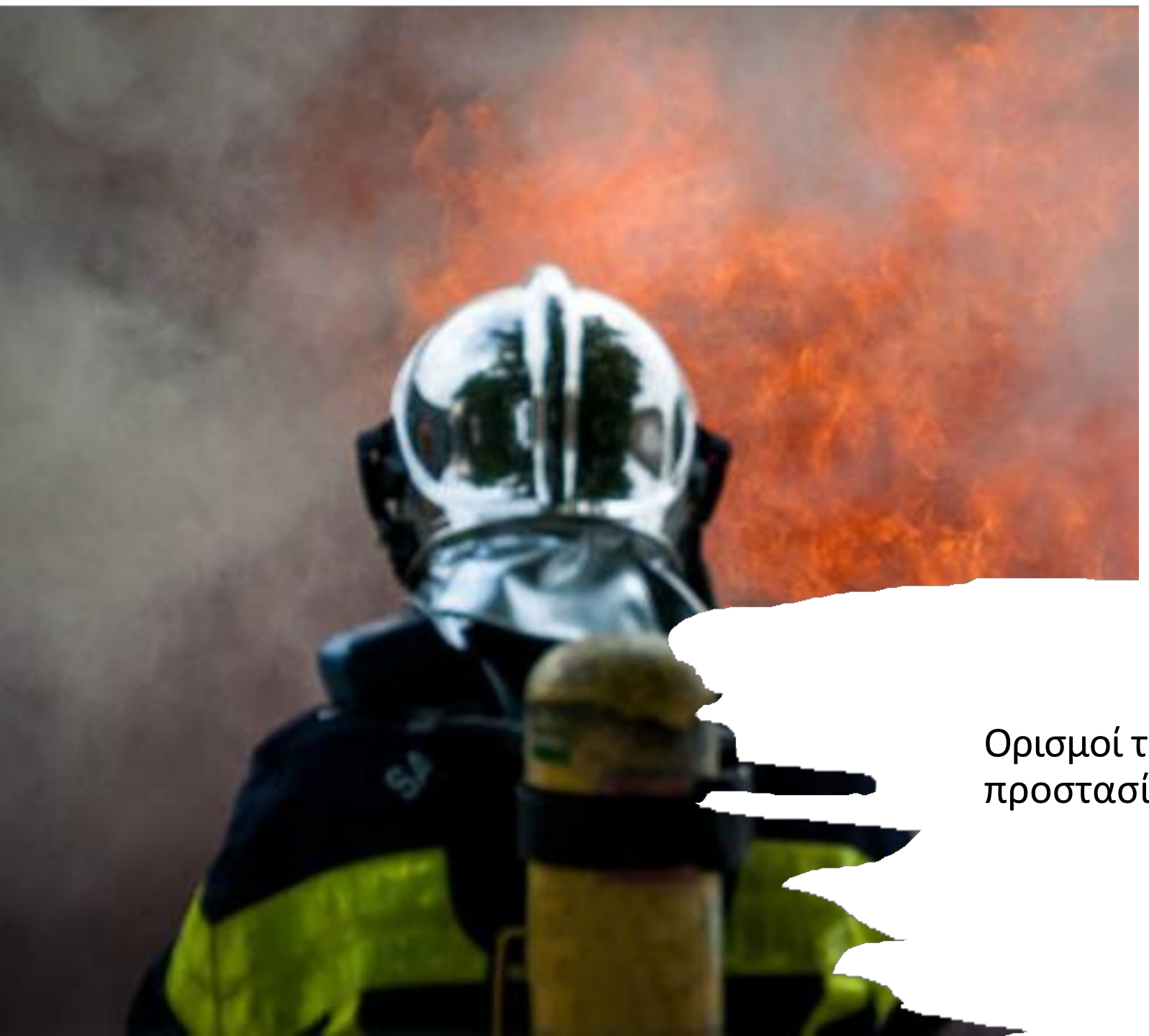
Ορισμοί των εννοιών ασφάλειας και προστασίας

Ενότητα 7 - Α1 Ασφάλεια και προστασία, δύο ξεχωριστοί αλλά εξίσου σημαντικοί τομείς

Ενότητα 7 – Δ1 Οι φάσεις της δράσης: πρόβλεψη και παρακολούθηση, αντίδραση και καταπολέμηση, αποκατάσταση (Μέρος)

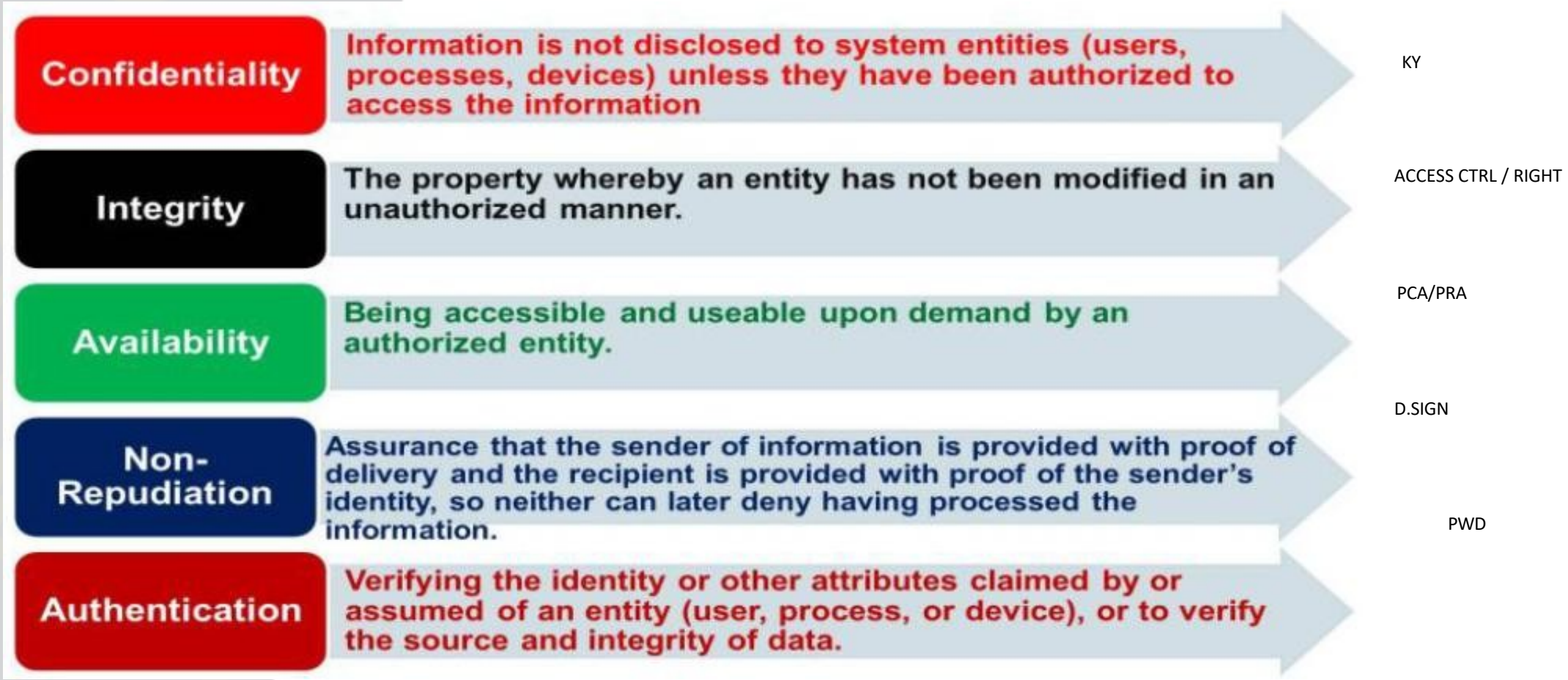
Ασφάλεια και προστασία

ΕΞΑΜΗΝΟ 10					
Ενότητα 7 - Εφαρμογή μιας αποτελεσματικής πολιτικής για την ασφάλεια στον κυβερνοχώρο		**BC 3**	**45**	*6*	**6**
Ενότητα 7-Α - Ορισμοί των εννοιών της ασφάλειας και προστασίας			**15**	**2**	**2**
Ενότητα 7-Α-1	Ασφάλεια και προστασία, δύο ξεχωριστοί τομείς αλλά ίσης σημασίας				
EU7-A-2	Κυβερνοασφάλεια: μια κοινή όραση μεταξύ χρηστών, σχεδιαστών εξοπλισμού, δίκτυα μετάδοσης, υπηρεσίες διαχείρισης δεδομένων				
UE7-C - Διαχείριση του κινδύνου που συνδέεται με τις κυβερνοεπιθέσεις			**15**	*2*	**2**
UE7-C-1	Προσδιορισμός λειτουργικών τομέων, χαρτογράφησή τους, εξασφάλιση ασφαλή διαλειτουργικότητα - Ανάγκες, διαπιστώσεις, ανάλυση				
UE7-C-2	Ασφάλιση για την κάλυψη των δαπανών που προκύπτουν από κυβερνοεπιθέσεις συστημάτων πληροφοριών				
UE7-D - Οργάνωση των διαδικασιών για τη διασφάλιση της κυβερνοασφάλειας της επιχείρησης και του περιβάλλοντός της			**15**	*2*	**2**
UE7-D-1	Οι φάσεις της δράσης: πρόβλεψη και παρακολούθηση, αντίδραση και καταπολέμηση, αποκατάσταση				
UE7-D-2	Διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας με τους συνεργάτες, τους προμηθευτές, τους πελάτες				



