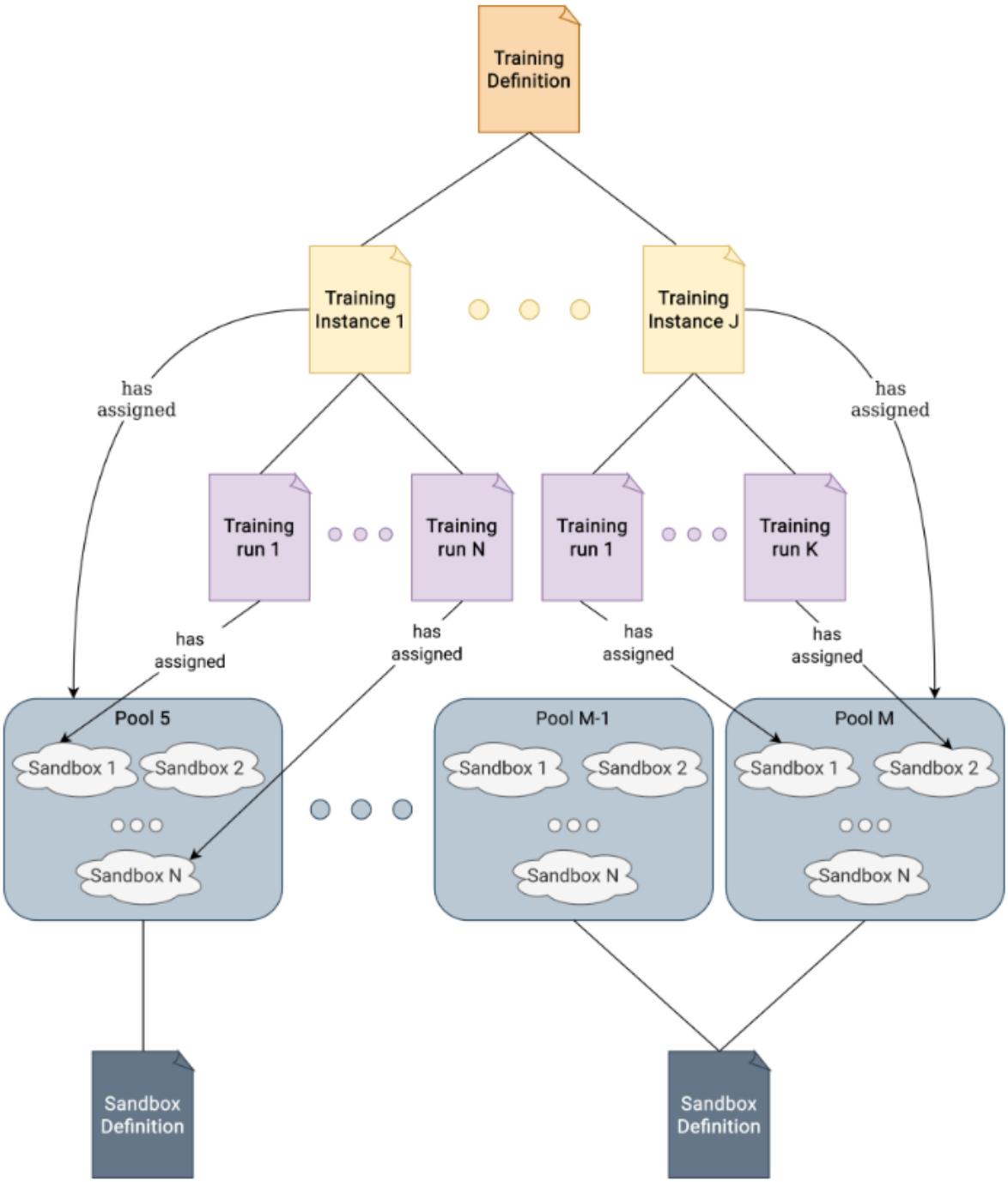
Εικόνα 34: Περιγραφή δημιουργίας σεναρίου εκπαίδευσης σε τοπική υλοποίηση[96]



Εικόνα 35: Γραφική αναπαράσταση "γραμμικής" εκπαίδευσης με KYPO[98]



Εικόνα 36: Γραφική αναπαράσταση "προσαρμοστικής" (adaptive) εκπαίδευσης με KYPO [99]



Εικόνα 37: Γραφική αναπαράσταση της διασύνδεσης μεταξύ σεναρίων εκπαίδευσης και sandboxes [100]

5. Συζήτηση – συμπεράσματα

Τα Cyber Ranges αποτελούν αποδεδειγμένα ένα πολύ καλό μέσο εκπαίδευσης και ένα εργαλείο σε θέματα μελέτης και εφαρμογής τεχνικών κυβερνοασφάλειας. Φαίνεται δε ότι το πρόβλημα της έλλειψης εξειδίκευσης σε θέματα κυβερνοασφάλειας θα γίνει εντονότερο και θα επηρεάσει την αγορά ανεξαρτήτως βιομηχανικού ή επιστημονικού πεδίου. Ένα ISMS επιτάσσει την εκπαίδευση του προσωπικού ενός οργανισμού σε θέματα Κυβερνοασφάλειας και Ασφάλειας Πληροφοριών από τη στιγμή που ο οργανισμός επιθυμεί να ακολουθήσει το πρότυπο του ISO:27001. Τα Cyber Ranges επιτρέπουν διάφορες μεθόδους εκπαίδευσης που κυμαίνονται από απλή εκτέλεση σεναρίων κυβερνοεπίθεσης, εκπαίδευση με ανάθεση ρόλων σύμφωνα με ένα σενάριο, σενάρια βασισμένα σε παίγνια (π.χ. CTF) μέχρι ένα προς ένα πραγματικής κλίμακας σενάρια επίθεσης. Μπορούν να υποστηρίξουν επίσης "paper-exercises" για να εξεταστεί ο χρόνος αντίδρασης, και αν οι ενέργειες που λαμβάνονται κατά τη διάρκεια του προσομοιωμένου σεναρίου είναι και οι αναμενόμενοι τρόποι αντίδρασης μετά από ένα συμβάν (information security incident)[26], [45], [101], [102].

Αξιοσημείωτο είναι το γεγονός ότι ο αριθμός των διαθέσιμων πεδίων δοκιμών κυβερνοασφάλειας είναι αρκετά μεγάλος. Είναι όμως ιδιαίτερα περιορισμένη η διαθεσιμότητα λύσεων ανοικτού κώδικα. Υπάρχει μεγάλο μερίδιο αγοράς που δικαιολογεί αυτή την κατάσταση, με κλειστού κώδικα λύσεις (proprietary), ή λύσεις που στοχεύουν κυρίως την αμυντική στρατιωτική βιομηχανία, καθώς η εκπαίδευση σε θέματα κυβερνοασφάλειας ανεξαρτήτως επιπέδου δυσκολίας είναι ιδιαίτερα περιζήτητη και κερδοφόρα. Δεν πρέπει να ξεχνάμε ότι το όπως πολλές λύσεις του σύγχρονου διαδικτύου, πολλές υλοποιήσεις Cyber Ranges ξεκίνησαν με αφορμή στρατιωτικές ανάγκες. Άλλωστε το ίδιο το NATO χρησιμοποιεί την έννοια της κυβερνοασφάλειας και του κυβερνοπολέμου στο λεξιλόγιό του ήδη εδώ και πολλά χρόνια [48]. Διακρίναμε επίσης ότι οι ελάχιστες διαθέσιμες λύσεις ανοιχτού κώδικα προέρχονται από τον ακαδημαϊκό κόσμο ή την ερευνητική κοινότητα [18], [44], [45], [60], [62]. Η πραγματικότητα αυτή δυστυχώς αποτελεί τροχοπέδη στην ανάπτυξη της επίγνωσης σε θέματα κυβερνοασφάλειας, καθώς δυσχεραίνεται η πρόσβαση των εκπαιδευτικών ιδρυμάτων, ή ερευνητών σε άρτιες λύσεις cyber ranges, καθώς οι κλειστού κώδικα λύσεις απαιτούν σεβαστές επενδύσεις σε χρήμα. Ακόμη και μικρές επιχειρήσεις που θα επιθυμούσαν την εκπαίδευση με χρήση cyber ranges έχουν ως αποτρεπτικό παράγοντα το κόστος.

