ΚΕΝΤΡΟ ΜΕΛΕΤΩΝ ΑΣΦΑΛΕΙΑΣ
CENTER FOR SECURITY STUDIES

Σχεδιασμός εκτίμησης επικινδυνότητας και ανάλυσης τρωτότητας κρίσιμων υποδομών

Αθανάσιος Σφέτσος

ΕΚΕΦΕ Δημόκριτος & ΚΕΜΕΑ

6ο SECURITY PROJECT 2018

Αθήνα 16/03/20187

ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ ΕΣΩΤΕΡΙΚΗΣ ΑΣΦΑΛΕΙΑΣ – ΤΟΜΕΑΣ ΑΣΤΥΝΟΜΙΚΗΣ ΣΥΝΕΡΓΑΣΙΑΣ (2014-2020)

ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

Δράση συγχρηματοδοτούμενη σε ποσοστό 75% από κοινοτικούς πόρους και 25% από εθνικούς πόρους που θα βαρύνει τις πιστώσεις του υπ΄ αριθμ. 2016ΣΕ05020013 Έργου της ΣΑΕ 050/2 με τίτλο: «Στοχευμένες Δράσεις για την Αύξηση της Προστασίας των Εθνικά Χαρακτηρισμένων ΕΥΖΣ».

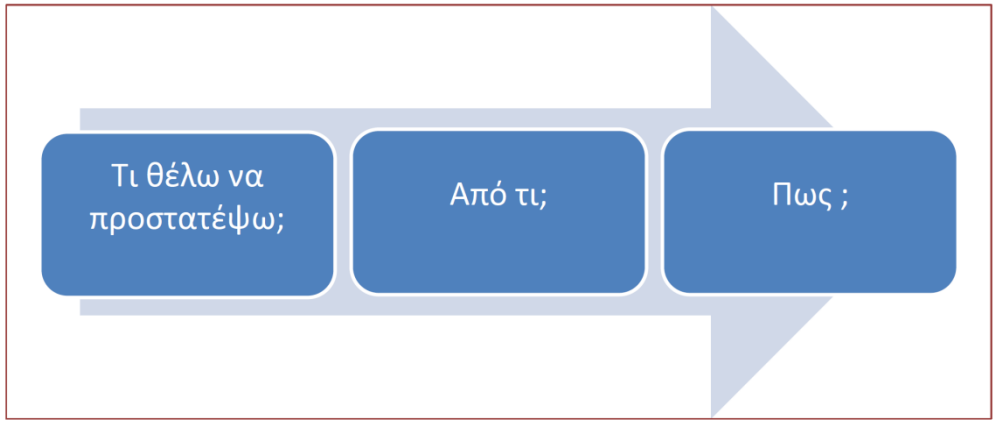
- Γενικές αρχές σχεδίου εκτίμησης επικινδυνότητας-τρωτότητας

✓ Αρχικό τμήμα του συνολικού σχεδίου ασφάλειας της εγκατάστασης

✓ Ολιστική προσέγγιση προστασίας ΚΥ βασισμένη στην εκτίμηση επικινδυνότητας και την σειρά κατάταξης κινδύνων

✓ Από την «ανάλυση κόστους-οφέλους» στην «ανάλυση κόστους-αποτελεσματικότητας»

Όταν γίνεται λόγος για προστασία πρέπει να απαντηθούν **τρία** ερωτήματα:



Σχέδιο επικινδυνότητας –τρωτότητας (ΣΕΤ)

Βήμα 1- Γενικό Πλαίσιο
- 1.1. Στόχοι ΣΕΤ
- 1.2. Σκοπός ΣΕΤ
- 1.3. Λόγοι και παραδοχές ΣΕΤ
- 1.4. Ομάδα εφαρμογής ΣΕΤ

Βήμα 2 – Χαρακτηρισμός εγκατάστασης
- 2.1 Περιγραφή εγκατάστασης
- 2.2 Πολιτική Ασφάλειας
- 2.3 Υπάρχοντα μέτρα προστασίας και αντίμετρα
- 2.4 Χαρακτηρισμός ελκυστικότητας εγκατάστασης