Ορισμοί των εννοιών ασφάλειας και προστασίας

Κυβερνοασφάλεια - Διασφάλιση πληροφοριών



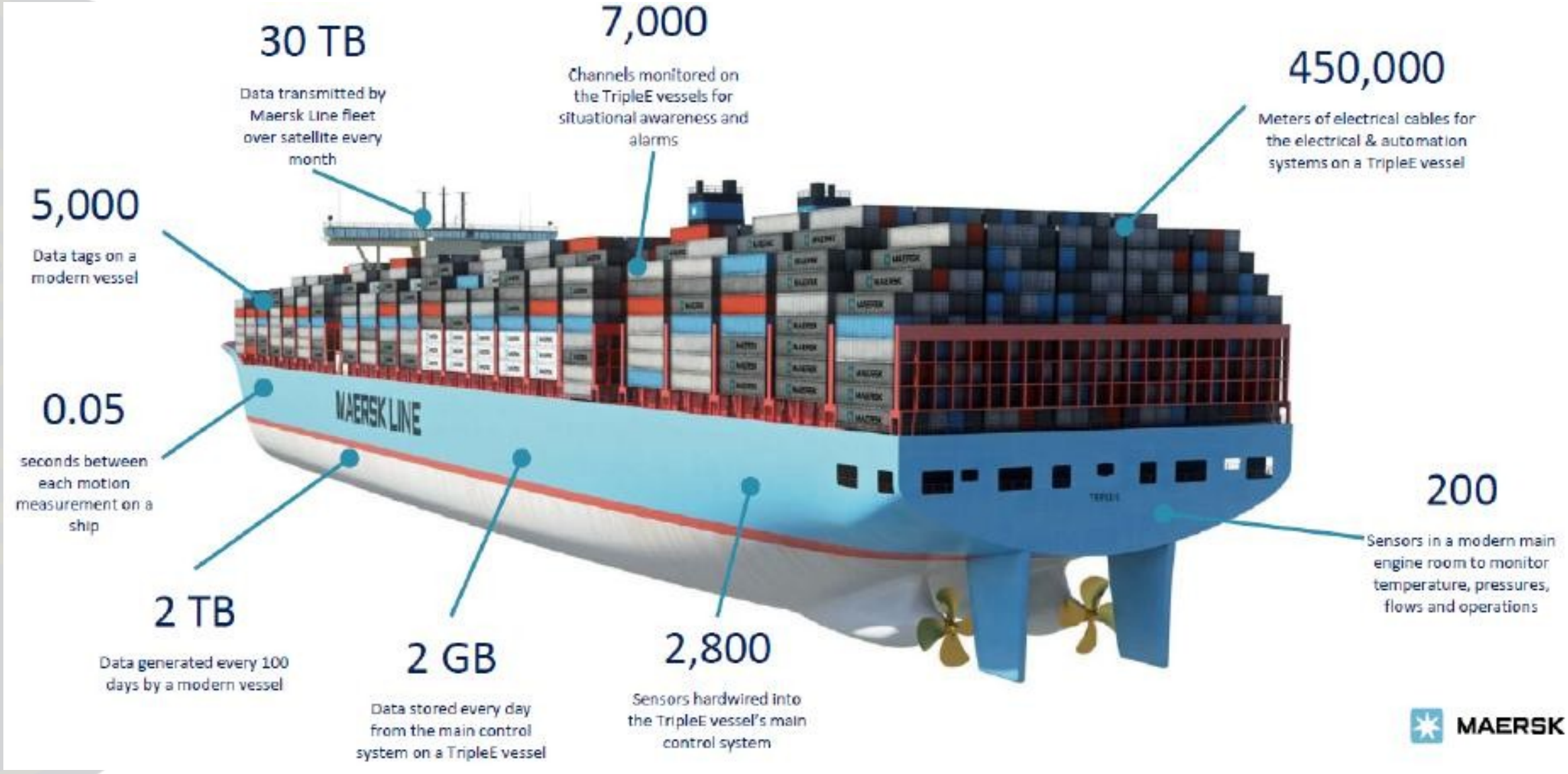
KY

ACCESS CTRL / RIGHT

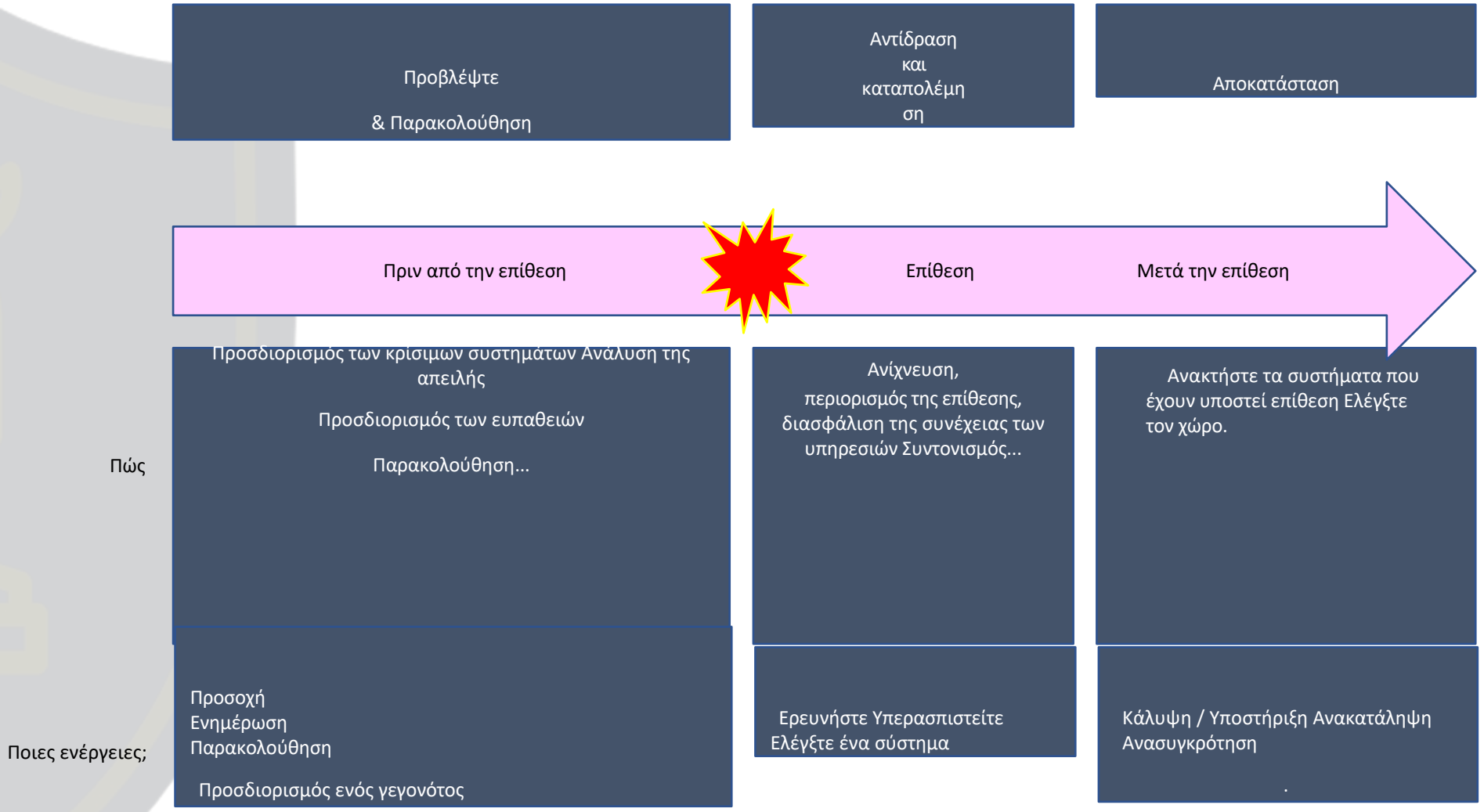
PCA/PRA

D.SIGN

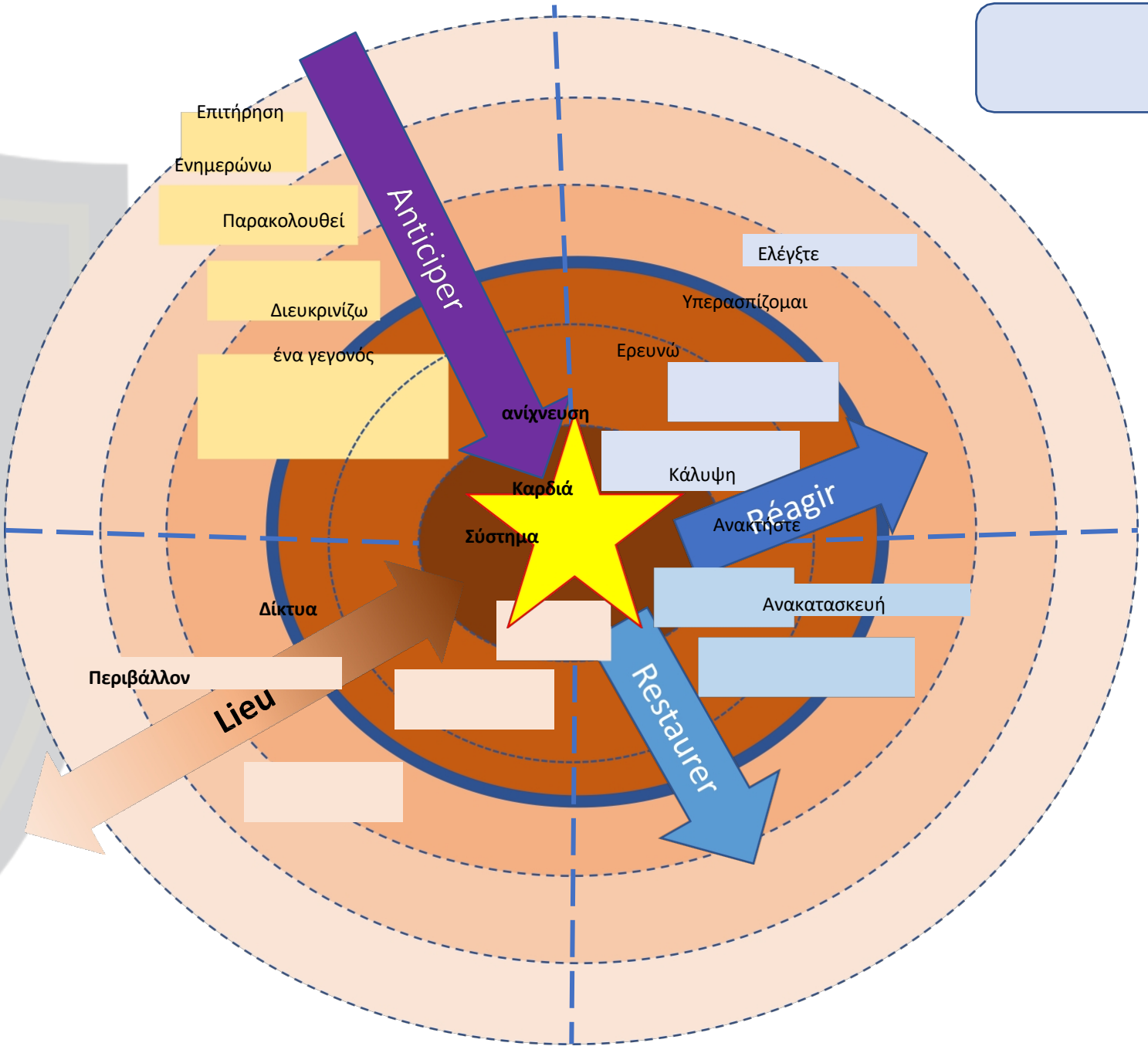
PWD


30 TB
Data transmitted by Maersk Line fleet over satellite every month
7,000
Channels monitored on the TripleE vessels for situational awareness and alarms
450,000
Meters of electrical cables for the electrical & automation systems on a TripleE vessel
5,000
Data tags on a modern vessel
0.05
seconds between each motion measurement on a ship
MAERSK LINE
2 TB
Data generated every 100 days by a modern vessel
2 GB
Data stored every day from the main control system on a TripleE vessel
2,800
Sensors hardwired into the TripleE vessel's main control system
200
Sensors in a modern main engine room to monitor temperature, pressures, flows and operations
MAERSK

Ασφάλεια – Προστασία: Οι φάσεις της καταπολέμησης



ΥΠΕΡΑΣΠΙΣΗ ΣΕ ΒΑΘΟΣ



Πρόληψη: Οργάνωση της κυβερνοασφάλειας

Διακυβέρνηση

- Ανταλλαγή πληροφοριών (ISAC)
- Κανονισμοί
  - Πλοία (ΔΝΟ)
  - Λιμενικό οικοσύστημα (NIS/LPM)
- Έλεγχοι
- Αναφορά περιστατικών