Επιλέχθηκε για μελέτη η ανοιχτού κώδικα λύση KYPO CRP, που προσφέρεται υπό την άδεια MIT, και μπορεί να υλοποιηθεί είτε τοπικά είτε σε cloud πλατφόρμα. Η πλατφόρμα έχει

πολύ καλή υποστήριξη και βλέπουμε ότι αναπτύσσεται ενεργά αλλά και χρησιμοποιείται σε διαλέξεις και εργαστήρια κυβερνοασφάλειας του Παν/μίου του Μάσαρικ. Υποστηρίζει εκτός των άλλων και προσομοιώσεις κρίσιμων υποδομών. Η αρχιτεκτονική του είναι κλιμακούμενη και ευέλικτη. Θεωρούμε ωστόσο, ότι λόγω του εύρους δυνατοτήτων που προσφέρει το KYPO και της πολύπλοκης αρχιτεκτονικής τους, δεν είναι εφικτό να απλοποιηθεί περαιτέρω ο τρόπος υλοποίησης και να μειωθούν οι απαιτήσεις του σε υλικό και λογισμικό. Είναι ιδιαίτερα απαιτητικό σε πόρους και μπορεί να συνεπάγεται μεγάλο κόστος σε υλοποιήσεις πλήρους κλίμακας στο cloud. Το γεγονός αυτό σε συνάρτηση με τις τεχνολογίες Infrastracture as Code και Cloud τεχνολογίες που χρησιμοποιούνται το κάνουν λιγότερα ελκυστικό στον μη μυημένο. Θα πρέπει ωστόσο να δώσουμε ιδιαίτερη μνεία στους δημιουργούς του KYPO για το γεγονός ότι προσπάθησαν να λύσουν το πρόβλημα της πολύπλοκης αρχιτεκτονικής και σύνθετης υλοποίησης, καταφέρνοντας να δώσουν στον όποιο ενδιαφερόμενο τη δυνατότητα να εγκαταστήσει μία λειτουργική πλατφόρμα με λίγες κινήσεις και μερικά λεπτά αναμονή. Δεν παύει όμως να είναι υλοποίηση απαιτητική σε υπολογιστικούς πόρους.

Παρατηρούμε επίσης ότι τα cyber ranges δεν διέπονται από κάποιο κανονιστικό πλαίσιο ή πρότυπο, κάτι που κάνει το διαχωρισμό και την ταξινόμησή τους αρκετά απαιτητική. Θεωρούμε ότι προς αυτή την κατεύθυνση μπορεί να συμβάλει το γεγονός ότι το πρότυπο ISO:27001 αποτελεί στόχο για τους περισσότερους οργανισμούς, με το πρότυπο να απαιτεί διαρκή εκπαίδευση σε θέματα κυβερνοασφάλειας. Άξιες αναφοράς είναι οι ενέργειες της στρατηγικής REWIRE [103] που προέρχεται από κινήσεις της ΕΕ και προσπαθεί να εστιάσει στο να παρέχει βιώσιμες λύσεις και προτάσεις που θα μειώσουν το χάσμα της έλλειψης γνώσεων κυβερνοασφάλειας μεταξύ της εκπαιδευτικής πραγματικότητας και των απαιτήσεων και αναγκών της βιομηχανίας. Επιπλέον, στόχος του REWIRE είναι η καινοτομία και η ανταγωνιστικότητα στον τομέα της Κυβερνοασφάλειας.

Οι ερευνητές ασφάλειας και όσοι επιθυμούν να εκπαιδευτούν έχουν με τα cyber ranges ένα σημαντικό εργαλείο στη διάθεσή τους. Στο άμεσο μέλλον πιστεύουμε ότι η ανάπτυξη και η υιοθέτηση της τεχνολογίας AI, θα συνεισφέρει στην αυτοματοποίηση και ταχύτερη εξέλιξη στις πλατφόρμες CR. Οι απαιτήσεις σε ένα μεταβαλλόμενο κόσμο Κυβερνοασφάλειας αυξάνονται συνεχώς καθώς οι επιθέσεις γίνονται πιο εξεζητημένες.

6. Αναφορές

[1] H. W. Security, 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back', *HP Wolf Security*, Jul. 21, 2022. https://threatresearch.ext.hp.com/evolution-of-cybercrime-report/ (accessed Jan. 30, 2023).

[2] European Union Agency for Cybersecurity., *ENISA threat landscape for supply chain attacks.* LU: Publications Office, 2021. Accessed: Jan. 27, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/168593

[3] European Union Agency for Cybersecurity., *ENISA threat landscape 2022: July 2021 to July 2022.* LU: Publications Office, 2022. Accessed: Jan. 27, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/764318

[4] C. Brooks, 'Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know', *Forbes*. https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/ (accessed Jan. 27, 2023).

[5] 'Cybercrime (and Security) Predictions for 2023', *The Hacker News*. https://thehackernews.com/2022/12/cybercrime-and-security-predictions-for.html (accessed Jan. 27, 2023).

[6] 'The Week in Ransomware - January 13th 2023 - LockBit in the spotlight', *BleepingComputer*. https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-13th-2023-lockbit-in-the-spotlight/ (accessed Jan. 27, 2023).

[7] A. Wolf, 'Why Ransomware Remains a Major Threat for 2023', *Arctic Wolf*, Jan. 18, 2023. https://arcticwolf.com/resources/blog/ransomware-remains-major-threat-2023/ (accessed Jan. 27, 2023).

[8] '7 Reasons Global Attacks Will Rise Significantly in 2023', *Security Intelligence*. https://securityintelligence.com/articles/7-reasons-global-attacks-will-soar-2023/ (accessed Jan. 27, 2023).

[9] 'One group that's embraced AI: Criminals', *POLITICO*, May 30, 2021. https://www.politico.eu/article/artificial-intelligence-criminals/ (accessed Mar. 09, 2023).

[10] 'Artificial Intelligence Cybersecurity Challenges', *ENISA*. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges (accessed Mar. 09, 2023).

[11] mimecast, 'Cybercrime-as-a-Service', *Mimecast*, Apr. 18, 2022. https://www.mimecast.com/blog/cybercrime-as-a-service-commoditization-fuels-threat-surge/ (accessed Jan. 30, 2023).

[12] T. S. Hyslip, 'Cybercrime-as-a-Service Operations', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds. Cham: Springer International Publishing, 2020, pp. 815–846. doi: 10.1007/978-3-319-78440-3_36.

[13] Financialnewsmedia.com, 'Global Cyber Security Market Projected to Grow to $376 Billion by 2029, Exhibiting a CAGR of 13.4%'. https://www.prnewswire.com/news-releases/global-cyber-security-market-projected-to-grow-to-376-billion-by-2029--exhibiting-a-cagr-of-13-4-301664335.html (accessed Jan. 26, 2023).

[14] 'Cyber Security Market Overview by Size, Growth & Trends, 2029'. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 (accessed Jan. 26, 2023).