Βήμα 3 – Ανάλυση πόρων και διεργασιών
- 3.1 Αναγνώριση κυρίων διεργασιών και πόρων
- 3.2 Κατηγοριοποίηση ελκυστικότητας διεργασιών και πόρων
- 3.3 Προσδιορισμός επιπτώσεων από σταμάτημα διεργασιών / καταστροφή πόρων
- 3.4 Προφίλ κινδύνου πόρων και διεργασιών

Βήμα 4 – Ανάλυση Απειλών
- 4.1 Εκτίμηση απειλών και τρόπων εκδήλωσης
- 4.2 Δημιουργία σεναρίων
- 4.3 Κατηγοριοποίηση

Βήμα 5 - ΣΕΤ
- 5.1 Δημιουργία σεναρίων απειλών
- 5.2 Εκτίμηση επικινδυνότητας
- 5.3 Ανάλυση τρωτότητας

Χαρακτηρισμός εγκατάστασης

- Γεωγραφικά, χωροταξικά και κτιριολογικά χαρακτηριστικά
- Τεχνικές υποδομές και συστήματα παραγωγής/λειτουργίας, μεταφοράς/διακίνησης, κλπ, υποστηρικτικά συστήματα και εξοπλισμός λειτουργίας και προστασίας
- Συναρτώμενες/συνδεδεμένες εξωτερικές υποδομές εξοπλισμός και συστήματα λειτουργίας ή υποστήριξης
- Αξία και κρισιμότητα, υποδομών, συστημάτων, λειτουργικών τομέων, δικτύων, εξοπλισμού, λειτουργιών, κλπ
- Χαρακτηριστικά από άποψη ασφάλειας εγγύς περιβάλλουσας περιοχής
- Αρχές Ασφάλειας και Έκτακτης Ανάγκης

Αναγνώριση κρίσιμων στοιχείων εγκατάστασης – δυνητικών στόχων

- Επιλογή κριτηρίων σημαντικότητας στόχων
  - Συνέπειες απώλειας : απώλειες, κόστος - χρόνος αποκατάστασης
- Αναγνώριση εγκατάστασης
  - Επιτόπιος έλεγχος, σχέδια, συνεντεύξεις με προσωπικό
  - Ανάλυση ιστορικών περιστατικών
  - Προηγούμενες αξιολογήσεις
  - «Εκ των έσω απειλή»