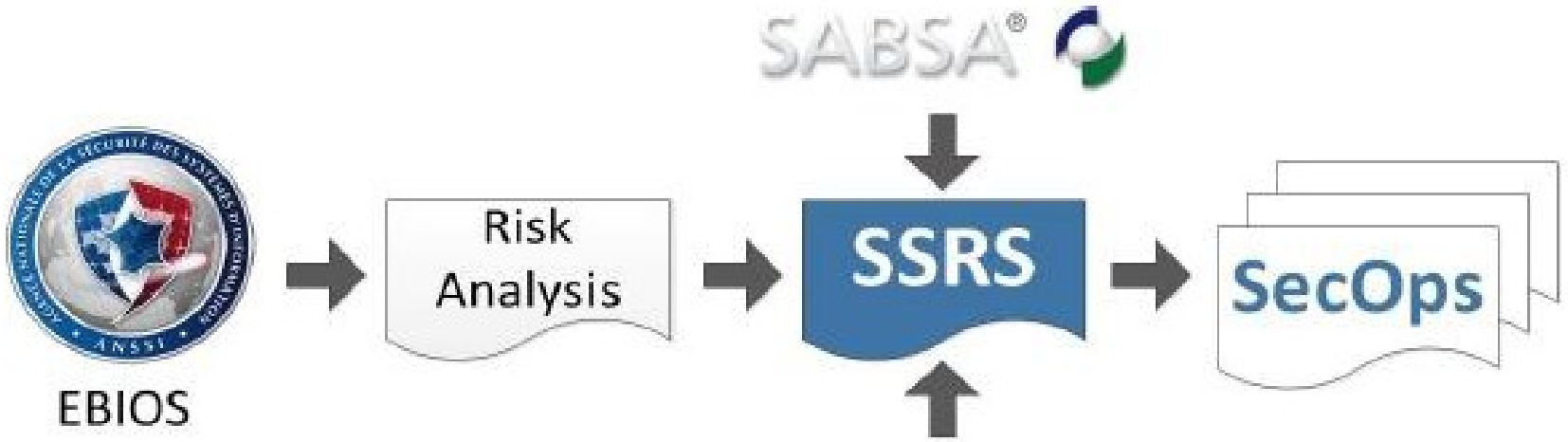
Προστασία

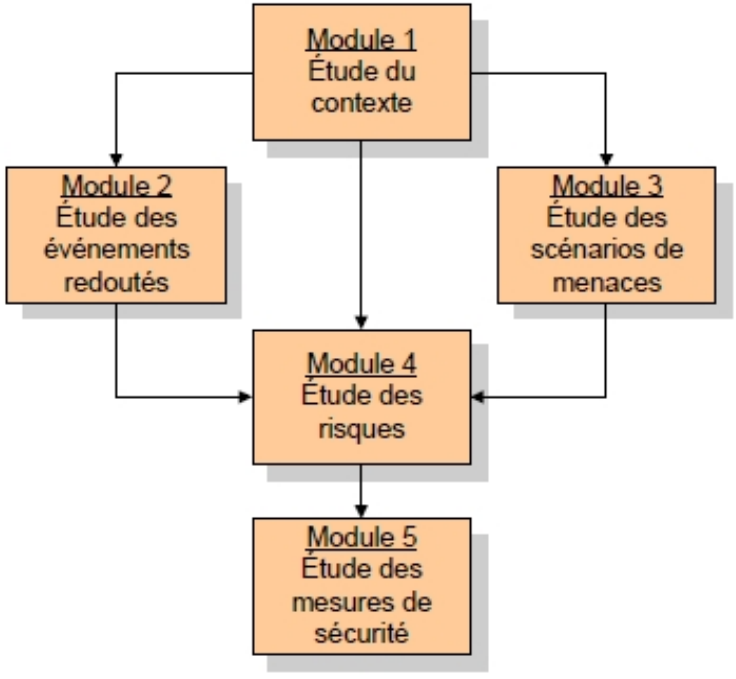
- Ευαισθητοποίηση και εκπαίδευση
- Ασφάλεια από το σχεδιασμό
- Κυβερνοβαθμοδοτήσεις (BV, DNV-GL)
- Ασφάλεια της «αλυσίδας εφοδιασμού»

Άμυνα

- M-CERT
- Επεξεργασία ειδοποιήσεων
- SOC Ναυτιλία
- Σχέδιο διαχείρισης κρίσεων τομεακός & ασκήσεις

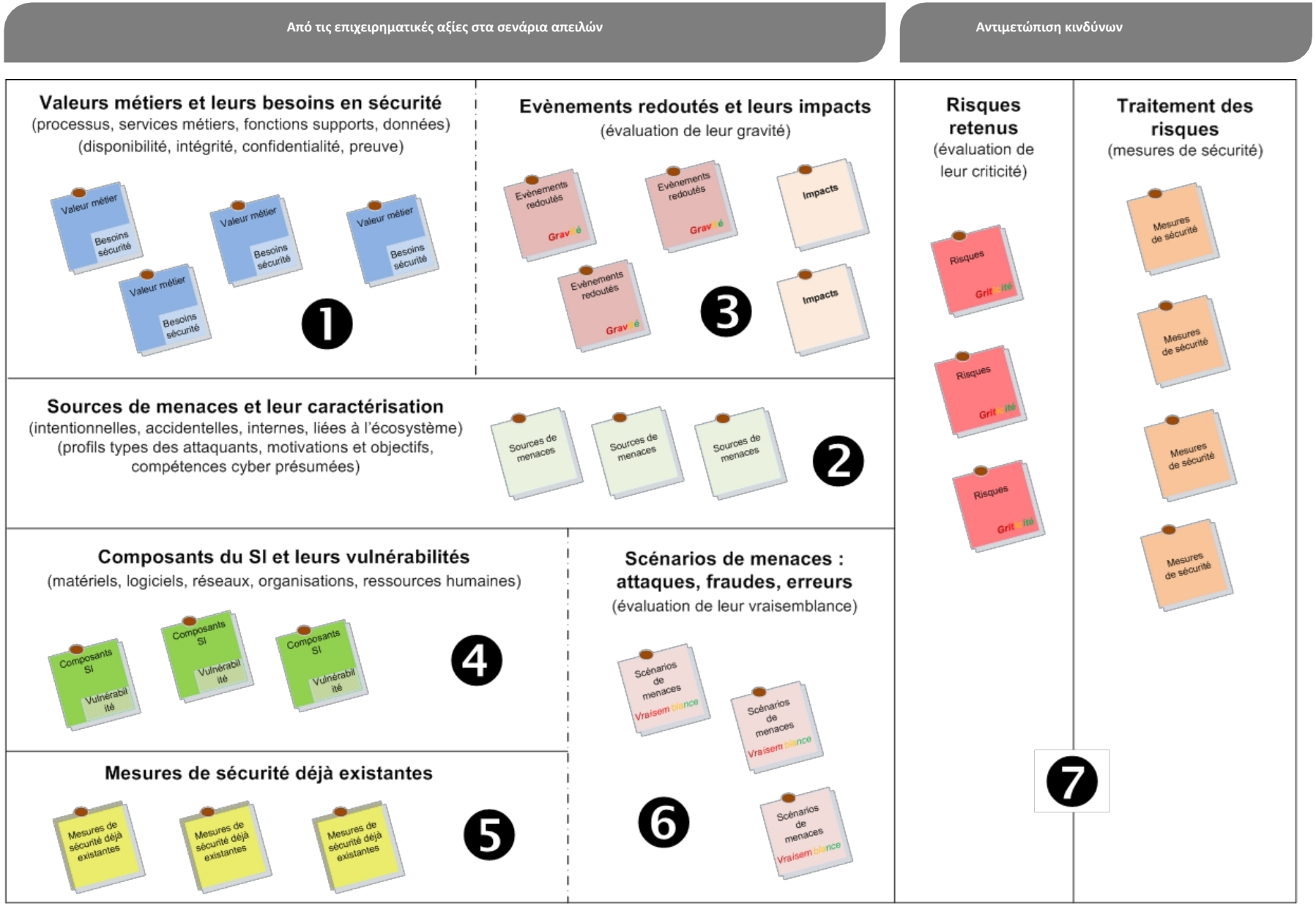
Πρόληψη: Τεκμηρίωση των κινδύνων



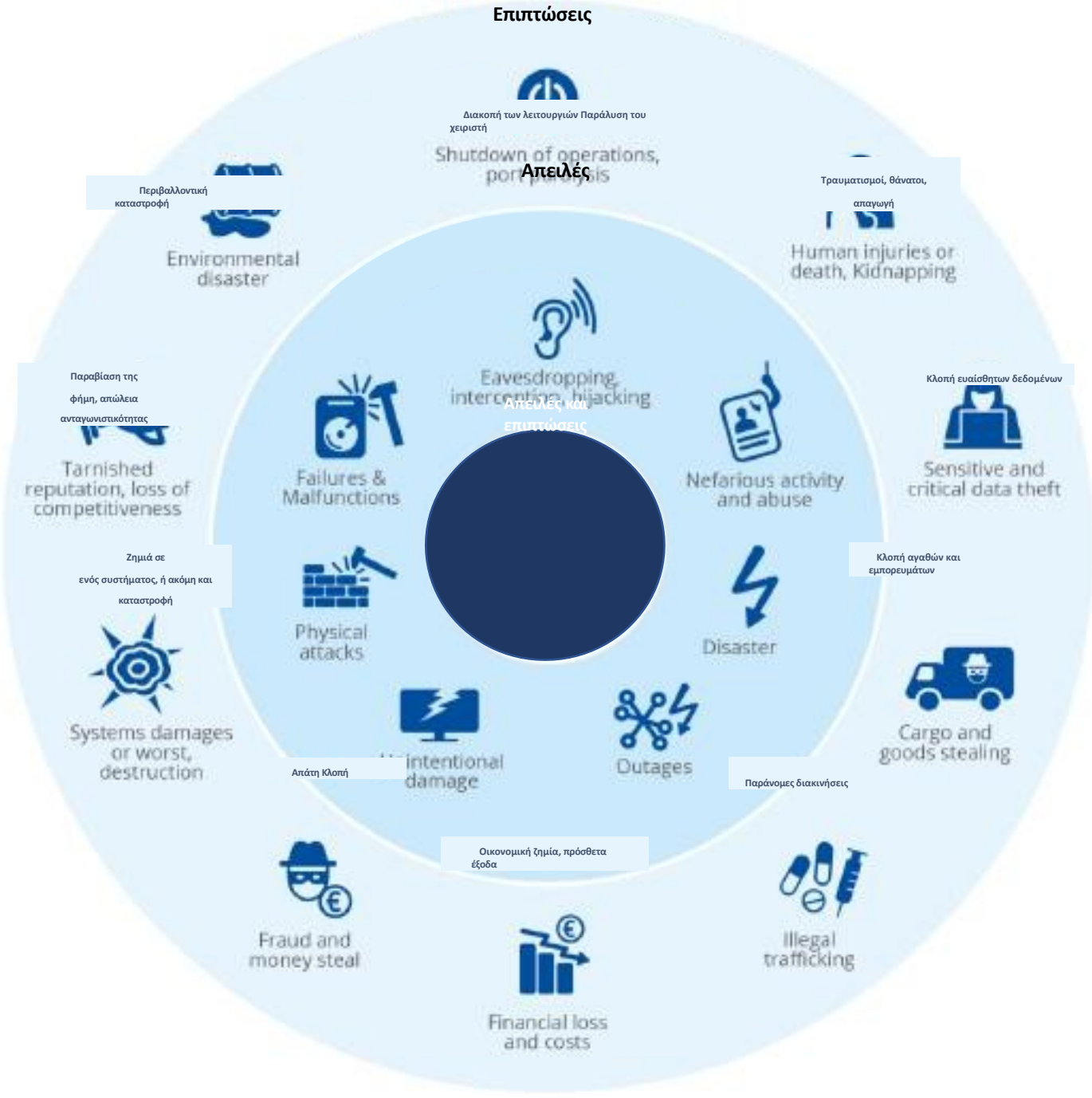


SABSA: Sherwood Applied Business Security Architecture **SSRS:** System-Specific Security Requirement Statement
SECOPS: Security Operational Procedures

Πρόληψη: Κίνδυνοι και αντιμετώπιση



Απειλές / Επιπτώσεις



Πρόληψη: Παράδειγμα

Ανάλυση επιχειρηματικών επιπτώσεων (BIA)

Σενάριο απειλής	Ευπάθεια	Κατάταξη
Κατάχρηση δεδομένων, Κατάχρηση δικαιωμάτων, Παραποίηση δικαιωμάτων, Άρνηση ενεργειών	Αδύναμα κωδικά πρόσβασης	Υψηλή
Κατασκοπεία «Παρακολούθηση»	Κωδικός πρόσβασης που αλλάζουν σπάνια	Πολύ Υψηλή

SSRS

Διαχείριση κωδικών πρόσβασης

Σύστημα

Εφαρμογή SSRS

Το σύστημα διαχείρισης χρηστών του δικτύου XXX επιβάλλει τη δημιουργία κωδικών πρόσβασης κατάλληλης πολυπλοκότητας:

Σχέδιο εφαρμογής

Ανάπτυξη πολιτικής κωδικών πρόσβασης. Θα καλύπτεται από το SSRS και το SecOPs.