[15] 'How The Talent Shortage Changes the Approach to Cybersecurity', *Security Intelligence*. https://securityintelligence.com/articles/how-talent-shortage-changes-cybersecurity/ (accessed Jan. 27, 2023).
[16] '$(ISC)^2$ 2022 Cybersecurity Workforce Study'. https://www.isc2.org:443/Research/Workforce-Study (accessed Jan. 27, 2023).
[17] S. Cordey, 'Software Supply Chain Attacks: An Illustrated Typological Review', ETH Zurich, Jan. 2023. doi: 10.3929/ETHZ-B-000584947.
[18] J. Vykopal, R. Oslejsek, P. Celeda, M. Vizvary, and D. Tovarnak, 'KYPO Cyber Range: Design and Use Cases':, in *Proceedings of the 12th International Conference on Software Technologies*, Madrid, Spain, 2017, pp. 310–321. doi: 10.5220/0006428203100321.
[19] 'Providers | Vagrant | HashiCorp Developer', *Providers | Vagrant | HashiCorp Developer*. https://developer.hashicorp.com/vagrant/docs/providers (accessed Mar. 04, 2023).
[20] B. Meijer, L. Hochstein, and R. Moser, *Ansible: up and running: automating configuration mangagement and deployment the easy way*, Third edition. Beijing Boston: O'Reilly, 2022.
[21] 'What is Terraform | Terraform | HashiCorp Developer', *What is Terraform | Terraform | HashiCorp Developer*. https://developer.hashicorp.com/terraform/intro (accessed Mar. 04, 2023).
[22] K. Morris, *Infrastructure as code: dynamic systems for the cloud age*, Second edition. Beijing [China] ; Boston [MA]: O'Reilly, 2021.
[23] W. Newhouse, S. Keith, B. Scribner, and G. Witte, 'National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework', National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-181, Aug. 2017. doi: 10.6028/NIST.SP.800-181.
[24] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, 'Workforce Framework for Cybersecurity (NICE Framework)', National Institute of Standards and Technology, Nov. 2020. doi: 10.6028/NIST.SP.800-181r1.
[25] ESCO, 'Understanding Cyber Ranges: From Hype to Reality, SWG 5.1 I Cyber Range Environments and Technical Exercises', *WG5 PAPER*, 2020, [Online]. Available: https://ecs-org.eu/ecso-uploads/2022/10/5fdb291cdf5e7.pdf
[26] B. Pandey and S. Ahmad, *Introduction to the Cyber Ranges*, 1st ed. Boca Raton: Chapman and Hall/CRC, 2022. doi: 10.1201/9781003206071.
[27] C. Onwubiko, 'Understanding Cyber Situation Awareness', *IJCSA*, vol. 1, no. 1, pp. 11–30, Dec. 2016, doi: 10.22619/IJCSA.2016.100101.
[28] R. Gutzwiller, J. Dykstra, and B. Payne, 'Gaps and Opportunities in Situational Awareness for Cybersecurity', *Digital Threats*, vol. 1, no. 3, pp. 1–6, Sep. 2020, doi: 10.1145/3384471.
[29] U. Franke and J. Brynielsson, 'Cyber situational awareness – A systematic review of the literature', *Computers & Security*, vol. 46, pp. 18–31, Oct. 2014, doi: 10.1016/j.cose.2014.06.008.
[30] U. Franke, A. Andreasson, H. Artman, J. Brynielsson, S. Varga, and N. Vilhelm, 'Cyber situational awareness issues and challenges', in *Cybersecurity and Cognitive Science*, Elsevier, 2022, pp. 235–265. doi: 10.1016/B978-0-323-90570-1.00015-2.
[31] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, and J. Komárková, 'CRUSOE: A toolset for cyber situational awareness and decision support in incident handling', *Computers & Security*, vol. 115, p. 102609, Apr. 2022, doi: 10.1016/j.cose.2022.102609.
[32] J. Davis and S. Magrath, 'A Survey of Cyber Ranges and Testbeds'.

[33] B. Ferguson, A. Tall, and D. Olsen, 'National Cyber Range Overview', in *2014 IEEE Military Communications Conference*, Baltimore, MD, USA, Oct. 2014, pp. 123–128. doi: 10.1109/MILCOM.2014.27.
[34] E. Ukwandu *et al.*, 'A Review of Cyber-Ranges and Test-Beds: Current and Future Trends'. arXiv, Oct. 14, 2020. Accessed: Dec. 13, 2022. [Online]. Available: http://arxiv.org/abs/2010.06850
[35] E. C. Chaskos, 'Cyber-security training: A comparative analysis of cyber- ranges and emerging trends', 2019.
[36] M. M. Yamin, B. Katt, and V. Gkioulos, 'Cyber ranges and security testbeds: Scenarios, functions, tools and architecture', *Comput. Secur.*, vol. 88, no. C, Jan. 2020, doi: 10.1016/j.cose.2019.101636.
[37] M. Leitner *et al.*, 'Enabling exercises, education and research with a comprehensive cyber range', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 12, no. 4, pp. 37–61, Dec. 2021, doi: 10.22667/JOWUA.2021.12.31.037.
[38] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, 'Cyber Ranges and TestBeds for Education, Training, and Research', *Applied Sciences*, vol. 11, no. 4, Art. no. 4, Jan. 2021, doi: 10.3390/app11041809.
[39] 'Acknowledgements - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/acknowledgements/ (accessed Feb. 22, 2023).
[40] 'The MIT License', *Open Source Initiative*, Oct. 31, 2006. https://opensource.org/license/mit/ (accessed Mar. 05, 2023).
[41] 'MUNI-KYPO-CRP · GitLab', *GitLab*, Aug. 24, 2022. https://gitlab.ics.muni.cz/muni-kypo-crp (accessed Feb. 22, 2023).
[42] 'KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/ (accessed Feb. 22, 2023).
[43] 'MUNI-KYPO-CRP / devops / kypo-lite · GitLab', *GitLab*, Oct. 31, 2022. https://gitlab.ics.muni.cz/muni-kypo-crp/devops/kypo-lite (accessed Feb. 22, 2023).
[44] J. Vykopal, P. Celeda, P. Seda, V. Svabensky, and D. Tovarnak, 'Scalable Learning Environments for Teaching Cybersecurity Hands-on', in *2021 IEEE Frontiers in Education Conference (FIE)*, Lincoln, NE, USA, Oct. 2021, pp. 1–9. doi: 10.1109/FIE49875.2021.9637180.
[45] I. Priyadarshini, 'Features and architecture of the modern cyber range: a qualitative analysis and survey', University of Delaware, 2018. Accessed: Feb. 22, 2023. [Online]. Available: http://udspace.udel.edu/handle/19716/23789
[46] N. M. Radziwill, 'Virginia cyber range', *Software Quality Professional*, vol. 19, no. 4, p. 46, 2017.
[47] T. Gustafsson and J. Almroth, 'Cyber Range Automation Overview with a Case Study of CRATE', in *Secure IT Systems*, Cham, 2021, pp. 192–209. doi: 10.1007/978-3-030-70852-8_12.
[48] P. Pernik, 'Improving Cyber Security: NATO and the EU'.
[49] 'Cyber and Air Joint Effects Demonstration (CAAJED)'.
[50] W. Meitzler, S. Ouderkirk, and C. Hughes, 'Security Assessment Simulation Toolkit (SAST)'.
[51] M. Varshney, K. Pickett, and R. Bagrodia, 'A Live-Virtual-Constructive (LVC) framework for cyber operations test, evaluation and training', in *2011 - MILCOM 2011 Military Communications Conference*, Baltimore, MD, USA, Nov. 2011, pp. 1387–1392. doi: 10.1109/MILCOM.2011.6127499.
[52] M. Liljenstam, J. Liu, D. Nicol, Yougu Yuan, Guanhua Yan, and C. Grier, 'RINSE: The Real-Time Immersive Network Simulation Environment for Network Security

Exercises', in *Workshop on Principles of Advanced and Distributed Simulation (PADS'05)*, Monterey, CA, USA, 2005, pp. 119–128. doi: 10.1109/PADS.2005.23.
[53] B. Brown, A. Cutts, D. McGrath, D. M. Nicol, T. P. Smith, and B. Tofel, 'Simulation of cyber attacks with applications in homeland defense training', presented at the AeroSense 2003, Orlando, FL, Sep. 2003, p. 63. doi: 10.1117/12.500847.
[54] M. E. Kuhl, M. Sudit, J. Kistner, and K. Costantini, 'Cyber attack modeling and simulation for network security analysis', in *2007 Winter Simulation Conference*, Washington, DC, USA, Dec. 2007, pp. 1180–1188. doi: 10.1109/WSC.2007.4419720.
[55] L. M. Rossey *et al.*, 'LARIAT: Lincoln adaptable real-time information assurance testbed', in *Proceedings, IEEE Aerospace Conference*, Big Sky, MT, USA, 2002, vol. 6, pp. 6-2671-2676,-6–2682. doi: 10.1109/AERO.2002.1036158.
[56] R. S. Anderson, 'CYBER SECURITY AND RESILIENT SYSTEMS'.
[57] C. Siaterlis, A. P. Garcia, and B. Genge, 'On the Use of Emulab Testbeds for Scientifically Rigorous Experiments', *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 929–942, 2013, doi: 10.1109/SURV.2012.0601112.00185.
[58] J. Mayo, R. Minnich, R. Armstrong, and D. Rudish, 'Approaches for scalable modeling and emulation of cyber systems : LDRD final report.', SAND2009-6068, 974866, Sep. 2009. doi: 10.2172/974866.
[59] P.-W. Tsai and C.-S. Yang, 'Testbed@TWISC: A network security experiment platform', *Int J Commun Syst*, vol. 31, no. 2, p. e3446, Jan. 2018, doi: 10.1002/dac.3446.
[60] N. Herold, M. Wachs, M. Dorfhuber, C. Rudolf, S. Liebald, and G. Carle, 'Achieving Reproducible Network Environments with INSALATA', in *Security of Networks and Services in an All-Connected World*, vol. 10356, D. Tuncer, R. Koch, R. Badonnel, and B. Stiller, Eds. Cham: Springer International Publishing, 2017, pp. 30–44. doi: 10.1007/978-3-319-60774-0_3.
[61] C. Ritu *et al.*, 'CyberVAN: A cyber security virtual assured network testbed', 2016.
[62] P. Gunathilaka, D. Mashima, and B. Chen, 'SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions', in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, Vienna Austria, Oct. 2016, pp. 113–124. doi: 10.1145/2994487.2994494.
[63] B. Clark, *RTFM: red team field manual: V 1.0*. Leipzig: CreateSpace by Amazon Distribution GmbH, 2014.
[64] A. White and B. Clark, *BTFM: blue team field manual*, Version 1, Rel 2. United States: Alan White, 2017.
[65] T. Bryant, *PTFM: Purple Team Field Manual*. Deutschland? Verlag nicht ermittelbar, 2020.
[66] 'Introducing the InfoSec colour wheel — blending developers with red and blue security teams. | HackerNoon'. https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700 (accessed Jan. 30, 2023).
[67] N. Wilhelmson and T. Svensson, 'Handbook for planning, running and evaluating information technology and cyber security exercises', 2011.
[68] G. Walters, 'Gamification for IT Security Training and Awareness Programs', Mar. 14, 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/9.pdf
[69] B. Serranti, 'Why gamification is ideal for cybersecurity awareness training', *Sababa Security*, Apr. 21, 2022. https://www.sababasecurity.com/why-gamification-is-ideal-for-cyber-security-awareness-training/ (accessed Mar. 09, 2023).
[70] 'Cybersecurity Gamification: Prepare for a Real Attack'. https://delinea.com/blog/cybersecurity-gamification (accessed Mar. 09, 2023).