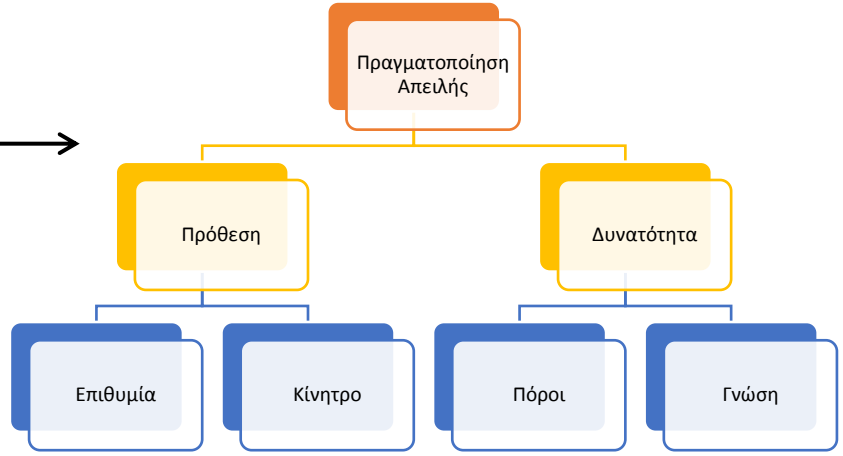
Κατηγοριοποίηση απειλών

- Ανάλυση διεθνούς, εθνικού και τοπικού περιβάλλον ασφάλειας

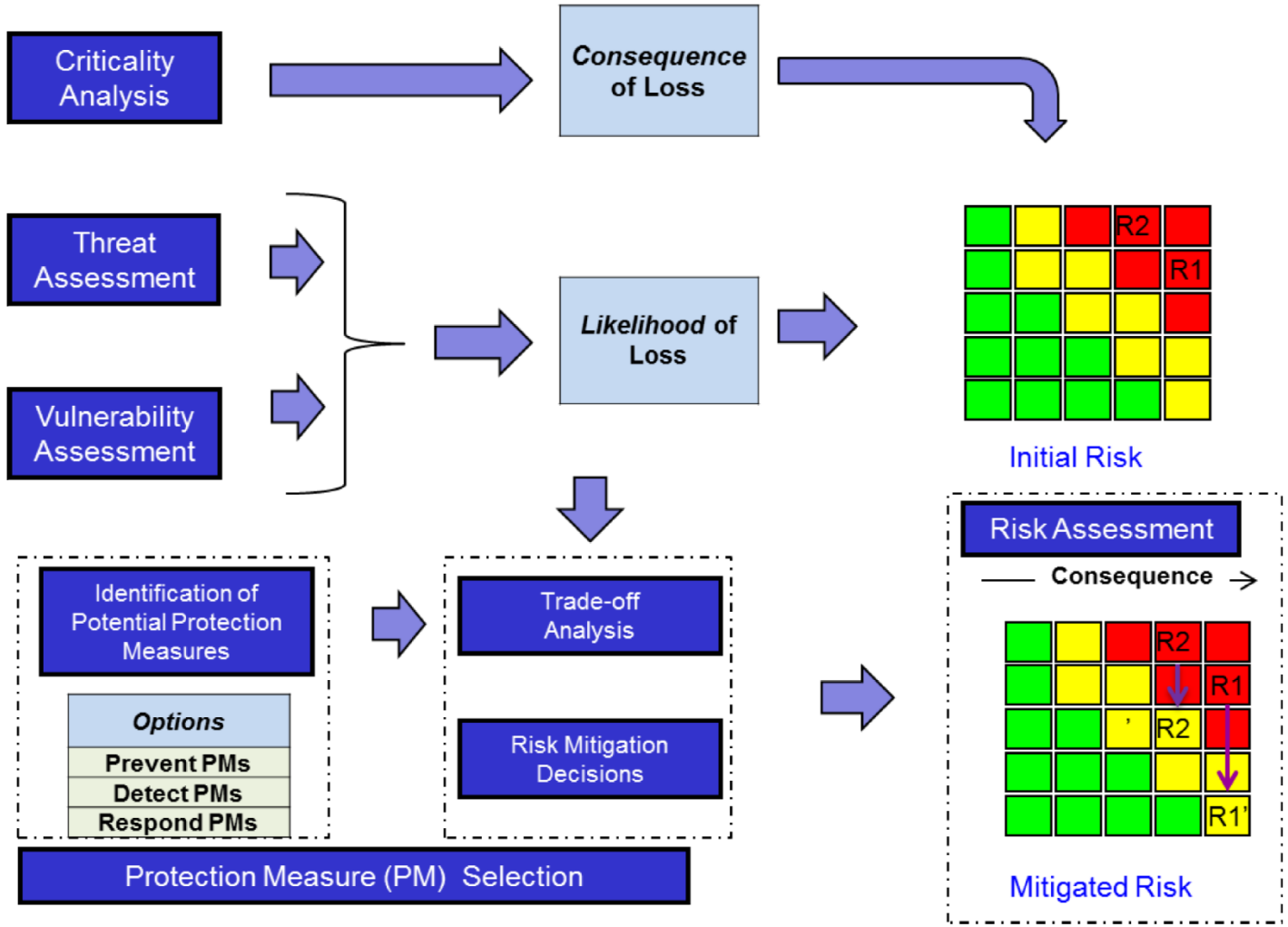
  - ✓ Αναγνώριση, καταγραφή και διάκριση απειλών/κινδύνων, συνολικά και ανά κρίσιμη υποδομή/σύστημα/ λειτουργικό τομέα
  - ✓ Ανθρωπογενείς απειλές (εξωτερικές)
  - ✓ “Εκ των έσω απειλή” (Insider threat)
  - ✓ Τεχνολογικοί κίνδυνοι-ατυχήματα
  - ✓ Κίνδυνοι από φυσικά φαινόμενα