SECopS

Διαχείριση πρόσβασης

Εφαρμογή SecOPs

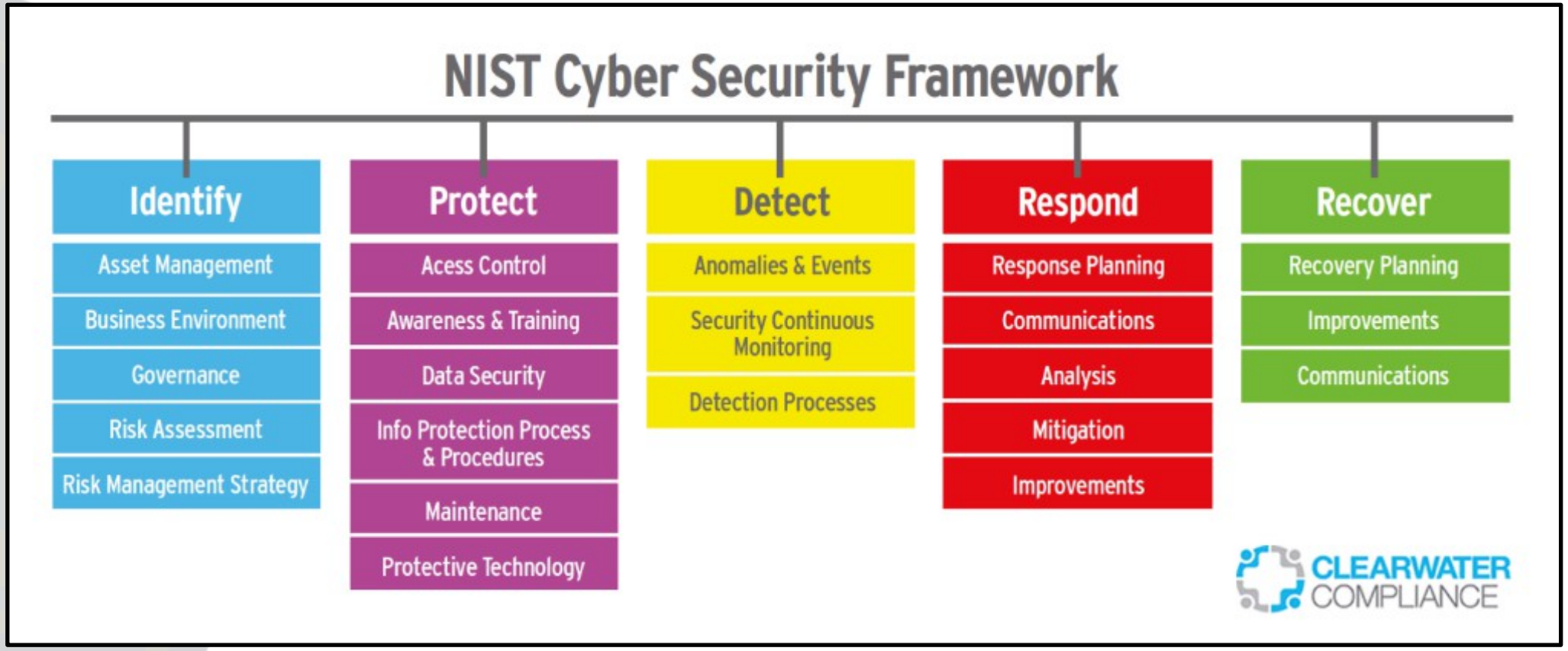
Το σύστημα διαχείρισης χρηστών του δικτύου XXX απαιτεί κωδικούς πρόσβασης

κατάλληλης πολυπλοκότητας:

- τουλάχιστον 10 χαρακτήρες
- Κωδικός πρόσβασης διαχειριστή: τουλάχιστον 12 χαρακτήρες.
- Πρέπει να συμμορφώνεται με 3 από τις 4 ομάδες χαρακτήρων:
  - τουλάχιστον ένα μικρό γράμμα (α έως ζ)
  - τουλάχιστον ένα κεφαλαίο γράμμα (Α έως Ζ)
  - τουλάχιστον ένα ψηφίο (0 έως 9) ή τουλάχιστον ένας ειδικός χαρακτήρας (π.χ.! @ # $% & *, κ.λπ.);
- Αλλάζει κάθε 90 ημέρες.

Ο κωδικός πρόσβασης νέου χρήστη ή διαχειριστή πρέπει να είναι διαφορετικός από τους 20 κωδικούς πρόσβασης που χρησιμοποιήθηκαν πρόσφατα.

πρόληψη/Δράση

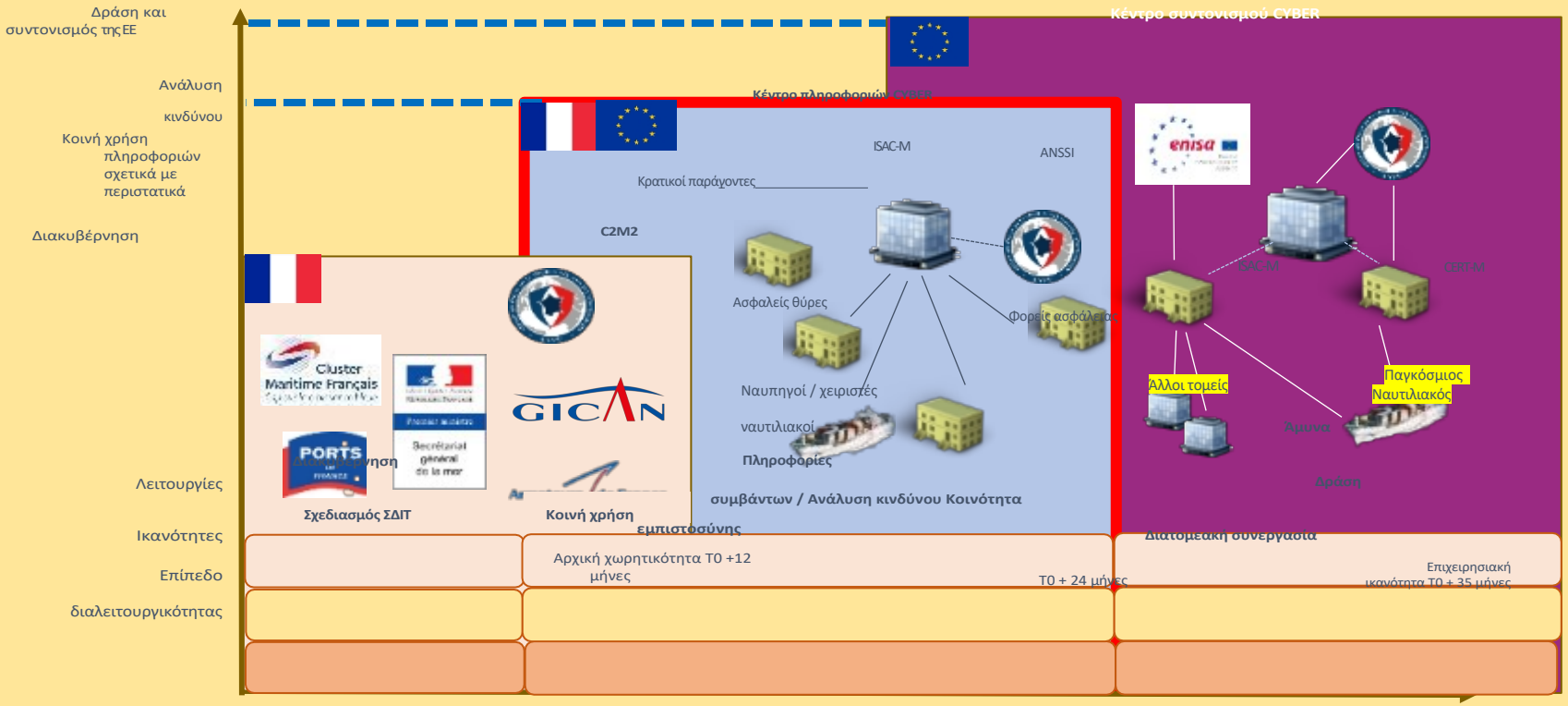


Ασφάλεια

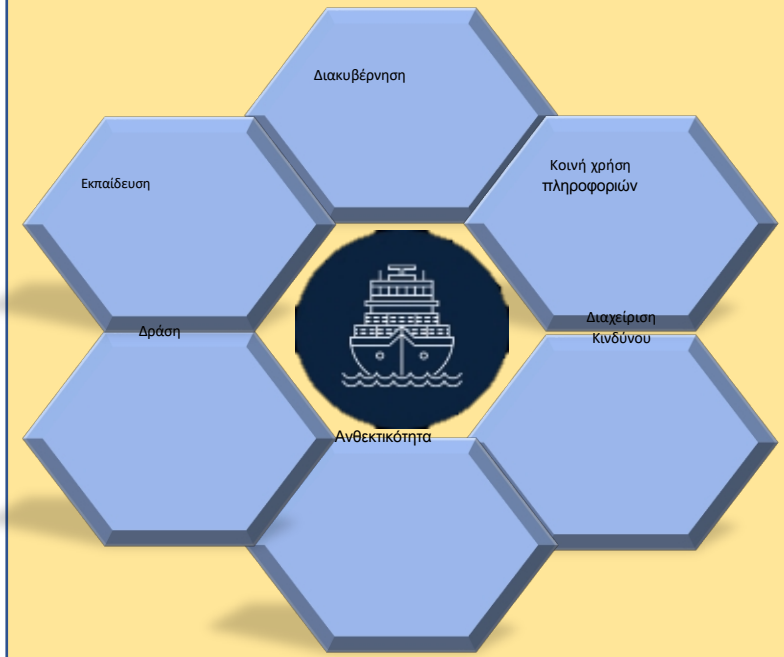
Ασφάλεια

Η πρωτοβουλία που ξεκίνησε η Επιτροπή Γαλλικής Ναυτιλίας (2018)

