PESCO Project
EL 6.5 / Cyber Threats and Incident Response Information Sharing Platform (CTISP)
“Ανάπτυξη πλατφόρμας διαμοιρασμού - εκμετάλλευσης πληροφοριών κυβερνοαπειλών και διαχείριση συμβάντων”

Πχος (Μ) Σ. Παπαγεωργίου ΠΝ
Δντης ΓΕΕΘΑ/Ε6(ΔΙΚΥΒ)
spapageorgiou@mil.gr

- Εισαγωγή
- Τεχνική Προβολή
- Συμμετέχοντα κράτη
- Αντικειμενικοί σκοποί
- Χρονοδιάγραμμα
- Παραδοτέα

Εισαγωγή

- **Το πρόβλημα:** Πως εντοπίζουμε και αντιμετωπίζουμε άγνωστες απειλές (κυβερνοεπιθέσεις)!
- **Ο σκοπός του έργου:**
  - Θα πρέπει να υλοποιήσουμε μία λύση που θα περιλαμβάνει εργαλεία, τακτικές, τεχνικές και διαδικασίες που θα μας βοηθήσουν στον εντοπισμό και στην αντιμετώπιση αγνώστων κυβερνοεπιθέσεων.
- Ο στόχος μας είναι η αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων (γνωστές και άγνωστες).

Λύσεις που υπάρχουν

- MISP (Malware Information Sharing Platform) http://www.misp-project.org/
- MITRE ATT&CK (https://attack.mitre.org/wiki/Main_Page)
- MITRE CAR (https://car.mitre.org/wiki/Main_Page)

MISP

Τι είναι η MISP πλατφόρμα.

- Η MISP, είναι μία πλατφόρμα ανοικτού λογισμικού που μας δίνει την δυνατότητα συλλογής, αποθήκευσης, διανομής και διαμοιρασμού πληροφριών που αφορούν ενδείκτες παραβίασης και πληροφορίες που αφορούν κυβερνοαπειλές. Παρέχει πληροφορίες ανάλυσης ιομορφικού λογισμικού. Σχεδιάστηκε από και για αναλυτές ιομορφικού λογισμικού για να διαμοιράζονται δομημένη πληροφορία.

MITRE ATT&CK

Τι είναι το MITRE ATT&CK

- MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) είναι μία βάση που παρέχει πληροφορίες για τις τακτικές, τεχνικές και διαδικασίες που ακολουθούν οι επιτιθέμενοι. Η συγκεκριμένη βάση μας δίνει την δυνατότητα να κατανοήσουμε την συμπεριφορά των επιτιθέμενων, ώστε να ασφαλίσουμε καλύτερα τα συστήματά μας.

MITRE CAR

Τι είναι το MITRE CAR (Cyber Analytics Repository)

- Το Cyber Analytics Repository (CAR) είναι μία βάση από ερωτήματα (analytics) που αναπτύχθηκε από την MITRE, βασιζόμενη στο μοντέλο Adversary Tactics, Techniques, and Common Knowledge (ATT&CK™).

Διαμοιρασμός πληροφοριών

Θα χρησιμοποιήσουμε το MISP για τον διαμοιρασμό πληροφοριών και θα περιλαμβάνουν τις παρακάτω πληροφορίες:

- **Ενδείκτες παραβίασης (IOC-**Indicators of compromise)
- **Τακτικές, τεχνικές και διαδικασίες των επιτιθέμενων (TTPs-** Adversaries: Tactics, techniques **and** procedures)
- **Ερωτήματα (Analytics).** Προκαθορισμένα ερωτήματα (φίλτρα) με σκοπό να εντοπίσουμε άγνωστες κυβερνοεπιθέσεις.

Endpoint Detection and Response (EDR)

Θα υλοποιήσουμε έναν αισθητήρα EDR (Endpoint Detection and Response).