[71] P. G. McLaren, R. Kuffel, R. Wierckx, J. Giesbrecht, and L. Arendt, 'A real time digital simulator for testing relays', *IEEE Trans. Power Delivery*, vol. 7, no. 1, pp. 207–213, Jan. 1992, doi: 10.1109/61.108909.
[72] 'Real-time Simulation for Cybersecurity', *RTDS Technologies*, Mar. 25, 2020. https://knowledge.rtds.com/hc/en-us/articles/360037038774-Real-time-Simulation-for-Cybersecurity (accessed Feb. 21, 2023).
[73] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, 'Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations', *IEEE Trans. Ind. Inf.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019, doi: 10.1109/TII.2018.2884728.
[74] Ram Mohan Reddi and A. K. Srivastava, 'Real time test bed development for power system operation, control and cyber security', in *North American Power Symposium 2010*, Arlington, TX, USA, Sep. 2010, pp. 1–6. doi: 10.1109/NAPS.2010.5618985.
[75] 'OpenStack Architecture Design Guide — arch-design 0.0.1.dev15 documentation'. https://docs.openstack.org/arch-design/index.html (accessed Feb. 25, 2023).
[76] 'Spice Project'. https://www.spice-space.org/index.html (accessed Mar. 09, 2023).
[77] 'Apache Guacamole™'. https://guacamole.apache.org/ (accessed Mar. 09, 2023).
[78] 'What is the Secure Shell (SSH) Protocol? | SSH Academy'. https://www.ssh.com/academy/ssh/protocol (accessed Mar. 09, 2023).
[79] 'Introduction | Vagrant | HashiCorp Developer', *Introduction | Vagrant | HashiCorp Developer*. https://developer.hashicorp.com/vagrant/intro (accessed Mar. 04, 2023).
[80] 'Oracle VM VirtualBox'. https://www.virtualbox.org/ (accessed Mar. 09, 2023).
[81] 'Overview - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-basic/overview/ (accessed Feb. 27, 2023).
[82] 'Creating a Base Box - VirtualBox Provider', *Vagrant by HashiCorp*. https://www.vagrantup.com/docs/providers/virtualbox/boxes (accessed Dec. 12, 2020).
[83] 'Sandbox Definition - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/sandboxes/sandbox-definition/ (accessed Jan. 31, 2023).
[84] 'APG Variabels - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/sandboxes/apg-variables/ (accessed Feb. 25, 2023).
[85] 'OpenStack Docs: Flavors'. https://docs.openstack.org/nova/rocky/user/flavors.html (accessed Feb. 25, 2023).
[86] 'Topology Definition - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/sandboxes/topology-definition/ (accessed Feb. 25, 2023).
[87] A. Hat Red, 'How it works'. https://www.ansible.com/overview/how-ansible-works (accessed Mar. 04, 2023).
[88] 'Glossary — Ansible Documentation'. https://docs.ansible.com/ansible/latest/reference_appendices/glossary.html#term-Idempotency (accessed Mar. 09, 2023).
[89] 'Sandbox Access - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/sandboxes/sandbox-access/ (accessed Feb. 27, 2023).
[90] 'Platform Components - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/installation-guide/platform-components/ (accessed Feb. 27, 2023).
[91] 'Overview - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-basic/overview/#kypo-portal-home-page (accessed Feb. 27, 2023).
[92] 'Adaptive Training Definition - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-basic/training-agenda/training-definition/adaptive-training-definition/#add-a-new-definition (accessed Mar. 05, 2023).

[93] 'Training Workflow - Cloud - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/basic-concepts/typical-training-workflow/training-workflow-cloud/ (accessed Mar. 05, 2023).
[94] 'Pool - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-basic/sandbox-agenda/pool/#create-pool (accessed Mar. 05, 2023).
[95] 'Linear Training Definition - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-basic/training-agenda/training-definition/linear-training-definition/#add-a-new-definition (accessed Mar. 05, 2023).
[96] 'Training Workflow - Local - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/basic-concepts/typical-training-workflow/training-workflow-local/ (accessed Mar. 05, 2023).
[97] 'Generating a Sandbox · Wiki · MUNI-KYPO-CSC / cyber-sandbox-creator · GitLab', *GitLab*, Jan. 26, 2022. https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator/-/wikis/3.0/Generating-a-Sandbox (accessed Mar. 05, 2023).
[98] 'Overview - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/trainings/trainings-overview/#linear-training (accessed Mar. 05, 2023).
[99] 'Overview - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/trainings/trainings-overview/#adaptive-training (accessed Mar. 05, 2023).
[100] 'Overview - KYPO Cyber Range Platform'. https://docs.crp.kypo.muni.cz/user-guide-advanced/trainings/trainings-overview/#overall (accessed Mar. 05, 2023).
[101] 'ISO - ISO/IEC 27001 — Information security management', *ISO*. https://www.iso.org/isoiec-27001-information-security.html (accessed Jun. 20, 2021).
[102] 'On the Design and Implementation of Next Generation Cyber Ranges'. https://iris.unige.it/handle/11567/1035459 (accessed Jan. 27, 2023).
[103] C. S. A. A. N. V. for E. REWIRE, 'Cyber Range Establishment methodology and roadmap'. REWIRE - Cybersecurity Skills Alliance A New Vision for Europe, Nov. 30, 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/12/R4.1.1-Cyberrange-Establishment-methodology-and-roadmap_vFINAL.pdf
[104] 'Objectives', *REWIRE*. https://rewireproject.eu/objectives/ (accessed Mar. 05, 2023).
[105] T. Sapák, 'How we migrated from Ansible & Docker Compose to Helm & Kubernetes and why you want that too', *Medium*, Sep. 02, 2022. https://faun.pub/how-we-migrated-from-ansible-docker-compose-to-helm-kubernetes-and-why-you-want-that-too-98c392d8d650 (accessed Dec. 15, 2022).
[106] 'Compute Engine: Virtual Machines (VMs)', *Google Cloud*. https://cloud.google.com/compute (accessed Mar. 04, 2023).
[107] 'Cloud Storage', *Google Cloud*. https://cloud.google.com/storage (accessed Mar. 04, 2023).
[108] 'tf-gcp-vm/README.md · master · MUNI-KYPO-CRP / devops / kypo-lite · GitLab', *GitLab*, May 24, 2022. https://gitlab.ics.muni.cz/muni-kypo-crp/devops/kypo-lite/-/blob/master/tf-gcp-vm/README.md (accessed Mar. 04, 2023).
[109] 'What is an SSH Tunnel & SSH Tunneling?' https://www.ssh.com/academy/ssh/tunneling (accessed Mar. 04, 2023).
[110] 'OpenStack Docs: Kolla Ansible Configuration'. https://docs.openstack.org/kayobe/train/configuration/kolla-ansible.html (accessed Dec. 12, 2022).
[111] 'Operating Kolla — kolla-ansible 15.1.0.dev2 documentation'. https://docs.openstack.org/kolla-ansible/latest/user/operating-kolla.html (accessed Dec. 11, 2022).

[112] ‘Setting up OIDC Provider - KYPO Cyber Range Platform’. https://docs.crp.kypo.muni.cz/installation-guide/setting-up-oidc-provider/#microsoft-azure-setup (accessed Mar. 05, 2023).