Συνιστώσες επικινδυνότητας

- Πιθανοφάνεια: εκτίμηση των συνθηκών για την εκδήλωση της απειλής/κινδύνου
  - Εγκατάσταση : α) ελκυστικότητα β) τρωτότητα
  - Δυνατότητες επιτιθεμένου



- Αντίκτυπος: Κατηγοριοποίηση επιπτώσεων
  - Ανθρώπινες απώλειες
  - Οικονομικές επιπτώσεις
  - Περιβαλλοντικές επιπτώσεις
  - Απώλειες παραγωγής
  - Επιπτώσεις σε διασυνδεδμένες υποδομές
  - Φήμη εταιρείας


Criticality Analysis
Consequence of Loss
Threat Assessment
Vulnerability Assessment
Likelihood of Loss
R2
R1
Initial Risk
Identification of Potential Protection Measures
Options
Prevent PMs
Detect PMs
Respond PMs
Trade-off Analysis
Risk Mitigation Decisions
Protection Measure (PM) Selection
Risk Assessment
Consequence
R2
R1
R2
R1'
Mitigated Risk

Μήτρα επικινδυνότητας

Πίνακας εκτίμησης κατηγορίας κινδύνων

	ΣΥΝΕΠΕΙΕΣ				
ΠΙΘΑΝΟΦΑΝΕΙΑ	ΑΜΕΛΗΤΕΑ	ΜΙΚΡΗ	ΜΕΤΡΙΑ	ΜΕΓΑΛΗ	ΣΟΒΑΡΗ
ΒΈΒΑΙΗ	ΜΙΚΡΟΣ	ΜΕΤΡΙΟΣ	ΜΕΓΑΛΟΣ	ΚΡΙΣΙΜΟΣ	ΚΡΙΣΙΜΟΣ
ΥΨΗΛΗ	ΠΟΛΥ ΜΙΚΡΟΣ	ΜΕΤΡΙΟΣ	ΜΕΤΡΙΟΣ	ΜΕΓΑΛΟΣ	ΚΡΙΣΙΜΟΣ
ΜΕΤΡΙΑ	ΠΟΛΥ ΜΙΚΡΟΣ	ΜΙΚΡΟΣ	ΜΕΤΡΙΟΣ	ΜΕΤΡΙΟΣ	ΜΕΓΑΛΗ
ΧΑΜΗΛΗ	ΠΟΛΥ ΜΙΚΡΟΣ	ΠΟΛΥ ΜΙΚΡΟΣ	ΜΙΚΡΟΣ	ΜΙΚΡΟΣ	ΜΕΤΡΙΟΣ
ΠΟΛΥ ΧΑΜΗΛΗ	ΠΟΛΥ ΜΙΚΡΟΣ	ΠΟΛΥ ΜΙΚΡΟΣ	ΠΟΛΥ ΜΙΚΡΟΣ	ΠΟΛΥ ΜΙΚΡΟΣ	ΜΙΚΡΟΣ

Ανάλυση τρωτότητας

Αναγνώριση ευπαθειών/αδυναμιών βάσει σεναρίων πιθανής εκδήλωσης κάθε συγκεκριμένης απειλής/κινδύνου, πρωτίστως στις κρίσιμα στοιχεία, υποδομές, συστήματα, λειτουργικούς τομείς της Κ.Υ., με διάκριση σε:

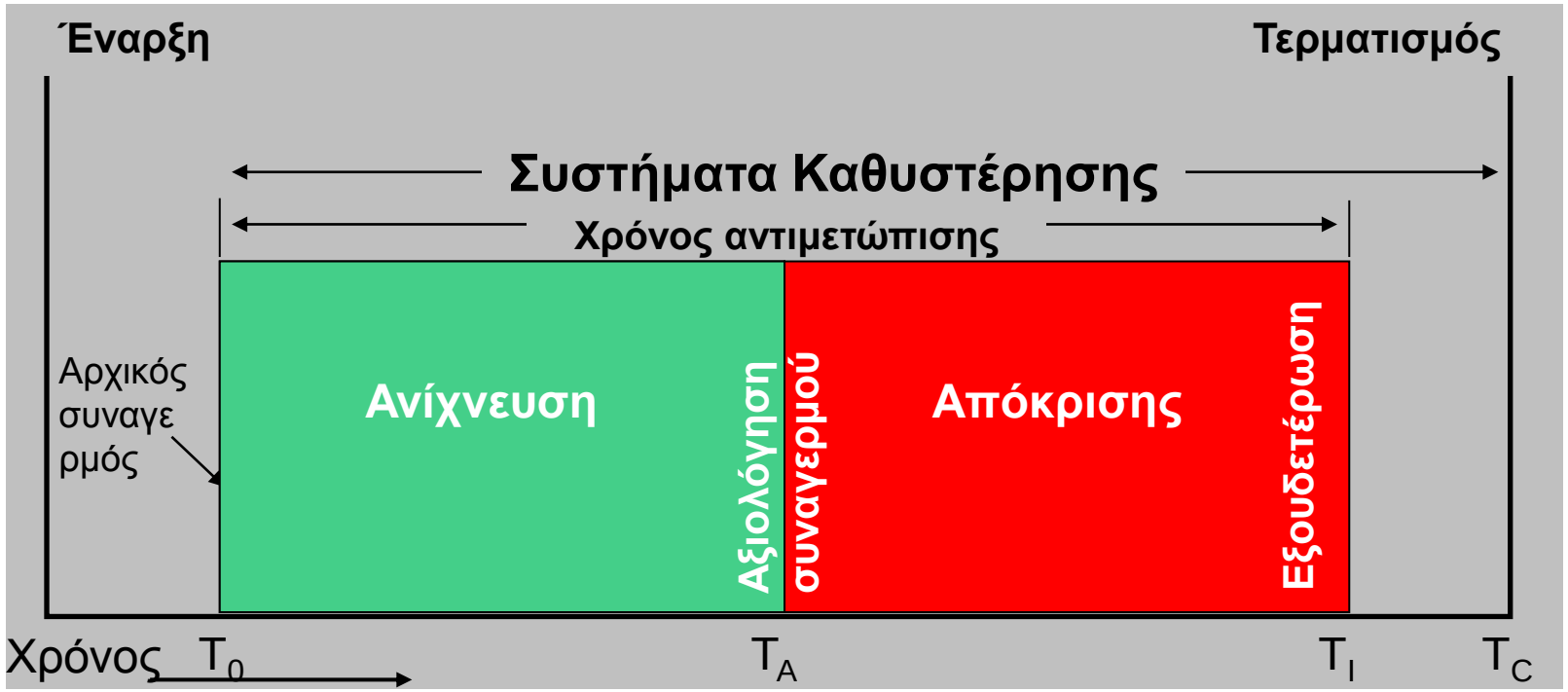
- Δομικές/κτιριολογικές, τεχνικού, λειτουργικού και υποστηρικτικού εξοπλισμού
- Συστήματα φυσικής και ηλεκτρονικής ασφάλειας
- Διοικητικές/Οργανωτικές
- Διαδικασιών λήψης αποφάσεων, συντονισμού και διαχείρισης συμβάντων/εκτάκτων αναγκών
- Ανθρώπινου παράγοντα/κουλτούρας ασφάλειας

Τρέχοντα επίπεδα τρωτότητας → Μεταβαλλόμενοι κίνδυνοι → Μελλοντικά επίπεδα τρωτότητας