- Ο Endpoint Detection and Response αισθητήρας θα έχει τα ακόλουθα χαρακτηριστικά:
  - **Θα ανιχνεύει κυβερνοεπιθέσεις σε επίπεδο προσωπικού υπολογιστή, με βάση τους ενδείκτες παραβίασης**
  - **Θα συλλέγει πληροφορίες σχετικές με συγκεκριμένη τεχνική επίθεσης.**
  - **Θα δίνει την δυνατότητα αντιμετώπισης της κυβερνοεπίθεσης.**

Αισθητήρες θα αναπτυχθούν για τα ακόλουθα λειτουργικά:

- **Windows**
- **Linux**

Πακέτα εργασίας
Work Packages

Management – Risk - Legal

WP 1	WP 2	WP 3
Management & Administration	Risk Assessment	Legal

Πακέτα εργασίας
Work Packages

MISP modules Development

WP 4

Sharing TTPs module

WP 5

Building Analytics module (pseudo code or Elastic search)

WP 6

Building IOCs module (common format)

Πακέτα εργασίας
Work Packages

EDR Agents Development

WP 7

Windows Agent

Capabilities:

- Scanning for IOCs
- Collecting Endpoint information
- Incident responding

WP 8

Linux Agent

Capabilities:

- Scanning for IOCs
- Collecting Endpoint information
- Incident responding

Work Packages

Evaluation - Dissemination

WP 9

WP 10

Evaluation

Dissemination

Παράδοση έργου

Θα παραδοθούν στο τέλος του έργου:

Επιπλέον δυνατότητες (Extra modules) στην πλατφόρμα MISP για να διαμοιραζόμαστε:

- Ενδείκτες παραβίασης (IOCs)
- Πληροφορίες σχετικές με νέες τακτικές, τεχνικές και διαδικασίες επιτιθέμενων που εντοπίζουμε.
- Ερωτήματα, φίλτρα (Analytics) με την μορφή ψευδοκώδικα.

Αισθητήρες (EDR) για Windows και Linux.

Όλοι τα κράτη που θα συμβάλλουν ενεργά, θα λάβουν τον πηγαίο κώδικα.

Ελλάδα Ηγετική χώρα

Συμμετέχοντες


AT


CY


ES


HU


IE


IT


PT

Παρατηρητές


BE


DE


EE


FI


LT


SI

Δράσεις

Βραχυπρόθεσμοι στόχοι

Μεσοπρόθεσμοι στόχοι

Μακροπρόθεσμοι στόχοι

Δράση 1

- Διερεύνηση του πεδίου κυβερνοαπειλών.
- Μελέτη και εντοπισμός των ανοικτών πηγών πληροφοριών κυβερνοαπειλών
- Αξιολόγηση των υφιστάμενων λύσεων συλλογής πληροφοριών από ανοικτές πηγές.
- Έλεγχος των υφισταμένων διαδικασιών ανταλλαγής πληροφοριών.
- Αξιολόγηση κινδύνου.
- Νομικά ζητήματα.