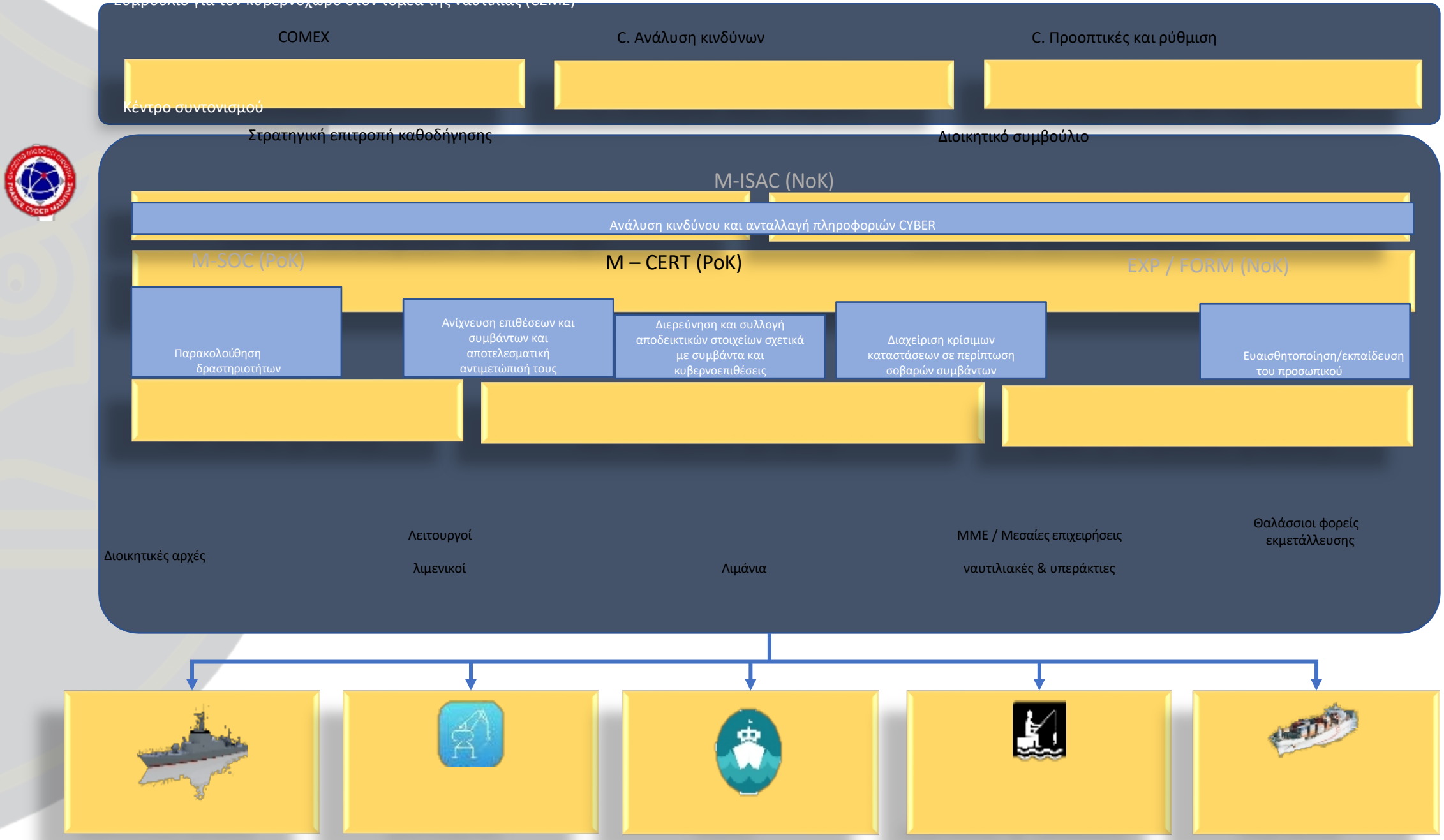
3 ΦΑΣΕΙΣ



6 ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ



Κυβερνοδιακυβέρνηση στον θαλάσσιο κόσμο – Πού βρισκόμαστε;



CERT / C-SIRT

Αποστολές

ΠΡΌΛΗΨΗ & THREAT INTEL (Παρακολούθηση, Έλεγχος και Ειδοποιήσεις)

- Ανάλυση απειλών και ανταλλαγή πληροφοριών
- Συμβουλές ασφάλειας και πληροφορίες για την κυβερνοασφάλεια
- Αναφορά δεικτών παραβίασης και υπογραφών
- Δημοσίευση ειδοποιήσεων
- Πρόληψη, εκπαίδευση, κατάρτιση.

ΔΙΑΧΕΊΡΙΣΗ ΚΑΙ ΣΥΝΤΟΝΙΣΜΌΣ ΠΕΡΙΣΤΑΤΙΚΏΝ

Τεχνική και οργανωτική διαχείριση συμβάντων.

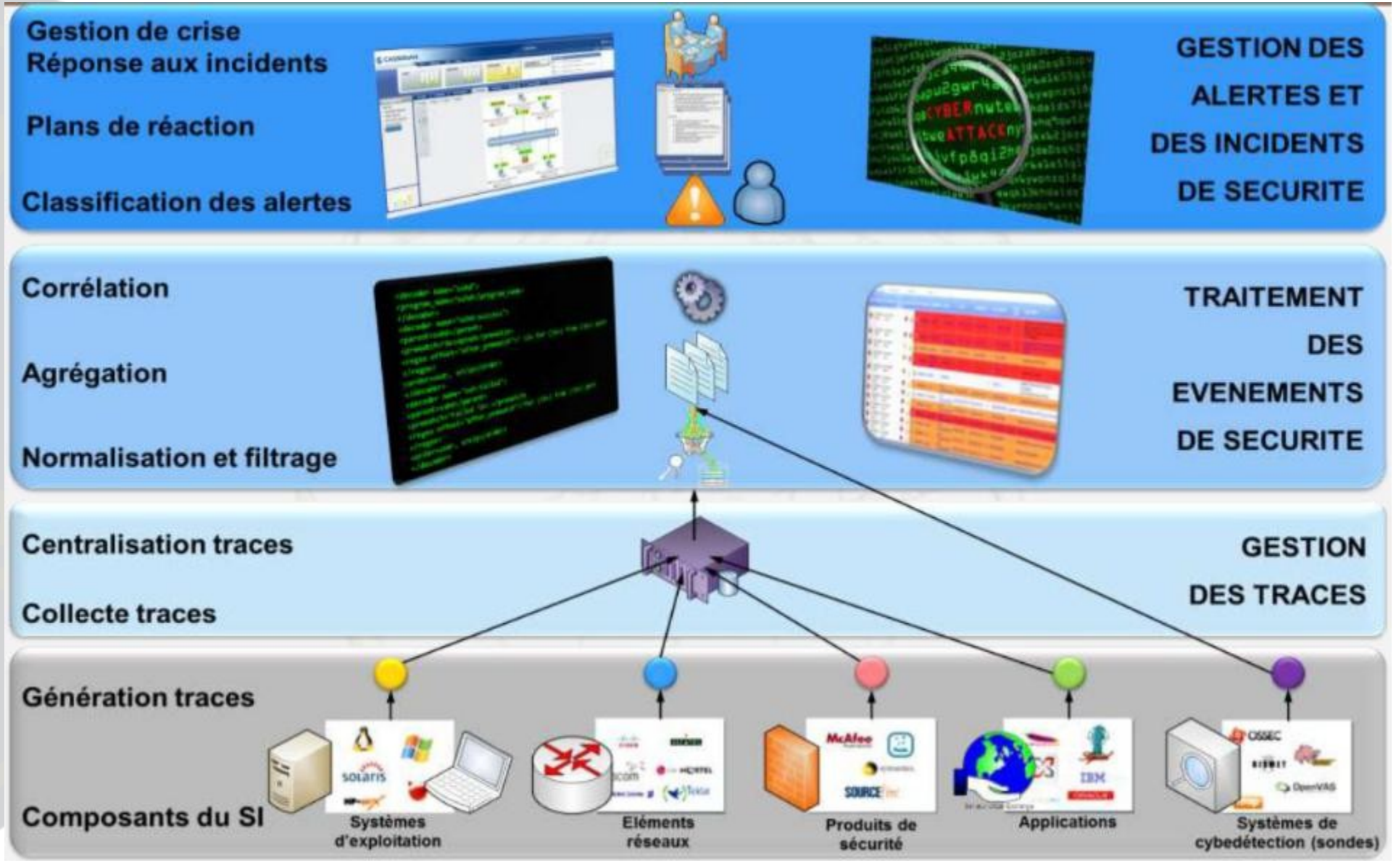
ΔΙΑΛΟΓΗ

- Συλλογή πληροφοριών σχετικά με τα περιστατικά,
- Σύνδεση περιστατικού / μέλη CERT
- Αξιολόγηση της σοβαρότητας του συμβάντος

ΣΥΝΤΟΝΙΣΜΌΣ

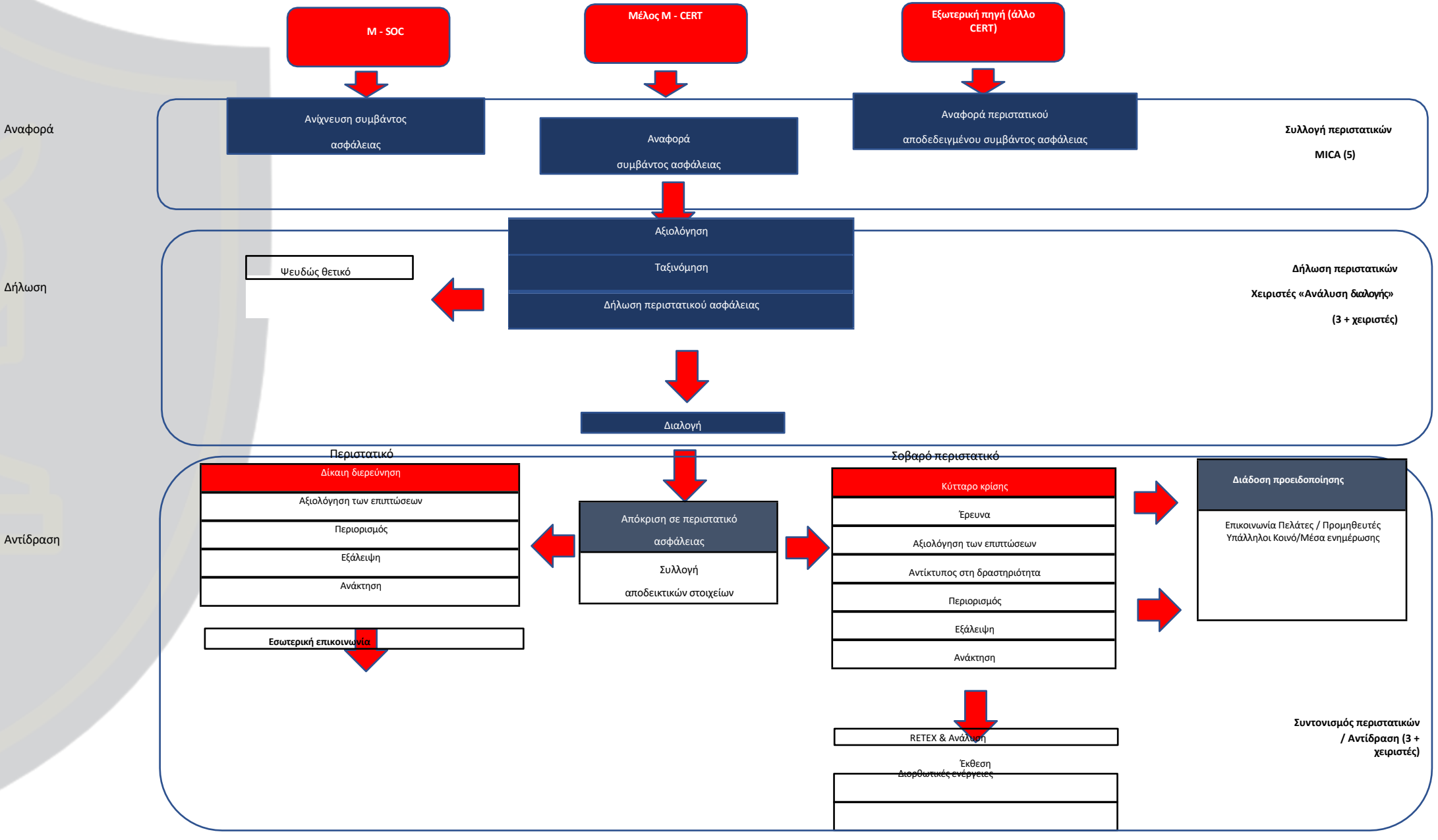
Συντονισμός (οντότητα που υποβάλλει την αναφορά, εταίροι που εμπλέκονται στην επίλυση του συμβάντος). Περιορισμός