7. Παράρτημα

a. Εγκατάσταση KYPO Lite σε GCP

Επιλέχθηκε Google Cloud Platform, καθώς για την εγκατάσταση του KYPO Lite σε πλατφόρμα Azure, ή VMware, συναντήθηκαν αρκετές δυσκολίες και προβλήματα στο στάδιο όπου απαιτείται η ύπαρξη nested virtualization. Οι δημιουργοί του KYPO άλλωστε προτείνουν το Google Cloud Platform διότι εμφανίζει επιπλοκές η εναλλακτική του MS Azure με το Hyper-V κατά το nested virtualization. Αν και σε χειροκίνητη εγκατάσταση δεν αντιμετωπίστηκε κάποια δυσκολία έως το στάδιο εγκατάστασης του OpenStack, παρατηρήθηκαν τα πρώτα προβλήματα κατά την εγκατάσταση των KYPO head proxy, αφού είχαν οριστεί και τα flavors επιτυχώς για το OpenStack.

Για την εγκατάσταση στις "πλήρους" έκδοσης του KYPO CRP, απαιτείται ιδιαίτερη επεξεργαστική ισχύ και πόροι. Το ελάχιστο σε απαιτήσεις σε αυτή την περίπτωση είναι 3 ξεχωριστά συστήματα και παραπέμπουστιστις αναφορές [103] [104]. Για την απόφαση των δημιουργών του KYPO CRP να αλλάξουν την τεχνολογία υλοποίησης λόγω αυξημένης πολυπλοκότητας και χρονοβόρας διαδικασίας υλοποίησης παραπέμπουμε στην αναφορά [105] όπου περιγράφονται οι λόγοι της σχετικής απόφασης. Σημαντικό κριτήριο συντέλεσε στην απόφαση η προτίμηση χρήσης IaC τεχνικών, έναντι συγκριτικά απλούστερων τεχνικών όπως η υλοποίηση με Ansible. Ωστόσο, στο αποθετήριο Git του Παν/μίου του Masaryk , μπορούμε ακόμα να βρούμε όλους τους τρόπους υλοποίησης.

Οι απαιτήσεις του **KYPO Lite** είναι οι παρακάτω:

- Ubuntu 20.04
- 8 VCPU, 44 GB RAM, 250 GB HDD (4 VCPU, 32 GB RAM είναι το ελάχιστο για βασικές λειτουργίες)

Υποστηριζόμενες Πλατφόρμες:

- physical server
- desktop
- VM with nested virtualization enabled
- Cloud flavors with virtualization support. Για το Google Cloud Platform προτείνονται instances **n2-highmem-4** and **n2-highmem-8**.

Επιλέχθηκε VM ένα Ubuntu 20.04 LTS server με τα τελευταία updates εγκατεστημένα και δημιουργήθηκαν ασφαλή κλειδιά ssh για την passwordless σύνδεση στο cloud hosted VM.

Η εγκατάσταση έγινε σε Google Cloud Platform με τις προτεινόμενες ρυθμίσεις, όπου ενεργοποιήθηκαν τα Compute και Storage Engine για το project που δημιουργήθηκε με

ονομασία kypo-lite23[106], [107]. Χρησιμοποιήθηκαν πόροι στη ζώνη "europe-west3-c". Επιπλέον σημαντικό βήμα, ήταν η δημιουργία ssh κλειδιού για τη σύνδεση με το δίκτυο του gcp, με τη χρήση ssh-tunnel [108], [109]. Το KYPO μετά την επιτυχή εγκατάσταση είναι διαθέσιμο μέσω browser αφού έχει γίνει ssh tunnel connection στο gcp δίκτυο (όχι την public IP του VM hosted στο cloud) με τη local IP address που παρέχεται στο output της εγκατάστασης.

Για την υλοποίηση χρησιμοποιήθηκε το terraform, και η ακολουθία εγκατάστασης παρουσιάζεται παρακάτω. Είναι τα ίδια βήματα, αυτοματοποιημένα αν επιλέγαμε να χρησιμοποιήσουμε χειροκίνητη, εν μέρει, εγκατάσταση των στοιχείων απαραίτητων για τη λειτουργία του KYPO (π.χ. OpenStack). Όλα τα βασικά στοιχεία του περιβάλλοντος δημιουργούνται αυτόματα και αναλύοντας τα επιμέρους κομμάτια κώδικα του terraform . Συνοπτικά, δημιουργούνται κλειδιά και πιστοποιητικά για το περιβάλλον και τις δια/επικοινωνίες των στοιχείων του, αλλά και τη διαχείρισή του και όλα τα απαραίτητα δίκτυα για τη λειτουργία του περιβάλλοντος του Openstack και στη συνέχεια του KYPO. Η δημόσια IP δεσμεύεται αυτόματα.

Ακολουθία εγκατάστασης KYPO Lite στην πλατφόρμα Google Cloud (GCP) [43] **με χρήση Terraform**.

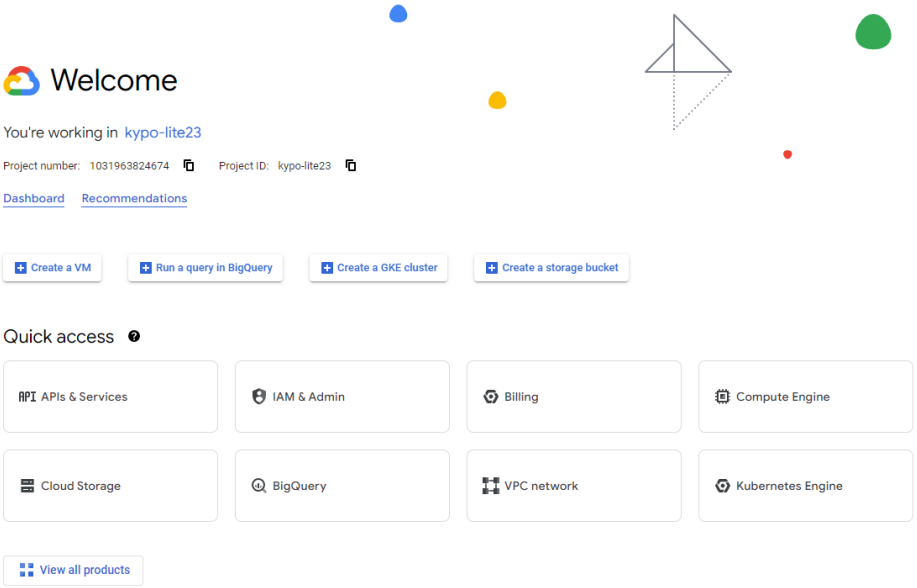
```
root@zws00nt:/home/demo/jokypo/kypo-lite/tf-gcp-vm# terraform init

Initializing the backend...

Initializing provider plugins...
- Reusing previous version of hashicorp/tls from the dependency lock file
- Reusing previous version of hashicorp/google from the dependency lock file
- Using previously-installed hashicorp/tls v3.4.0
- Using previously-installed hashicorp/google v4.21.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
root@zws00nt:/home/demo/jokypo/kypo-lite/tf-gcp-vm# terraform apply

Terraform used the selected providers to generate the following execution plan. Resource
actions are indicated with the following symbols:
  + create

Terraform will perform the following actions:

  # google_compute_firewall.ssh will be created
  + resource "google_compute_firewall" "ssh" {
      + creation_timestamp = (known after apply)
```

```
      + destination_ranges = (known after apply)
      + direction          = "INGRESS"
      + enable_logging     = (known after apply)
      + id                 = (known after apply)
      + name               = "allow-ssh"
      + network            = "default"
      + priority           = 1000
      + project            = (known after apply)
      + self_link          = (known after apply)
      + source_ranges      = [
          + "0.0.0.0/0",
        ]
      + target_tags        = [
          + "ssh",
        ]

      + allow {
          + ports    = [
              + "22",
            ]
          + protocol = "tcp"
        }
    }

  # google_compute_instance.ubuntu will be created
  + resource "google_compute_instance" "ubuntu" {
      + can_ip_forward       = false
      + cpu_platform         = (known after apply)
      + current_status       = (known after apply)
      + deletion_protection  = false
      + guest_accelerator    = (known after apply)
      + id                   = (known after apply)
      + instance_id          = (known after apply)
      + label_fingerprint    = (known after apply)
      + machine_type         = "n2-highmem-8"
      + metadata             = (known after apply)
      + metadata_fingerprint = (known after apply)
      + min_cpu_platform     = (known after apply)
      + name                 = "kypo-lite23"
      + project              = (known after apply)
      + self_link            = (known after apply)
      + tags                 = [
          + "ssh",
        ]
      + tags_fingerprint     = (known after apply)
      + zone                 = "europe-west3-c"

      + advanced_machine_features {
          + enable_nested_virtualization = true
        }

      + boot_disk {
          + auto_delete                = true
          + device_name                = (known after apply)
          + disk_encryption_key_sha256 = (known after apply)
          + kms_key_self_link          = (known after apply)
          + mode                       = "READ_WRITE"
          + source                     = (known after apply)

          + initialize_params {
              + image  = "projects/ubuntu-os-cloud/global/images/ubuntu-2004-focal-v20220419"
              + labels = (known after apply)
              + size   = 250
              + type   = (known after apply)
            }
        }
```