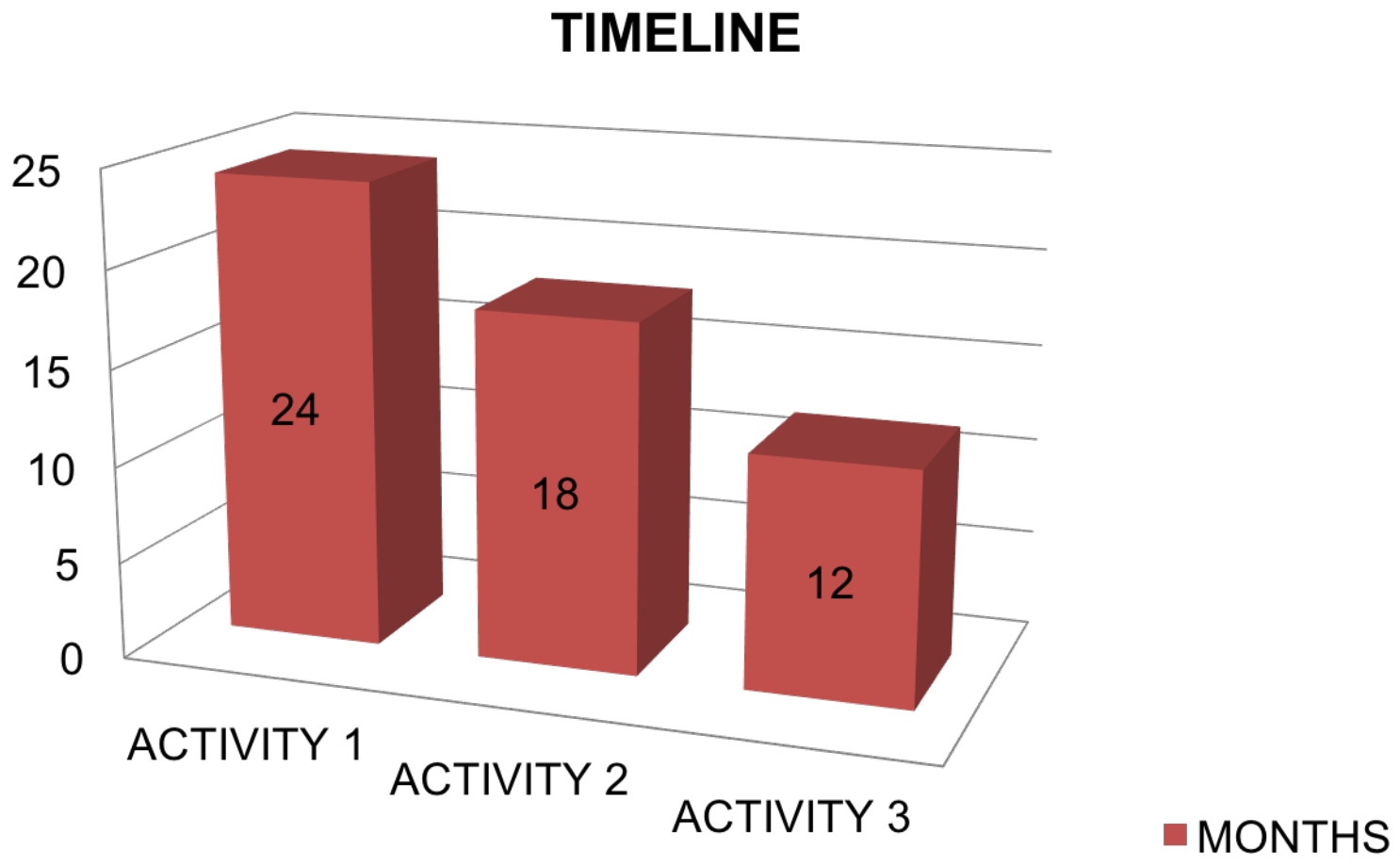
Δράση 2

- Ανάπτυξη της πλατφόρμας διαμοιρασμού πληροφοριών
- Ανάπτυξη αισθητήρων
- Ανάπτυξη διαδικασιών διαμοιρασμού πληροφοριών, βελτίωση υπαρχόντων.
- Μελέτη συμβατότητας με την ισχύουσα ευρωπαϊκή νομοθεσία

Δράση 3

- Αξιολόγηση της αναπτυχθείσας πλατφόρμας μέσω δοκιμών πεδίου.
- Αξιολόγηση των νέων τακτικών και διαδικασιών.
- Εκπαίδευση στον χειρισμό της αναπτυχθείσας πλατφόρμας.
- Παρουσίαση-διάδοση του προγράμματος.

Χρονοδιάγραμμα



Χρονοδιάγραμμα

Κόστος - Πόροι

- Προσωπικό
- Λογισμικό
- Υλικό
- Έμμεσα έξοδα

Οικονομικά

Οικονομικές Πληροφορίες

Σύνολο κόστους 2,235,000

Δράση 1

1ος Χρόνος : 430,000
2ος Χρόνος : 430,000
Σύνολο : 860,000

Δράση 2

1ος Χρόνος : 400,000
2ος Χρόνος : 780,000
Σύνολο : 1180,000

Δράση 3

2ος Χρόνος : 195,000
Σύνολο : 195,000

Συμμετοχή τρίτων

Βιομηχανία
(Μικρές, Μεσαίες και Μεγάλες εταιρίες)
Ερευνητικά κέντρα, ακαδημαϊκή κοινότητα

ΣΤΟΧΟΙ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

- **Επαύξηση διαμοιρασμού πληροφορίας απειλών κυβερνοχώρου.**
- **Επέκταση των συνεργατικών μηχανισμών μεταξύ των συμμετεχόντων Ευρωπαϊκών Κρατών.**
- **Ανάπτυξη πλατφόρμας διαμοιρασμού πληροφορίας σχετικά με απειλές στον κυβερνοχώρο με δυνατότητες αναζήτησης κυβερνοαπειλών (Threat Hunting Capabilities).**
- **Αντιμετώπιση κυβερνο-περιστατικών με βάση τις σχετικές πληροφορίες (Ενεργητική Κυβερνοάμυνα - Active Defense)**