Τεχνική οργάνωση ενός CERT



Λειτουργία μιας CERT Maritime

Οργανόγραμμα διαχείρισης περιστατικών



Κίνδυνοι και ικανότητες

Έξι τύποι απειλών

Κακόβουλο λογισμικό: Κακόβουλο λογισμικό του οποίου η διάδοση είναι ανεξέλεγκτη

Script kiddy (απασχολούμενος έφηβος ή, γενικότερα, μοναχικός και ευκαιριακός εισβολέας):

- Πολύ περιορισμένα μέσα (< 100 €)
- Το παιχνίδι (και ενδεχομένως το κέρδος) ως κίνητρο
- Ευκαιριακή επίθεση

Κακόβουλος υπάλληλος (μνησικακία / απληστία):

- Μικρά μέσα (< 1.000 €)
- Κύρια κίνητρο: να βλάψει τον εργοδότη του, αποφεύγοντας τα θύματα
- Διακριτικότητα, όταν είναι δυνατόν
- Εύκολη πρόσβαση σε όλα τα μέρη του πλοίου

Τρομοκρατική ομάδα:

- Μέτρια μέσα (από 10 έως 50 000 €)
- Αναζήτηση ανθρώπινων θυμάτων, υλικών ζημιών, υψηλή προβολή στα μέσα μαζικής ενημέρωσης

Εγκληματική οργάνωση:

- Υψηλά μέσα (της τάξης του ενός εκατομμυρίου ευρώ)
- Στόχος κερδοφορίας
- Χαμηλές ηθικές υποχρεώσεις
- Αναζήτηση διακριτικότητας

Κατάσταση:

- Σχεδόν απεριόριστα μέσα
- Στόχοι κάθε είδους
- Απουσία ηθικών περιορισμών
- Απαιτείται διακριτικότητα

Ανίχνευση περιστατικών

SIEM

1 – Εφαρμογή των κανονισμών

Ανταλλαγή πληροφοριών

- Παρακολούθηση υποδομών
- Εστίαση (συλλογή αρχείων καταγραφής & διατήρησης)
- Αντιμετώπιση συμβάντων
- Συντονισμένες επιχειρήσεις

2 – Ικανότητα κυβερνοάμυνας

(ενάντια στις πιο διαδεδομένες επιθέσεις)

- Δυνατότητες ανίχνευσης (όλων των τύπων συμβάντων – εσωτερικών/εξωτερικών)
- Λίστα προκαθορισμένων σεναρίων
- Διαδικασία αντίδρασης
- Συντονισμός SOC

3 – προσφορά συνολικής ασφάλειας στον κυβερνοχώρο

Κοινή χρήση της ανάλυσης κινδύνου

- Παρακολούθηση κρίσιμων συστημάτων
- Προβλέψεις απειλών
- Ισχυρή διακυβέρνηση (δείκτες & συγκριτική αξιολόγηση)
- Λήψη υπόψη των κινδύνων του τομείς εκτός του κυβερνοχώρου

SIEM = SIM + SEM (Συμβάν + Γεγονός)

Αναφορά: ETSI GS ISI 004 V1.1.1 (2013-12) - Δείκτες ασφάλειας πληροφοριών (ISI) · Κατευθυντήριες γραμμές για την εφαρμογή ανίχνευσης συμβάντων

ETSI GS ISI 003 V1.1.2 (2014-06) - Δείκτες ασφάλειας πληροφοριών (ISI) · Βασικοί δείκτες απόδοσης ασφάλειας (KPSI)

ΚΙΝΔΥΝΟΙ

Σενάρια Πολιτικό

πλοίο

Γενικευμένη επίθεση μέσω παραβίασης ενός δορυφορικού φορέα εκμετάλλευσης Κατασκοπεία

Σκόπιμη πρόκληση κρίσης πανικού
Υπερφόρτωση των δικτύων

Τροποποίηση ναυτικών χαρτών (παραβίαση ενός εκδότη)

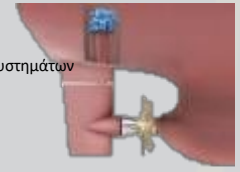
Παραβίαση του συστήματος πληροφοριών του πλοιοκτήτη από πλοίο

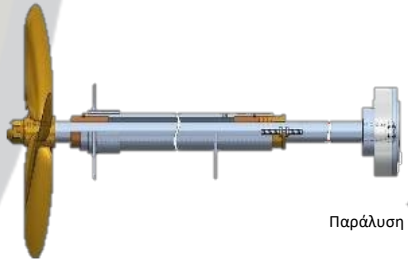
Τροποποίηση των χαρτογραφικών αναφορών

Παράπλευρη GPS / Ραντάρ

Παράλυση συστημάτων

ελιγμών





Ψευδείς συναγερμοί πυρκαγιάς

Παράλυση του πλοίου (λογισμικό εκβιασμού)

Διακοπή ρεύματος

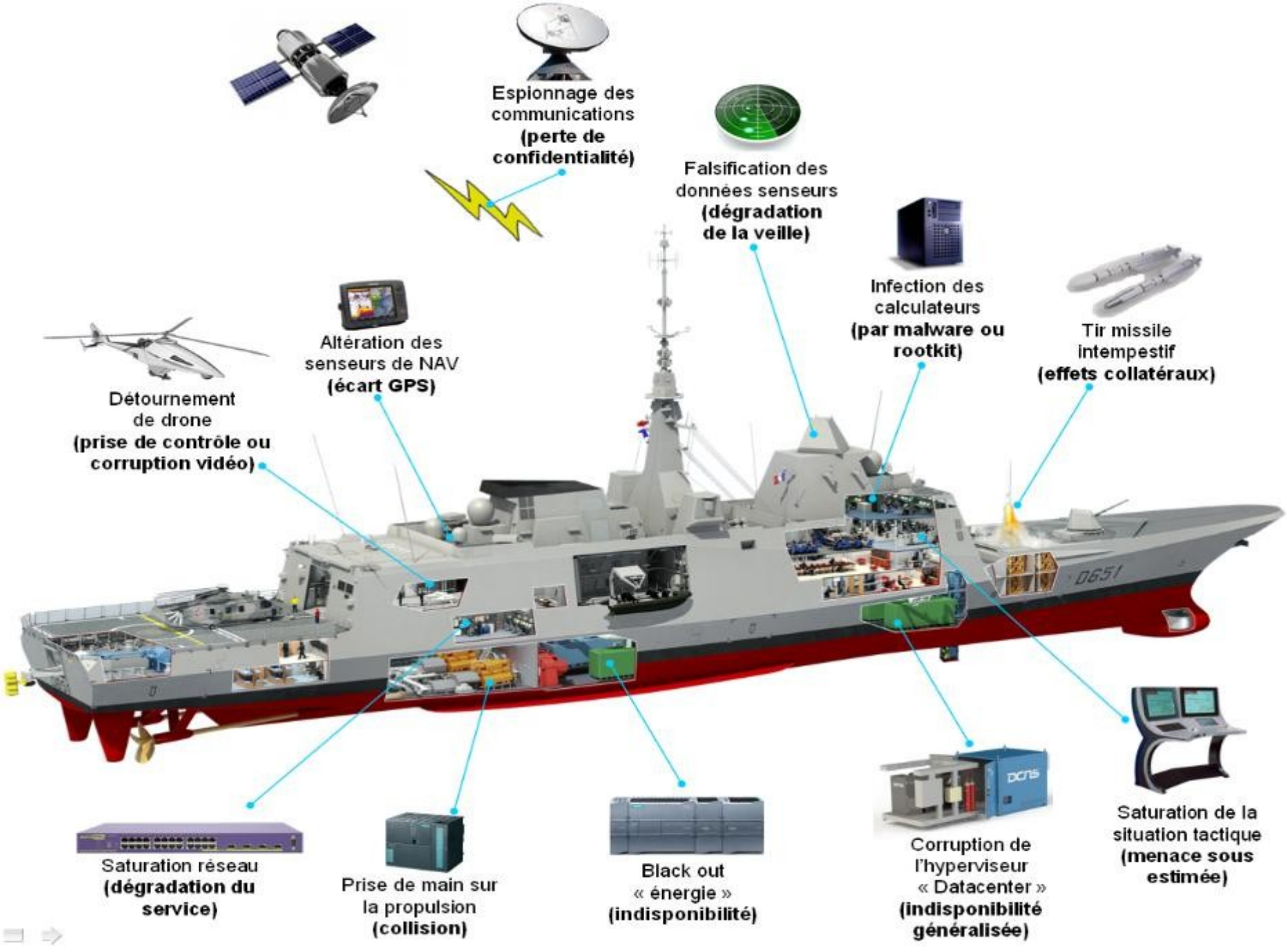
Σαμποτάζ πλοίου / στόλου (στοχευμένη επίθεση)

Βλάβη στη σταθερότητα του πλοίου

Κίνδυνος ειδικός για κάθε περιβάλλον / σύστημα

ΚΙΝΔΥΝΟΙ

Σενάρια Στρατιωτικό πλοίο



ΣΤΡΑΤΗΓΙΚΕΣ

Παρουσίαση της στρατηγικής

Στρατηγικές κατευθύνσεις

ΟΙ ΚΥΡΙΕΣ ΣΤΡΑΤΗΓΙΚΕΣ ΓΡΑΜΜΕΣ

Μεταφορά στον τομέα της ναυτιλίας και των λιμένων των βασικών αρχών της κυβερνοασφάλειας που έχουν ορίστηκαν σε διατομεακό επίπεδο από τον νόμο LPM και την οδηγία NIS σχετικά με:

- ***Τη διακυβέρνηση (γενική πολιτική για την κυβερνοασφάλεια)***
- ***Την προστασία των δικτύων και των συστημάτων πληροφοριών***
- ***Την άμυνα των δικτύων και των συστημάτων πληροφοριών***
- ***Η ανθεκτικότητα των δραστηριοτήτων***

Καθορισμός δράσεων και καθηκόντων

Πίνακας παρακολούθησης δράσεων/δείκτες

Παρουσίαση της στρατηγικής

Σχέδιο δράσης (1.1 έως 1.7)

Τομέας	Αρ. Δράση	Δράση	Εργασία(-ες)	Υπεύθυνος	Συνεισφέροντες	Προθεσμία	Σχόλια	Πρόοδος προ
L1: ΔΙΑΚΥΒΕΡΝΗΣΗ	Δράση 1.1	Δημιουργία και προώθηση της διακυβέρνησης της θαλάσσιας κυβερνοασφάλειας	Ανάπτυξη και προώθηση του συμβουλίου για την κυβερνοασφάλεια στον που συστάθηκε το 2019	Γραμματεία του C2M2	Επιτροπές του C2M2	2019		Πραγματοποιήθηκε
			Δημιουργία και τήρηση πίνακα παρακολούθησης των δράσεων και των υπευθύνων	Γραμματεία του C2M2	Επιτροπές του C2M2	Σεπτέμβριος 2021	Ο πίνακας αυτός θα αναθεωρείται κάθε συνεδρίαση του COMEX	Να ξεκινήσει
	Δράση 1.2	Δημιουργία και διατήρηση χαρτογράφησης των κινδύνων του θαλάσσιου τομέα	Δημιουργία χαρτογράφησης των χρησιμοποιούμενων συστημάτων πληροφοριών στον τομέα της ναυτιλίας και των λιμένων, πριν από την χαρτογράφησης των κινδύνων.	Επιτροπή ανάλυσης Κίνδυνοι C2M2	Όλοι οι φορείς σχετικοί κίνδυνοι του ναυτιλιακού	Ιανουάριος 2022	Καθορισμός του πεδίου εφαρμογής και βάθος ανάλυσης των λεπτομερειών κοινή χρήση πληροφοριών...	ξεκίνησε
			Δημιουργία και ενημέρωση χαρτογράφησης των κινδύνων στον κυβερνοχώρο στον ναυτιλιακό τομέα.	Επιτροπή ανάλυσης κινδύνων C2M2	Όλοι οι σχετικοί σχετικοί φορείς του ναυτιλιακού	Ιούνιος 2022		Να ξεκινήσει
	Δράση 1.3	Εφαρμογή και εφαρμογή για τον ναυτιλιακό τομέα της εθνικοί δείκτες κυβερνοασφάλειας για την παρακολούθηση των πολιτικών και την αξιολόγηση της αποτελεσματικότητάς τους.	Ανάπτυξη δεικτών παρακολούθησης των δράσεων της της παρούσας στρατηγικής	Επιτροπές του C2M2	Επιτροπές του C2M2	Απρίλιος 2022	Προσθήκη στήλης δεικτών στον παρόντα πίνακα	Να ξεκινήσει
			Ενημέρωση του πίνακα ελέγχου για την εξέλιξη των δεικτών	Επιτροπές του C2M2	Επιτροπές του C2M2	Απρίλιος 2022	Μόνιμη δράση	Να ξεκινήσει
			Ετήσια ανασκόπηση των δεικτών και εξέταση των δράσεων που πρέπει να αναληφθούν αναλόγως	COMEX του C2M2	Επιτροπές του C2M2	Απρίλιος 2022	Συνάντηση του COMEX	Να ξεκινήσει
	Δράση 1.4	Συντονισμός των θέσεων και την δράση της Γαλλίας των διεθνών εταίρων του διεθνείς	Συνεισφορά στη σύνταξη ανακοινώσεων και προτάσεις προς τον IMO	DGITM/DAM (πλοία) DGITM/DST (λιμάνια)	C2M2	Δράση μόνιμη	Το C2M2 συντονίζει, αλλά το Η επικύρωση είναι διαυπουργική και RP με τον IMO.	ξεκίνησε
			Συμβολή στις ευρωπαϊκές εργασίες μέσω των ομάδων εργασία της ΕΚ (π.χ. MARSEC, NIS Cooperation group, ECGFF Cybersecurity WG)	Επιτροπών C2M2	SGMER, MIMER, MTE, ANSSI, Επιτροπή France Maritime	Δράση μόνιμη		που ξεκίνησε
	Δράση 1.5	Υλοποίηση δράσεων ευαισθητοποίησης σχετικά με Κυβερνοασφάλεια και δημιουργία πλαίσιο κατάρτισης απευθύνεται σε όλους τους επαγγέλματα του ναυτιλιακού τομέα	Προσδιορισμός των υφιστάμενων προσφορών και υποβολή τους στον τομέα ναυτιλιακούς οδηγούς (FR, EE)	France Cyber Ναυτιλία	C2M2 DGITM/DAM (πλοία) DGITM/DST (λιμάνια)	Μάρτιος 2022	Ενημέρωση των οδηγών καλών πρακτικών υφιστάμενες πρακτικές	Να ξεκινήσει
			Ανάπτυξη πλατφόρμας ευαισθητοποίησης CYBER ναυτιλιακού τομέα σε σχέση με τις εθνικές και υφιστάμενες ευρωπαϊκές	France Cyber ναυτιλιακές	C2M2 DGITM/DAM (πλοία) DGITM/DST (λιμάνια)	Ιούνιος 2022	Σε σχέση με Cybermalveillance.gouv.fr	Να ξεκινήσει
	Δράση 1.6	Οργάνωση και έλεγχος του ανταλλαγή πληροφοριών για όλοι οι φορείς	Εκδώστε ένα ενημερωτικό δελτίο C2M2 cyber ανά έτος (γενικά θέματα και διεθνή επικαιρότητα, έργα)	Γραμματεία του C2M2	Επιτροπές C2M2	Τριμηνιαία	Ξεκίνησε το 2018 · επισημοποίηση της πεδίο εφαρμογής της παρούσας επιστολής με την FCM	Ολοκληρώθηκε
			Ανάπτυξη και δημοσίευση τεχνικών δελτίων	France Cyber Maritime	ANSSI (CERT-FR)		Σύμφωνα με το πρόγραμμα που θα καταρτιστεί από τη France Cyber Maritime	Να ξεκινήσει

Παρουσίαση της στρατηγικής

Σχέδιο δράσης (2.1 έως 2.4)

Τομέας	Αρ. Δράση	Δράση	Εργασία(-ες)	Υπεύθυνος	Συνεισφέροντες	Προθεσμία	Σχόλια	Πρόοδος προ
L2: ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ	Δράση 2.1	Ανάλυση των αναγκών των νομοθετικών και κανονιστικών εξελίξεων που ισχύουν στον ναυτιλιακό τομέα	Συμπεράσματα από την ανάλυση των κινδύνων, συμπεριλαμβανομένων των εμπειριών από περιστατικά ασφαλείας, προκειμένου να καθοριστούν οι ανάγκες για εξελίξεις.	Επιτροπή Προοπτικής και Ρύθμισης C2M2	France Cyber Maritime, Επιτροπή Ανάλυσης Κινδύνων	Μόνιμη δράση		Να ξεκινήσει
			Παρακολούθηση των εξελίξεων των διεθνών κειμένων και προτύπων που ενδέχεται να δικαιολογούν την αναθεώρηση των εθνικών κειμένων εθνικών	Επιτροπή Προοπτικής και ρύθμισης C2M2	DGITM/DAM (πλοία) DGITM/DST (λιμάνια) ANSSI	Δράση μόνιμη		ξεκίνησε
	Δράση 2.2	Συμβολή στη δημιουργία ενός πλαισίου πιστοποίησης/σήμανσης προϊόντων και υπηρεσιών που ανταποκρίνονται στις ανάγκες του ναυτιλιακού τομέα	Υποστήριξη μιας διαδικασίας πιστοποίησης/σήμανσης ενώπιον του ΔΝΟ σε συνεργασία με τις διοικήσεις και τα νηογνώμονα με βάση τις υπάρχουσες εργασίες υφιστάμενων	MIMER / DAM	DGITM/DAM (πλοία) DGITM/DST (λιμάνια) ANSSI	2024	Σημειώστε τις δράσεις που πραγματοποιήθηκαν κατά τη διάρκεια του έτους	Να ξεκινήσει
	Δράση 2.3	Καθορισμός ενός πλαισίου αναφοράς για τη συστηματική συνεκτίμηση του κυβερνοχώρου στα σχέδια σχεδιασμού και κατασκευής πλοίων και λιμενικών υποδομών	Ανάπτυξη της «κυβερνοασφάλειας από το σχεδιασμό» μεταξύ των βιομηχανικών φορέων	Επιτροπή Προοπτικής και Ρύθμισης C2M2	GICAN ANSSI	Μόνιμη δράση	Σημειώστε τις δράσεις που πραγματοποιήθηκαν κατά τη διάρκεια του έτους	Να ξεκινήσει
			Ενσωμάτωση της κυβερνοασφάλειας στις σκέψεις για την ανάπτυξη του αυτόνομου πλοίου	Επιτροπή Προοπτικής και ρύθμισης C2M2	DGITM / DAM CLUSTER MARITIME ANSSI	Δράση μόνιμη	Στο πλαίσιο του ΔΝΟ διεξάγονται συζητήσεις στις ομάδες που ασχολούνται με τα αυτόνομα πλοία.	Να ξεκινήσει
	Δράση 2.4	Διεξαγωγή ειδικών έργων για την ασφάλεια των βασικών συστημάτων	Ενσωμάτωση των κινδύνων παρεμβολών και παραπλάνησης των GNSS και των συνεπειών τους σε συστήματα όπως το AIS ή τις πληροφορίες PNT	Επιτροπή ανάλυσης Κινδύνων C2M2	DGITM CNES ANFR	Σεπτέμβριος 22	Διαυπουργική ομάδα εργασίας - Παρεμβολές AIS / GNSS	ξεκίνησε
			Συνέχιση της διασφάλισης των συστημάτων πλοήγησης	Επιτροπή ανάλυσης κινδύνου C2M2	CNES CCTA	2024		Να ξεκινήσει
			Συμβολή στην ασφάλεια των λιμενικών συστημάτων και των συστημάτων διαχείρισης εμπορευμάτων	Μεγάλα θαλάσσια λιμάνια	Γαλλία PCS	2024	Τριετές πρόγραμμα PIA	Πρόκειται να ξεκινήσει
			Συνέχιση της ανάπτυξης της ασφάλειας των ηλεκτρικών δικτύων των λιμένων	Μεγάλα θαλάσσια λιμάνια	Γαλλία PCS	2024	Τριετές πρόγραμμα PIA	Πρόκειται να ξεκινήσει
			Προώθηση της εφαρμογής λύσεων παρακολούθησης και ανίχνευσης περιστατικών ασφαλείας στα λιμενικά συστήματα	Μεγάλα θαλάσσια λιμάνια	France Cyber Maritime MICA	2024		Να ξεκινήσει

Παρουσίαση της στρατηγικής

Σχέδιο δράσης (δράσεις 3.1, 4.1 και 4.2)