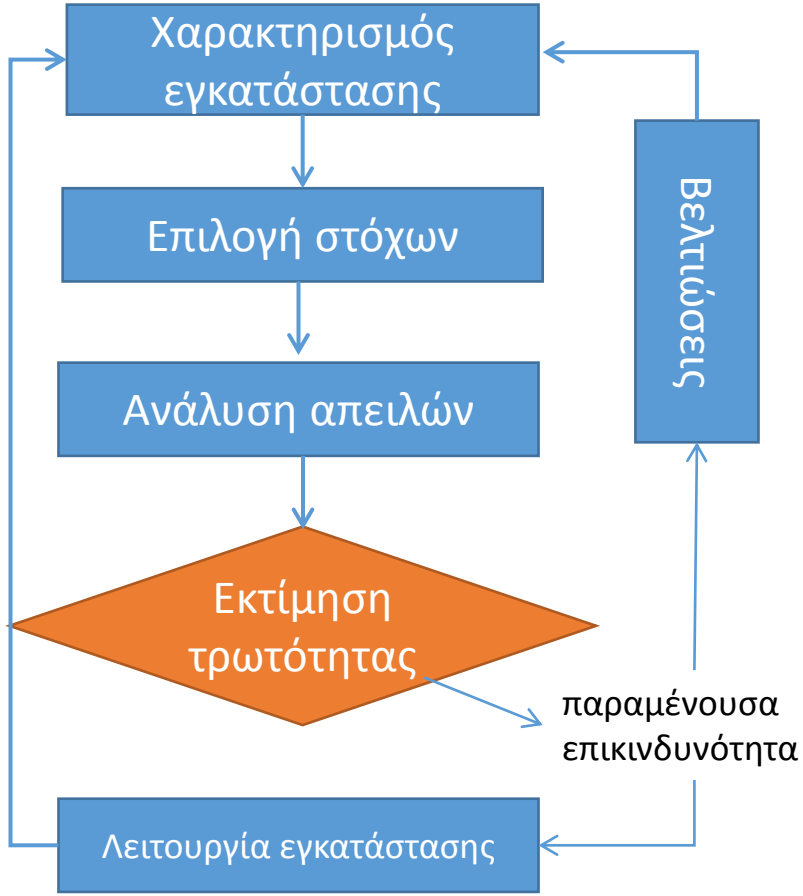
10

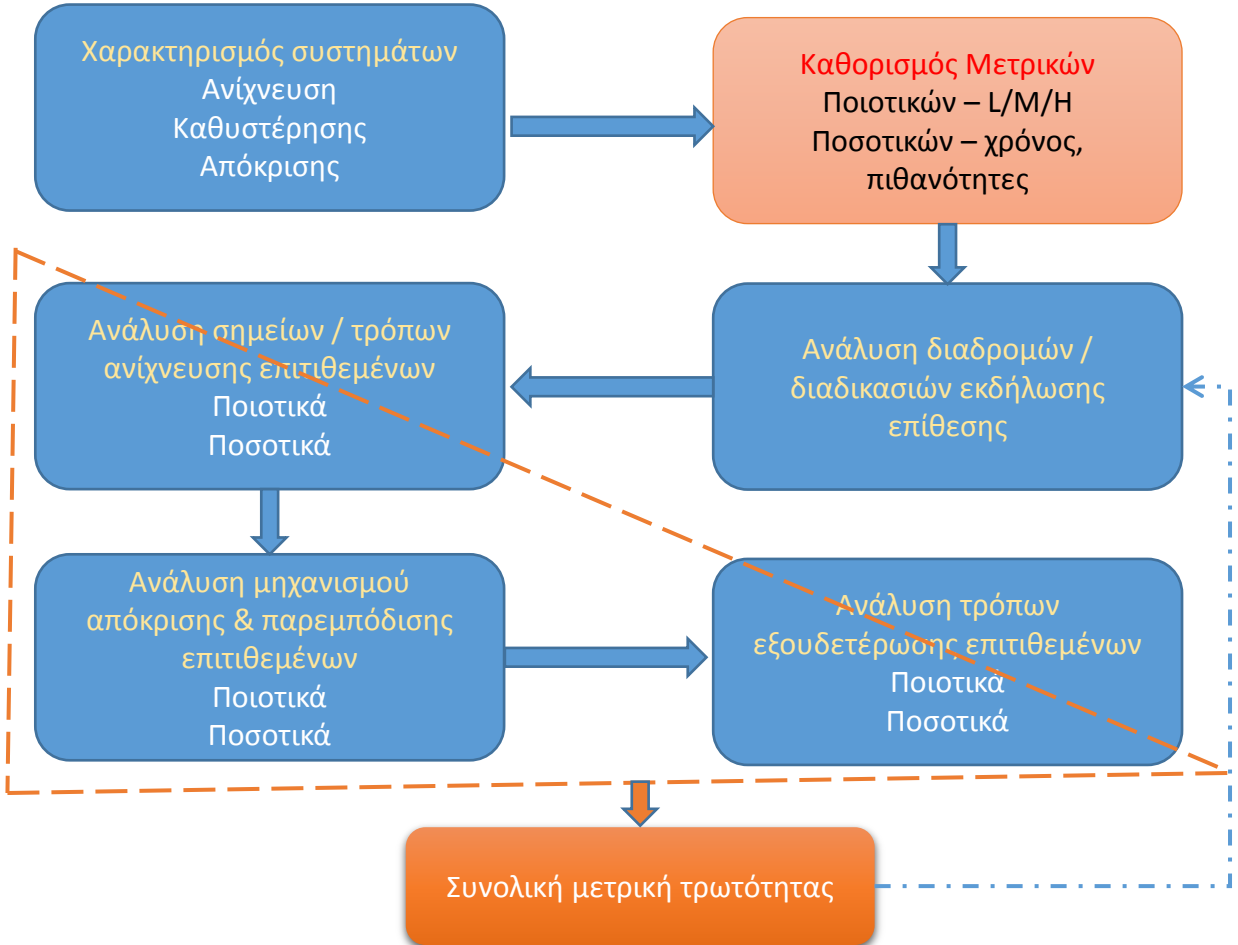
Εκτίμηση τρωτότητας

Χρήση της αρχής: «Αποτροπή, ανίχνευση, καθυστέρηση, εξουδετέρωση» (Deter, detect, delay, response)



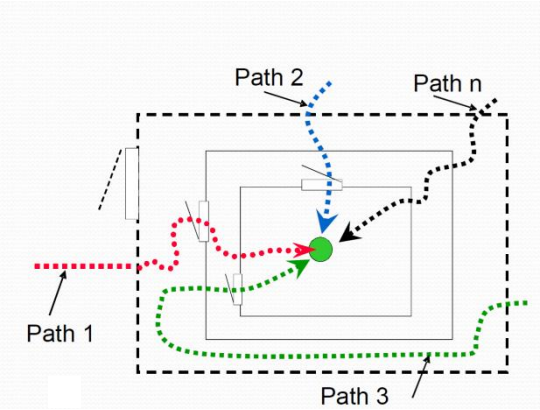
Διαδικασία εκτίμησης τρωτότητας

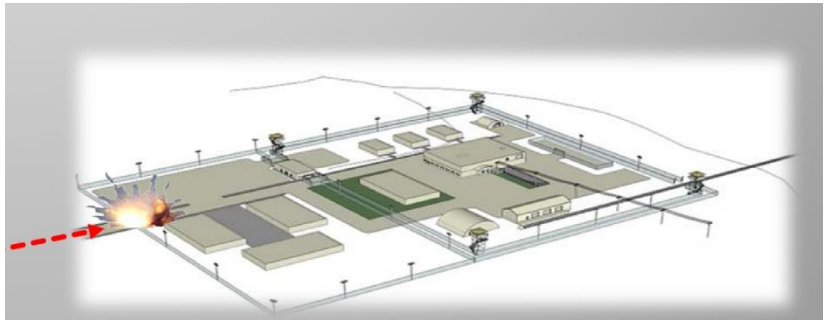




Επιλογή σεναρίου

- Επιτιθέμενοι – ομάδα αντιμετώπισης
- Ανάλυση σεναρίου και εκτίμηση χρόνων για κάθε δράση
- Τα σενάρια να έχουν σημαντικές διαφοροποιήσεις ώστε να είναι διακριτές οι διαφορές τους και η να προτεραιοποιούνται οι απειλές
- Οι επιτιθέμενοι να χρησιμοποιούν όλο το εύρος των δυνατοτήτων (cyber, εναέριες, μαζικές, …) και συνδυαστικά
- Επιλογή διαδρομής εκδήλωσης της επίθεσης να συμπεριλαμβάνει όλα τα στοιχεία της εγκατάστασης
  - Περαιτέρω ανάλυση για τα πιο επικρατέστερα
  - Τρόπος διαφυγής





Ευχαριστώ για την προσοχή σας!

Ερωτήσεις