ΑΝΑΠΤΥΞΗ ΠΛΑΤΦΟΡΜΑΣ ΔΙΑΜΟΙΡΑΣΜΟΥ ΠΛΗΡΟΦΟΡΙΑΣ ΣΧΕΤΙΚΑ ΜΕ ΚΥΒΕΡΝΟΑΠΕΙΛΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΥΒΕΡΝΟΠΕΡΙΣΤΑΤΙΚΩΝ (Cyber Threats and Incident Response Information Sharing Platform - CTISP)

Βραχυπρόθεσμοι Στόχοι

Μεσοπρόθεσμοι Στόχοι

Μακροπρόθεσμοι Στόχοι

ΔΡΑΣΤΗΡΙΟΤΗΤΑ 1

- Διερεύνηση του πεδίου κυβερνο απειλών - Διαθέσιμες ανοιχτές πηγές πληροφορίας σχετικά με τις απειλές στον κυβερνοχώρο.
- Αξιολόγηση των υφισταμένων λύσεων
- Αξιολόγηση των υφισταμένων διαδικασιών διαμοιρασμού πληροφορίας και τακτικών κυβερνοάμυνας.

ΔΡΑΣΤΗΡΙΟΤΗΤΑ 2

- Ανάπτυξη πλατφόρμας διαμοιρασμού πληροφορίας σχετικά με Κυβερνο-απειλές και Αντιμετώπιση Κυβερνο-περιστατικών.
- Ανάπτυξη νέων μεθόδων και διαδικασιών και βελτίωση υπαρχόντων.
- Μελέτη συμβατότητας με την ισχύουσα Ευρωπαική Νομοθεσία.

ΔΡΑΣΤΗΡΙΟΤΗΤΑ 3

- Αξιολόγηση της αναπτυχθείσης πλατφόρμας μέσω δοκιμών πεδίου.
- Αξιολόγηση των αναπτυχθέντων τακτικών και διαδικασιών.
- Επιχειρησιακή Ανάπτυξη της πλατφόρμας.
- Εφαρμογή Δόγματος αντιμετώπισης κυβερνο-περιστατικών με βάση τις σχετικές πληροφορίες (Ενεργητική Κυβερνοάμυνα - Active Defense)
- Παρουσίαση – διάδοση του Προγράμματος

1ο Τρίμηνο 2018 | 2ο Τρίμηνο 2018 | 3ο Τρίμηνο 2018 | 4ο Τρίμηνο 2018 | 1ο Τρίμηνο 2019 | 2ο Τρίμηνο 2019 | 3ο Τρίμηνο 2019 | 4ο Τρίμηνο 2019

24 μήνες

Δραστηριότητα 1

18 μήνες

Δραστηριότητα 2

12 μήνες

Δραστηριότητα 3

Limited Human Resources

Limited Financial Resources

MS Participation

Εμπειρία χρήσης MISP

Εμπειρία Συμμετοχής CERTCOOP

Εμπειρία Κέντρου Αντιμετώπισης Κυβερνοπεριστατικών

Βασικό Επίπεδο Ωριμότητας

Δραστηριότητα 1 Σύνολο: 860,000 €

Δραστηριότητα 2 Σύνολο: 1180,000 €

Δραστηριότητα 3 Σύνολο: 195,000 €

Σύνολο: 2,235,000

ΓΕΕΘΑ/Ε6
Δνση Κυβερνοάμυνας

Αποστολή

- Ο συντονισμός και η διεξαγωγή επιχειρήσεων κυβερνοάμυνας σε στρατηγικό, επιχειρησιακό και τακτικό επίπεδο σε περίοδο ειρήνης, κρίσης ή πολέμου.

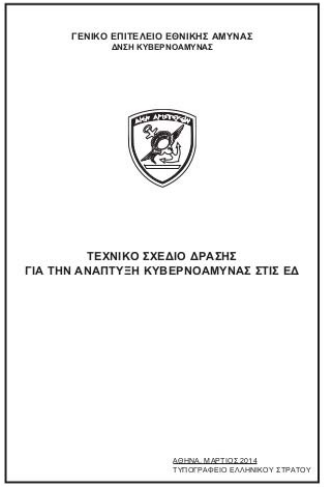
Σημαντικές ολοκληρωμένες δραστηριότητες

Εκπόνηση των παρακάτω κειμένων:

- Κατευθυντήριο πλαίσιο (Στρατιωτική Στρατηγική) Κυβερνοάμυνας.
- Δόγμα επιχειρήσεων Κυβερνοχώρου.
- Πολιτική Κυβερνοάμυνας.
- Τεχνικό σχέδιο δράσεως ανάπτυξης κυβερνοάμυνας στις ΕΔ.
- Τεχνικό εγχειρίδιο ασφαλείας προσωπικού υπολογιστή.