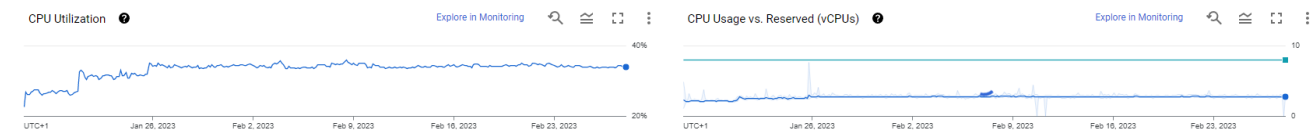
```
      + confidential_instance_config {
          + enable_confidential_compute = (known after apply)
        }

      + network_interface {
          + ipv6_access_type   = (known after apply)
          + name               = (known after apply)
          + network            = "default"
          + network_ip         = (known after apply)
          + stack_type         = (known after apply)
          + subnetwork         = (known after apply)
          + subnetwork_project = (known after apply)

          + access_config {
              + nat_ip       = (known after apply)
              + network_tier = (known after apply)
            }
        }

      + reservation_affinity {
          + type = (known after apply)

          + specific_reservation {
              + key    = (known after apply)
              + values = (known after apply)
            }
        }

      + scheduling {
          + automatic_restart   = (known after apply)
          + min_node_cpus       = (known after apply)
          + on_host_maintenance = (known after apply)
          + preemptible         = (known after apply)
          + provisioning_model  = (known after apply)

          + node_affinities {
              + key      = (known after apply)
              + operator = (known after apply)
              + values   = (known after apply)
            }
        }
    }

  # tls_private_key.admin will be created
  + resource "tls_private_key" "admin" {
      + algorithm                     = "ECDSA"
      + ecdsa_curve                   = "P384"
      + id                            = (known after apply)
      + private_key_openssh           = (sensitive value)
      + private_key_pem               = (sensitive value)
      + public_key_fingerprint_md5    = (known after apply)
      + public_key_fingerprint_sha256 = (known after apply)
      + public_key_openssh            = (known after apply)
      + public_key_pem                = (known after apply)
      + rsa_bits                      = 2048
    }

Plan: 3 to add, 0 to change, 0 to destroy.

Changes to Outputs:
  + public_ip_address = (known after apply)
  + tls_private_key   = (sensitive value)

Do you want to perform these actions?
  Terraform will perform the actions described above.
```

```
  Only 'yes' will be accepted to approve.

  Enter a value: yes




  tls_private_key.admin: Creating...
tls_private_key.admin: Creation complete after 0s
[id=ced241b4a2bcb06cd53b9eb29ad4c0eeacda3a79]
google_compute_firewall.ssh: Creating...
google_compute_instance.ubuntu: Creating...
google_compute_firewall.ssh: Still creating... [10s elapsed]
google_compute_instance.ubuntu: Still creating... [10s elapsed]
google_compute_firewall.ssh: Creation complete after 12s [id=projects/kypo-
lite23/global/firewalls/allow-ssh]
google_compute_instance.ubuntu: Creation complete after 15s [id=projects/kypo-
lite23/zones/europe-west3-c/instances/kypo-lite23]

Apply complete! Resources: 3 added, 0 changed, 0 destroyed.

Outputs:

public_ip_address = "34.141.76.7"
tls_private_key = <sensitive>
root@zws00nt:/home/demo/jokypo/kypo-lite/tf-gcp-vm#



apt install -y qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager vagrant
vagrant-libvirt
```

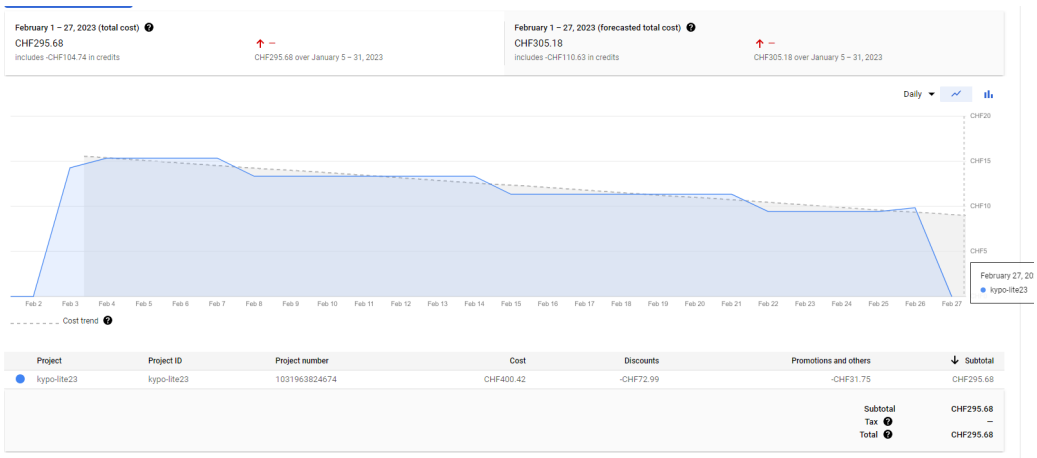
b. Στιγμιότυπα από το dashboard του GCP για το project kypo-lite23



Εικόνα 38: Dashboard Google Cloud Platform, project overview



Εικόνα 39: GCP CPU Utilization, σε αδρανή κατάσταση (idle), η εγκατάσταση κατάναλώνει πραγματικά περίπου το 40% των δεσμευμένων vCPU, κάτι που στο σενάριο υλοποίησής μας ήταν αναμενώμενο, καθώς φόρτος υπάρχει μόνο κατά τη διάρκειεα εκτέλεσης σεναρίων εκπαίδευσης. Είναι χαρακτηριστικό παράδειγμα overutilization, που μπορεί να οδηγήσει σε over-provisioning πόρων και κατά συνέπεια σε αυξημένο συνολικό κόστος. Προτείνεται on-demand/ad-hoc provisioning σε τέτοιες υλοποιήσεις για να αποφευχθούν τα παραπάνω προβλήματα.



Εικόνα 40: Εκτίμηση-Πρόβλεψη κόστους για τη χρήση των υπολογιστικών πόρων (compute-engine) και των πόρων αποθηκευτικού χώρου (storage-engine). Το κόστος χρήσης του βασικής υλοποίησης KYPO-lite, κυμαίνεται στα 12€ ημερησίως, μη λαμβάνοντας υπόψη το ενδεχόμενο υπερβολικής τηλεπικοινωνιακής κίνησης από και προς το σύστημα.

c. Προβλήματα εγκατάστασης στην περίπτωση χρήσης του Openstack και KYPO σε VMware ή Azure περιβάλλον

Στιγμιότυπα από προσπάθειες εγκατάστασης KYPO σε VMWare ή Azure

Παρακάτω παρατίθεται στιγμιότυπο από την αποτυχημένη απόπειρα εγκατάστασης σε VM, σε VMware του περιβάλλοντος του KYPO, ενώ το στάδιο της εγκατάστασης του Openstack με kolla-ansible [110], [111] ήταν επιτυχές, στο σημείο όπου δημιουργούνταν οι βασικές οντότητες του KYPO, το Head-stack και proxy-jump stack αποτύγχαναν. Η εγκατάσταση αφορούσε "all-in-one" σενάριο εγκατάστασης. Η συμπεριφορά παρατηρήθηκε τόσο σε τοπική εγκατάσταση VMware, αλλά και στο MS Azure, παρόλο που Azure υποστηρίζεται [112]