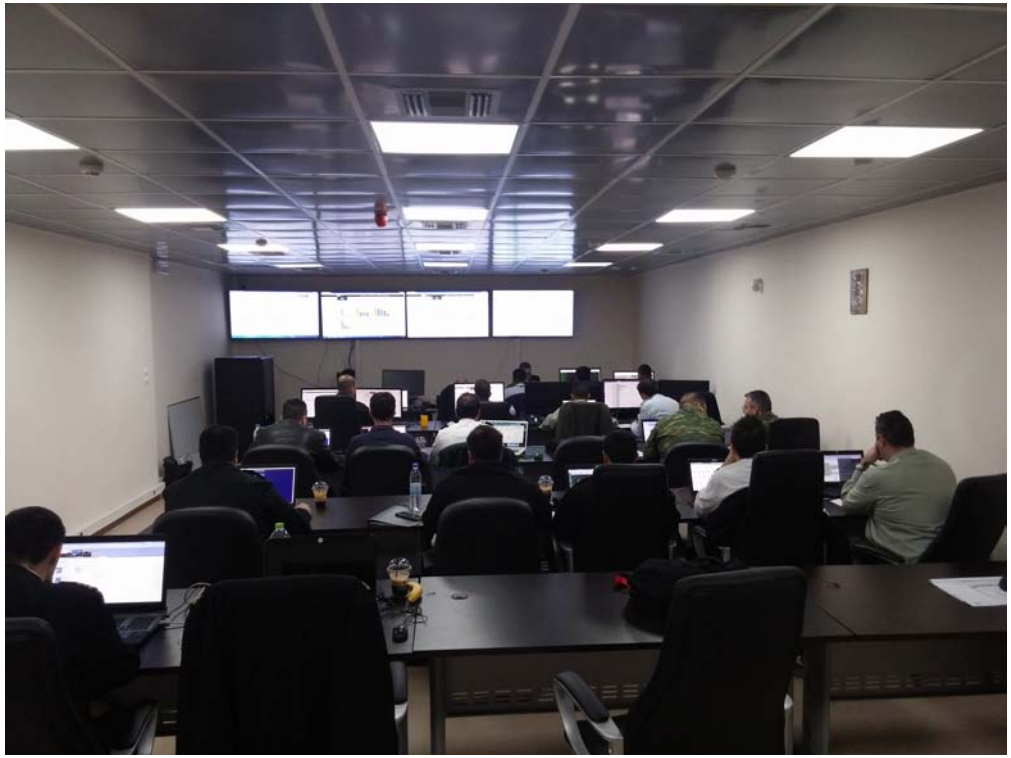
Ανάπτυξη και διατήρηση:

- Πίνακα ηλεκτρονικού ταχυδρομείου (Mailing list) Κυβερνοασφάλειας-Κυβερνοάμυνας (περιλαμβάνει τους ειδικούς επί του αντικειμένου σε εθνικό επίπεδο).



Σημαντικές δραστηριότητες σε εξέλιξη (1/2)

- Εφαρμογή του σχεδίου δράσης ανάπτυξης κυβερνοάμυνας στις ΕΔ.
- Επέκταση δυνατοτήτων Στρατιωτικού Κέντρου Αντιμετώπισης Κυβερνοπεριστατικών (ΣΚΑΚ).



Σημαντικές δραστηριότητες σε εξέλιξη (2/2)

- Οργάνωση **διαδραστικού σχολείου ενημέρωσης** στελεχών σε θέματα Κυβερνοάμυνας-κυβερνοασφάλειας.
- **Επικαιροποίηση** τεχνικού εγχειριδίου ασφαλείας προσωπικού υπολογιστή.
- **Εκπόνηση** τεχνικού εγχειριδίου διαχείρισης κυβερνοεπιθέσεων σε windows OS.
- **Εκπόνηση** τεχνικού εγχειριδίου διαχείρισης κυβερνοεπιθέσεων σε Linux OS.
- **Ανάπτυξη λογισμικού** συλλογής πληροφοριών για τον εντοπισμό κυβερνοεπιθέσεων.
- **Συνδρομή** στην σύνταξη της Εθνικής Στρατηγικής Κυβερνοασφάλειας (Έτοιμο προσχέδιο).


ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

«Η ΚΥΒΕΡΝΟΑΜΥΝΑ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ»

10 Βασικές Συμβουλές Ασφαλούς Χρήσης Η/Υ

1. Χρησιμοποιούμε μόνο νόμιμο λογισμικό ή λογισμικό ανοικτού κώδικα (Open Source)
2. Ενημερώνουμε συχνά το λογισμικό μας για τις πλέον πρόσφατες ενημερώσεις ασφαλείας (Security Updates, Patches, κλπ)
3. Χρησιμοποιούμε λογισμικό προστασίας (Anti-Virus, Firewall και Anti-Spyware)
4. Χρησιμοποιούμε πολύπλοκους Συνθηματικά (Passwords).
5. Δεν αποθηκεύουμε Συνθηματικά σε αρχεία του Η/Υ ή στον φυλλομετρητή (Browser) και δεν τα αποκαλύπτουμε σε κανέναν
6. Δεν ακολουθούμε (κάνουμε κλικ) τους συνδέσμους διαδίκτυου (Links-URLs) που μας αποστέλλονται με EMail ή Instant Messaging, αν δεν είμαστε σίγουροι για την ασφάλεια του περιεχομένου
7. Δεν ανοίγουμε οποιαναντήποτε αρχεία σε Emails, αν δεν είμαστε σίγουροι για την ασφάλεια του περιεχομένου
8. Κρυπτογραφούμε προσωπικά και "ευαίσθητα" δεδομένα
9. Ελέγχουμε συχνά τις εξωτερικές αποθηκευτικές συσκευές (π.χ. USB Drives) για μολυσμένα "αρχεία"
10. Δεν αποθηκεύουμε, επεξεργαζόμαστε ή διακινούμε Διαβαθμισμένες πληροφορίες σε Αδιαβάθμητο δίκτυο (π.χ. Internet)

Αναφέρατε κάθε ύποπτο περιστατικό ασφαλείας Η/Υ στην αρμόδια υπηρεσία του επιτελείου που υπηρετείτε και στο ΓΕΕΘΑ/ΔΙΚΥΒ/Σ.Κ.Α.Κ. (MCIRC)

ΓΕΕΘΑ/ΔΙΚΥΒ
Στρατιωτικό Κέντρο Αντιμετώπισης Κυβερνοεπιθέσεων (Σ.Κ.Α.Κ.)
Military Cyber Incident Response Center (MCIRC)
Τηλ.: (όλοι) 210-6575242, (στρατ.) 9-580-4242
E-Mail: mcirc@dt.mil.gr

Ευρωπαϊκά προγράμματα

Συμμετοχή στα παρακάτω Ευρωπαϊκά προγράμματα (HORIZON 2020)

- **Cyber Road** (Ολοκληρώθηκε)
- **Dogana** (Σε εξέλιξη)
- **CERTCOOP** (Σε εξέλιξη)

Συμμετοχή στα παρακάτω Ευρωπαϊκά προγράμματα του EDA

- **Cyber Ranges** (Σε εξέλιξη)
- **Depocyte** (Σε εξέλιξη)

EUROPEAN DEFENCE AGENCY

European Commission

HORIZON 2020

The EU Framework Programme for Research and Innovation

Εκπαίδευση

Οργάνωση και διεξαγωγή:
- **Βασικού σχολείου κυβερνοάμυνας**
- **Προκεχωρημένου σχολείου κυβερνοάμυνας**

Εκπαιδευτικά αντικείμενα των σχολείων:
- Ασφάλεια Υπολογιστών και Δικτύων
- Ψηφιακή σήμανση
- Εντοπισμός και αντιμετώπιση κυβερνοεπιθέσεων
- Έλεγχος διείσδυσης
- Ανάλυση Ιομορφικών λογισμικών
- Ασφάλεια κινητών τηλεφώνων

Συνεργασίες με άλλους φορείς

Σε Εθνικό επίπεδο:

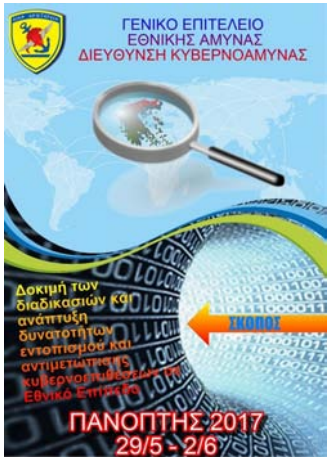
- Με ακαδημαϊκή κοινότητα
  - Εκπόνηση διατριβών κυβερνοάμυνας
- Εθνικά Κέντρα Αντιμετώπισης Κυβερνοπεριστατικών (Ανταλλαγή Πληροφοριών):
  - Εθνικό CERT (ΕΥΠ)
  - ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας)
  - ΙΤΕ (Ίδρυμα Τεχνολογίας και Έρευνας)

Σε Διεθνές επίπεδο

- EDA (European Defence Agency)
- NCIRC (NATO Computer Incident Response Capability)
- ENISA (European Union Agency for Network and Information Security)

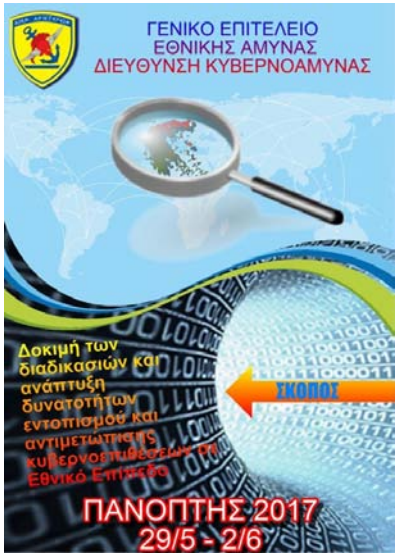
Συμμετοχή σε Διεθνείς Ασκήσεις Κυβερνοάμυνας

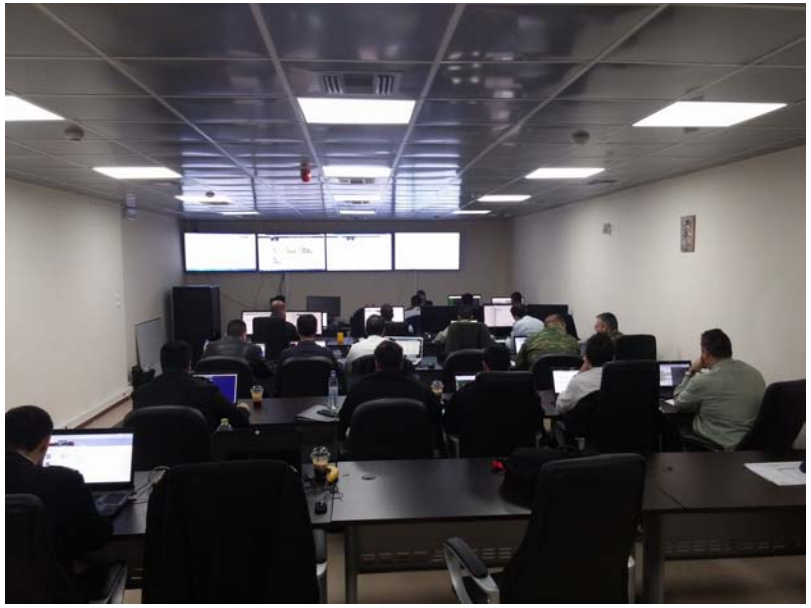
- Συμμετοχή στην Νατοϊκή άσκηση Κυβερνοάμυνας “Cyber Coalition” από το 2009.
- Συμμετοχή στην άσκηση Κυβερνοάμυνας “Locked Shields” από το 2014.
- Συμμετοχή στην άσκηση Κυβερνοάμυνας “Cyber Europe” από το 2014.
- Συμμετοχή στην άσκηση Κυβερνοάμυνας “Crossed Swords” από το 2016.



Εθνικές Ασκήσεις Κυβερνοάμυνας

- Διοργάνωση της **Εθνικής Άσκησης Κυβερνοάμυνας "ΠΑΝΟΠΤΗΣ"** από το 2010 (7 ασκήσεις μέχρι τώρα). Επόμενη άσκηση Μάιος του 18.
  - Στην άσκηση συμμετέχουν οι Ένοπλες Δυνάμεις, ΕΥΠ, ΕΛΑΣ, φορείς του δημόσιου και του ιδιωτικού τομέα, καθώς και της ακαδημαϊκής κοινότητας.
- Διοργάνωση Εθνικής Άσκησης Κυβερνοάμυνας σε Στρατηγικό επίπεδο.





Q&A