Stack kypo-head-stack CREATE_FAILED

Stack kypo-proxy-jump-stack CREATE_FAILED

```
(kypo-crp-openstack-base-pEB50oVc) root@kypos:~/kypo-crp-openstack-base# ./bootstrap.sh public
Floating IP kypo-base-head for network public does not exist. Creating...
Floating IP kypo-base-proxy for network public does not exist. Creating...
No keypair with a name or ID of 'admin_kypo-base-key' exists.
Creating keypair admin_kypo-base-key.
fingerprint: f9:4a:ed:f0:85:01:1b:62:03:4f:9f:03:0e:68:2a:26
name: admin_kypo-base-key
user_id: 3640599e52324d28a11b621fa4f227b4
Private key for user access does not exist. Creating...
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.................+++++
e is 65537 (0x010001)
(kypo-crp-openstack-base-pEB50oVc) root@kypos:~/kypo-crp-openstack-base# ./create-base.sh
2022-12-14 22:18:32Z [kypo-base-networking-stack]: CREATE_IN_PROGRESS  Stack CREATE started
2022-12-14 22:18:32Z [kypo-base-networking-stack.kypo-base-router-public]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:33Z [kypo-base-networking-stack.kypo-base-net]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:18:33Z [kypo-base-networking-stack.kypo-base-router-public]: CREATE_COMPLETE
state changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-net]: CREATE_COMPLETE  state
changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-subnet]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-subnet]: CREATE_COMPLETE  state
changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-router-public-port]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:35Z [kypo-base-networking-stack.kypo-base-router-public-port]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:35Z [kypo-base-networking-stack.kypo-base-router-public-interface]:
```

```
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:36Z [kypo-base-networking-stack.kypo-base-router-public-interface]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:36Z [kypo-base-networking-stack]: CREATE_COMPLETE  Stack CREATE completed
successfully
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | cafc1e50-3e40-4bd6-a51e-b63874cc12be |
| stack_name          | kypo-base-networking-stack           |
| description         | KYPO base networking.                |
| creation_time       | 2022-12-14T22:18:32Z                 |
| updated_time        | None                                 |
| stack_status        | CREATE_COMPLETE                      |
| stack_status_reason | Stack CREATE completed successfully  |
+---------------------+--------------------------------------+
2022-12-14 22:18:40Z [kypo-base-security-groups-stack]: CREATE_IN_PROGRESS  Stack CREATE
started
2022-12-14 22:18:41Z [kypo-base-security-groups-stack.kypo-sandbox-man-int-sg]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:41Z [kypo-base-security-groups-stack.kypo-sandbox-man-int-sg]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:42Z [kypo-base-security-groups-stack.kypo-sandbox-man-sg]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:42Z [kypo-base-security-groups-stack.kypo-sandbox-man-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:43Z [kypo-base-security-groups-stack.kypo-base-proxy-sg]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:43Z [kypo-base-security-groups-stack.kypo-base-proxy-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:44Z [kypo-base-security-groups-stack.kypo-sandbox-internal-sg]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:44Z [kypo-base-security-groups-stack.kypo-sandbox-internal-sg]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:44Z [kypo-base-security-groups-stack.kypo-sandbox-remote-security-groups]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:45Z [kypo-base-security-groups-stack.kypo-sandbox-access-sg]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:45Z [kypo-base-security-groups-stack.kypo-sandbox-access-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:46Z [kypo-base-security-groups-stack.kypo-global-ingress-icmp]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:46Z [kypo-base-security-groups-stack.kypo-global-ingress-icmp]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:47Z [kypo-base-security-groups-stack.kypo-base-head-sg]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:47Z [kypo-base-security-groups-stack.kypo-base-head-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:47Z [kypo-base-security-groups-stack.kypo-global-remote-security-groups]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:49Z [kypo-base-security-groups-stack.kypo-sandbox-remote-security-groups]:
```

```
CREATE_COMPLETE  state changed
2022-12-14 22:19:00Z [kypo-base-security-groups-stack.kypo-global-remote-security-groups]:
CREATE_COMPLETE  state changed
2022-12-14 22:19:00Z [kypo-base-security-groups-stack]: CREATE_COMPLETE  Stack CREATE
completed successfully
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 35e712c0-9114-4007-b2dd-10f4aaff3ccc |
| stack_name          | kypo-base-security-groups-stack      |
| description         | KYPO base security groups.           |
| creation_time       | 2022-12-14T22:18:40Z                 |
| updated_time        | None                                 |
| stack_status        | CREATE_COMPLETE                      |
| stack_status_reason | Stack CREATE completed successfully  |
+---------------------+--------------------------------------+
2022-12-14 22:19:03Z [kypo-head-stack]: CREATE_IN_PROGRESS  Stack CREATE started
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head-port]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head-port]: CREATE_COMPLETE  state changed
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head-floating-ip]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:19:05Z [kypo-head-stack.kypo-head-floating-ip]: CREATE_COMPLETE  state changed
2022-12-14 22:19:55Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance cfa84bc0-76ec-41b0-
bc35-065f486c3500., Code: 500"
2022-12-14 22:19:55Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:19:57Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:01Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:20:05Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance af8b2b8e-ea37-4654-
bfd9-01a2bce66d5b., Code: 500"
2022-12-14 22:20:05Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:06Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:11Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:20:15Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance e383dd60-2645-4286-
a31e-5605cdcfa13e., Code: 500"
2022-12-14 22:20:15Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:17Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:27Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:20:31Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance 5d783719-9e08-473e-
91f0-6799b2425771., Code: 500"
2022-12-14 22:20:31Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:32Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:49Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
```

```
2022-12-14 22:20:53Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance f111fad6-9c1c-47e5-
8240-867ede9608c1., Code: 500"
2022-12-14 22:20:53Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:54Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:21:27Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:21:31Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance 03698d26-b2a8-4ff3-
a86f-afdb15cd4c89., Code: 500"
2022-12-14 22:21:31Z [kypo-head-stack]: CREATE_FAILED  Resource CREATE failed:
ResourceInError: resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum
number of retries. Exhausted all hosts available for retrying build failures for instance
cfa84bc0-76ec-41b0-bc35-065f486c3500., Code: 500

 Stack kypo-head-stack CREATE_FAILED

2022-12-14 22:21:37Z [kypo-proxy-jump-stack]: CREATE_IN_PROGRESS  Stack CREATE started
2022-12-14 22:21:37Z [kypo-proxy-jump-stack.kypo-proxy-jump-port]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:21:38Z [kypo-proxy-jump-stack.kypo-proxy-jump-port]: CREATE_COMPLETE  state
changed
2022-12-14 22:21:38Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:21:38Z [kypo-proxy-jump-stack.kypo-proxy-jump-floating-ip]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:21:39Z [kypo-proxy-jump-stack.kypo-proxy-jump-floating-ip]: CREATE_COMPLETE
state changed
2022-12-14 22:21:42Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance 998e4676-fef2-
4cf1-8125-6c1e15d9117f., Code: 500"
2022-12-14 22:21:42Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:21:44Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:21:47Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:21:52Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance 641f9278-c611-
40a7-b927-b029634d3cfd., Code: 500"
2022-12-14 22:21:52Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:21:53Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:21:59Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:22:03Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance f7272087-476c-
4457-b284-e2496c57510e., Code: 500"
```

```
2022-12-14 22:22:03Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:22:04Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:22:13Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:22:17Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance 964a90ba-6ecb-
4cfb-8b1d-71bde5e70bad., Code: 500"
2022-12-14 22:22:17Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:22:18Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:22:35Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:22:39Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance bac0620c-e424-
42c1-bd24-de033f6d3f3a., Code: 500"
2022-12-14 22:22:39Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:22:40Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:23:13Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:23:17Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance c053162e-384e-
4a72-b4b1-faac9c236494., Code: 500"
2022-12-14 22:23:17Z [kypo-proxy-jump-stack]: CREATE_FAILED  Resource CREATE failed:
ResourceInError: resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded
maximum number of retries. Exhausted all hosts available for retrying build failures for
instance 998e4676-fef2-4cf1-8125-6c1e15d9117f., Cod

 Stack kypo-proxy-jump-stack CREATE_FAILED
(kypo-crp-openstack-base-pEB50oVc) root@kypos:~/kypo-crp-openstack-base# ./bootstrap.sh public
Floating IP kypo-base-head for network public does not exist. Creating...
Floating IP kypo-base-proxy for network public does not exist. Creating...
No keypair with a name or ID of 'admin_kypo-base-key' exists.
Creating keypair admin_kypo-base-key.
fingerprint: f9:4a:ed:f0:85:01:1b:62:03:4f:9f:03:0e:68:2a:26
name: admin_kypo-base-key
user_id: 3640599e52324d28a11b621fa4f227b4
Private key for user access does not exist. Creating...
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.................+++++
e is 65537 (0x010001)
(kypo-crp-openstack-base-pEB50oVc) root@kypos:~/kypo-crp-openstack-base# ./create-base.sh
2022-12-14 22:18:32Z [kypo-base-networking-stack]: CREATE_IN_PROGRESS  Stack CREATE started
2022-12-14 22:18:32Z [kypo-base-networking-stack.kypo-base-router-public]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:33Z [kypo-base-networking-stack.kypo-base-net]: CREATE_IN_PROGRESS  state
```

```
changed
2022-12-14 22:18:33Z [kypo-base-networking-stack.kypo-base-router-public]: CREATE_COMPLETE
state changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-net]: CREATE_COMPLETE  state
changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-subnet]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-subnet]: CREATE_COMPLETE  state
changed
2022-12-14 22:18:34Z [kypo-base-networking-stack.kypo-base-router-public-port]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:35Z [kypo-base-networking-stack.kypo-base-router-public-port]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:35Z [kypo-base-networking-stack.kypo-base-router-public-interface]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:36Z [kypo-base-networking-stack.kypo-base-router-public-interface]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:36Z [kypo-base-networking-stack]: CREATE_COMPLETE  Stack CREATE completed
successfully
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | cafc1e50-3e40-4bd6-a51e-b63874cc12be |
| stack_name          | kypo-base-networking-stack           |
| description         | KYPO base networking.                |
| creation_time       | 2022-12-14T22:18:32Z                 |
| updated_time        | None                                 |
| stack_status        | CREATE_COMPLETE                      |
| stack_status_reason | Stack CREATE completed successfully  |
+---------------------+--------------------------------------+
2022-12-14 22:18:40Z [kypo-base-security-groups-stack]: CREATE_IN_PROGRESS  Stack CREATE
started
2022-12-14 22:18:41Z [kypo-base-security-groups-stack.kypo-sandbox-man-int-sg]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:41Z [kypo-base-security-groups-stack.kypo-sandbox-man-int-sg]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:42Z [kypo-base-security-groups-stack.kypo-sandbox-man-sg]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:42Z [kypo-base-security-groups-stack.kypo-sandbox-man-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:43Z [kypo-base-security-groups-stack.kypo-base-proxy-sg]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:43Z [kypo-base-security-groups-stack.kypo-base-proxy-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:44Z [kypo-base-security-groups-stack.kypo-sandbox-internal-sg]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:44Z [kypo-base-security-groups-stack.kypo-sandbox-internal-sg]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:44Z [kypo-base-security-groups-stack.kypo-sandbox-remote-security-groups]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:45Z [kypo-base-security-groups-stack.kypo-sandbox-access-sg]:
```

```
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:45Z [kypo-base-security-groups-stack.kypo-sandbox-access-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:46Z [kypo-base-security-groups-stack.kypo-global-ingress-icmp]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:46Z [kypo-base-security-groups-stack.kypo-global-ingress-icmp]:
CREATE_COMPLETE  state changed
2022-12-14 22:18:47Z [kypo-base-security-groups-stack.kypo-base-head-sg]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:18:47Z [kypo-base-security-groups-stack.kypo-base-head-sg]: CREATE_COMPLETE
state changed
2022-12-14 22:18:47Z [kypo-base-security-groups-stack.kypo-global-remote-security-groups]:
CREATE_IN_PROGRESS  state changed
2022-12-14 22:18:49Z [kypo-base-security-groups-stack.kypo-sandbox-remote-security-groups]:
CREATE_COMPLETE  state changed
2022-12-14 22:19:00Z [kypo-base-security-groups-stack.kypo-global-remote-security-groups]:
CREATE_COMPLETE  state changed
2022-12-14 22:19:00Z [kypo-base-security-groups-stack]: CREATE_COMPLETE  Stack CREATE
completed successfully
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 35e712c0-9114-4007-b2dd-10f4aaff3ccc |
| stack_name          | kypo-base-security-groups-stack      |
| description         | KYPO base security groups.           |
| creation_time       | 2022-12-14T22:18:40Z                 |
| updated_time        | None                                 |
| stack_status        | CREATE_COMPLETE                      |
| stack_status_reason | Stack CREATE completed successfully  |
+---------------------+--------------------------------------+
2022-12-14 22:19:03Z [kypo-head-stack]: CREATE_IN_PROGRESS  Stack CREATE started
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head-port]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head-port]: CREATE_COMPLETE  state changed
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:19:04Z [kypo-head-stack.kypo-head-floating-ip]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:19:05Z [kypo-head-stack.kypo-head-floating-ip]: CREATE_COMPLETE  state changed
2022-12-14 22:19:55Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance cfa84bc0-76ec-41b0-
bc35-065f486c3500., Code: 500"
2022-12-14 22:19:55Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:19:57Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:01Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:20:05Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance af8b2b8e-ea37-4654-
bfd9-01a2bce66d5b., Code: 500"
2022-12-14 22:20:05Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:06Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:11Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
```

```
2022-12-14 22:20:15Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance e383dd60-2645-4286-
a31e-5605cdcfa13e., Code: 500"
2022-12-14 22:20:15Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:17Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:27Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:20:31Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance 5d783719-9e08-473e-
91f0-6799b2425771., Code: 500"
2022-12-14 22:20:31Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:32Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:20:49Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:20:53Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance f111fad6-9c1c-47e5-
8240-867ede9608c1., Code: 500"
2022-12-14 22:20:53Z [kypo-head-stack.kypo-head]: DELETE_IN_PROGRESS  state changed
2022-12-14 22:20:54Z [kypo-head-stack.kypo-head]: DELETE_COMPLETE  state changed
2022-12-14 22:21:27Z [kypo-head-stack.kypo-head]: CREATE_IN_PROGRESS  state changed
2022-12-14 22:21:31Z [kypo-head-stack.kypo-head]: CREATE_FAILED  ResourceInError:
resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum number of retries.
Exhausted all hosts available for retrying build failures for instance 03698d26-b2a8-4ff3-
a86f-afdb15cd4c89., Code: 500"
2022-12-14 22:21:31Z [kypo-head-stack]: CREATE_FAILED  Resource CREATE failed:
ResourceInError: resources.kypo-head: Went to status ERROR due to "Message: Exceeded maximum
number of retries. Exhausted all hosts available for retrying build failures for instance
cfa84bc0-76ec-41b0-bc35-065f486c3500., Code: 500

 Stack kypo-head-stack CREATE_FAILED

2022-12-14 22:21:37Z [kypo-proxy-jump-stack]: CREATE_IN_PROGRESS  Stack CREATE started
2022-12-14 22:21:37Z [kypo-proxy-jump-stack.kypo-proxy-jump-port]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:21:38Z [kypo-proxy-jump-stack.kypo-proxy-jump-port]: CREATE_COMPLETE  state
changed
2022-12-14 22:21:38Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:21:38Z [kypo-proxy-jump-stack.kypo-proxy-jump-floating-ip]: CREATE_IN_PROGRESS
state changed
2022-12-14 22:21:39Z [kypo-proxy-jump-stack.kypo-proxy-jump-floating-ip]: CREATE_COMPLETE
state changed
2022-12-14 22:21:42Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance 998e4676-fef2-
4cf1-8125-6c1e15d9117f., Code: 500"
2022-12-14 22:21:42Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:21:44Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:21:47Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
```

```
changed
2022-12-14 22:21:52Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance 641f9278-c611-
40a7-b927-b029634d3cfd., Code: 500"
2022-12-14 22:21:52Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:21:53Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:21:59Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:22:03Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance f7272087-476c-
4457-b284-e2496c57510e., Code: 500"
2022-12-14 22:22:03Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:22:04Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:22:13Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:22:17Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance 964a90ba-6ecb-
4cfb-8b1d-71bde5e70bad., Code: 500"
2022-12-14 22:22:17Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:22:18Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:22:35Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:22:39Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance bac0620c-e424-
42c1-bd24-de033f6d3f3a., Code: 500"
2022-12-14 22:22:39Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_IN_PROGRESS  state
changed
2022-12-14 22:22:40Z [kypo-proxy-jump-stack.kypo-proxy-jump]: DELETE_COMPLETE  state changed
2022-12-14 22:23:13Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_IN_PROGRESS  state
changed
2022-12-14 22:23:17Z [kypo-proxy-jump-stack.kypo-proxy-jump]: CREATE_FAILED  ResourceInError:
resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded maximum number of
retries. Exhausted all hosts available for retrying build failures for instance c053162e-384e-
4a72-b4b1-faac9c236494., Code: 500"
2022-12-14 22:23:17Z [kypo-proxy-jump-stack]: CREATE_FAILED  Resource CREATE failed:
ResourceInError: resources.kypo-proxy-jump: Went to status ERROR due to "Message: Exceeded
maximum number of retries. Exhausted all hosts available for retrying build failures for
instance 998e4676-fef2-4cf1-8125-6c1e15d9117f., Cod

 Stack kypo-proxy-jump-stack CREATE_FAILED
```