Τομέας	Αριθμός δράσης	Δράση	Καθήκον(τα)	Υπεύθυνος	Συνεισφέροντες	Προθεσμία	Σχόλια	Πρόοδος
L3: ΥΠΕΡΑΣΠΙΣΗ ΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ	Δράση 3.1	Συνοδεία των φορέων του ναυτιλιακού τομέα στην εφαρμογή διαδικασιών παρακολούθησης, ανίχνευσης και αντίδρασης σε περιστατικά κυβερνοασφάλειας.	Προώθηση της αναφοράς περιστατικών στους των φορέων του ναυτιλιακού τομέα	France Cyber maritime	C2M2 MICA Center	Δεκέμβριος-2021	Υπάρχουν ήδη υποχρεώσεις αναφοράς (LPM, NIS). Το 2018, η DAM εξέδωσε έναν οδηγό που διανεμήθηκε σε όλους τους πλοιοκτήτες.	Προς έναρξη
			Ανάπτυξη και εφαρμογή μηχανισμών καταγραφής περιστατικών	France Cyber maritime	MICA Center ANSSI (CERT-FR)	Δεκέμβριος 2021		Να ξεκινήσει
			Δημιουργία ενός CERT Maritime	France Cyber Maritime	Κέντρο MICA ΝΑΥΤΙΚΗ ΑΣΤΥΝΟΜΙΑ ANSSI	Δεκέμβριος 2023		Να ξεκινήσει
L4: ΑΝΘΕΚΤΙΚΟΤΗΤΑ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ	Δράση 4.1	Οργάνωση της ανθεκτικότητας του τομέα	Εφαρμογή και δοκιμή διαδικασιών διαχείρισης κρίσεων.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Δεκέμβριος 2021	Καθορισμός στόχων, πεδίων εφαρμογής και αλληλεπιδράσεων με τα υπάρχοντα ασκήματα	Να ξεκινήσει
			Ανάπτυξη του συντονισμού μεταξύ των φορέων και ανάπτυξη της ανταλλαγής βέλτιστων πρακτικών.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Δεκέμβριος 2021		Να ξεκινήσει
	Δράση 4.2	Σε συνεργασία με τους τομείς της ναυτιλίας και των λιμένων, διοργάνωση ασκήσεων αντιμετώπισης κυβερνοκρίσεων	Καθιέρωση προγραμματισμού ασκήσεων για τους θαλάσσιους και λιμενικούς τομείς, σε συνάρτηση με τις μεγάλες εθνικές ασκήσεις.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Κάθε δύο χρόνια	Καθιέρωση προγράμματος ασκήσεων για τους θαλάσσιους και λιμενικούς τομείς.	Να ξεκινήσει
			Διανομή σε όλους τους ενδιαφερόμενους της ανάλυσης των συμπερασμάτων των ασκήσεων και των επακόλουθων ενεργειών.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Κάθε δύο χρόνια		Να ξεκινήσει

Μόνιμη στάση στον τομέα της κυβερνοασφάλειας

Αναγκαία αναδιοργάνωση

- Επιστροφή στα βασικά: ορθές πρακτικές

Προστασία: από το στάδιο του σχεδιασμού

- Αδιάβροχη σε όλες τις συνθήκες
- Ιχνηλασιμότητα και ακεραιότητα του παραδοθέντος κώδικα
- Χαρτογράφηση και έλεγχος ροών
- Πραγματισμός προς όφελος των δυνατοτήτων!

Άμυνα

- Δυναμική εποπτεία της ασφάλειας:
- αισθητήρες και κονσόλα

Συνέχεια της δραστηριότητας – ανθεκτικότητα

- PCA / PRA
- MCS και Σχέδια συνέχειας και ανάκαμψης μετά από συμβάν

Μόνιμη στάση στον τομέα της κυβερνοασφάλειας

Αύξηση της ισχύος

- Ποσοτική
- Ποιοτική
- Κοινή

Εκπαίδευση

- Ευαισθητοποίηση
- Πανεπιστημιακές εκπαιδεύσεις
- CYBERSECPRO

Εκπαιδεύσεις

- Ασκήσεις με θέμα την ασφάλεια
- Κανάλι εμπνευσμένο από την καταπολέμηση των καταστροφών
- Ενσωμάτωση στους δείκτες της εταιρείας

Παράδειγμα σχεδίου δράσης

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΣΧΕΔΙΟ ΔΡΑΣΗΣ

I	Ευαισθητοποίηση και εκπαίδευση	ΠΡΟΤΥΠΟ	ΕΝΙΣΧΥΜΕΝΟ
1	Εκπαίδευση των επιχειρησιακών ομάδων στην ασφάλεια των συστημάτων πληροφοριών		
2	Ευαισθητοποίηση των χρηστών σχετικά με τις βασικές ορθές πρακτικές ασφάλειας των πληροφοριών		
3	Διαχείριση των κινδύνων της διαχείρισης πληροφορικής		
II	Γνωρίστε το σύστημα πληροφοριών		
4	Προσδιορισμός των πιο ευαίσθητων πληροφοριών και διακομιστών και διατήρηση ενός διαγράμματος του δικτύου		
5	Διαθέτει έναν πλήρη κατάλογο των προνομιακών λογαριασμών και τον διατηρεί ενημερωμένο		
6	Οργανώστε τις διαδικασίες άφιξης, αναχώρησης και αλλαγής θέσης των χρηστών		
7	Επιτρέψτε τη σύνδεση στο δίκτυο της οντότητας μόνο σε ελεγχόμενο εξοπλισμό		
III	Αυθεντικοποίηση και έλεγχος πρόσβασης		
8	Ταυτοποίηση κάθε ατόμου που έχει πρόσβαση στο σύστημα και διάκριση των ρόλων χρήστη/διαχειριστή		
9	Ανάθεση των κατάλληλων δικαιωμάτων πρόσβασης σε ευαίσθητους πόρους του συστήματος πληροφοριών		
10	Ορίστε και ελέγξτε τους κανόνες επιλογής και μεγέθους των κωδικών πρόσβασης		
11	Προστασία των κωδικών πρόσβασης που είναι αποθηκευμένοι στα συστήματα		
12	Αλλαγή των προεπιλεγμένων στοιχείων πιστοποίησης σε εξοπλισμό και υπηρεσίες		
13	Προτιμήστε, όποτε είναι δυνατόν, την ισχυρή πιστοποίηση		

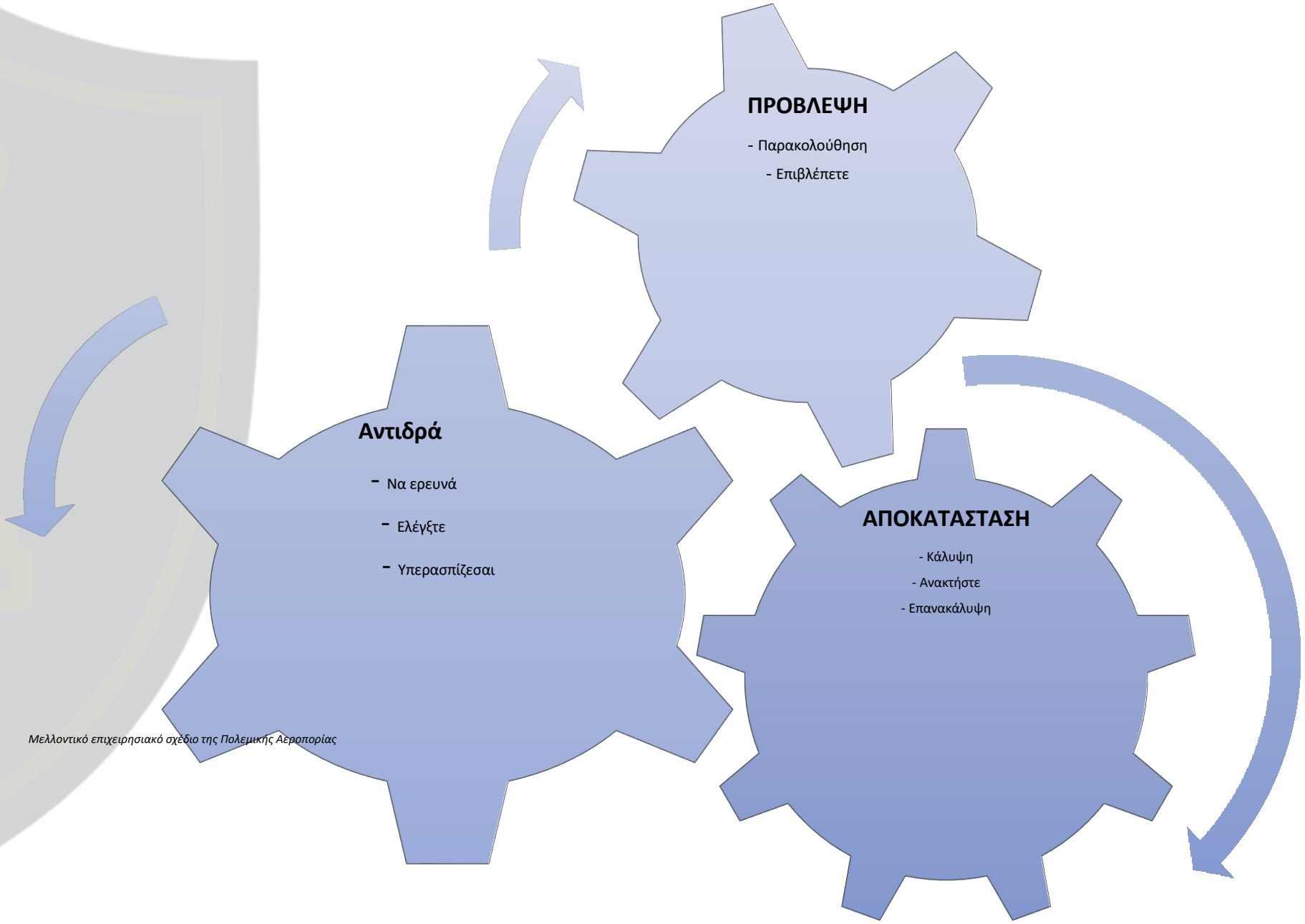
ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΣΧΕΔΙΟ ΔΡΑΣΗΣ

IV	Ασφάλεια των θέσεων εργασίας		
14	Εφαρμογή ενός ελάχιστου επιπέδου ασφάλειας σε όλο το δίκτυο υπολογιστών		
15	Προστασία από απειλές που σχετίζονται με τη χρήση αφαιρούμενων μέσων αποθήκευσης		
16	Χρήση ενός εργαλείου κεντρικής διαχείρισης για την ομογενοποίηση των πολιτικών ασφάλειας		
17	Ενεργοποίηση και διαμόρφωση του τοπικού τείχους προστασίας των σταθμών εργασίας		
18	Κρυπτογράφηση ευαίσθητων δεδομένων που μεταδίδονται μέσω του Διαδικτύου		
V	Ασφάλιση του δικτύου		
19	Τμηματοποίηση του δικτύου και δημιουργία διαχωριστικών μεταξύ των ζωνών		
20	Διασφάλιση της ασφάλειας των δικτύων Wi-Fi και του διαχωρισμού των χρήσεων		
21	Χρησιμοποιήστε ασφαλή πρωτόκολλα, εφόσον υπάρχουν.		
22	Εγκαταστήστε μια πύλη ασφαλούς πρόσβασης στο Διαδίκτυο.		
23	Διαχωρισμός των υπηρεσιών που είναι ορατές από το Διαδίκτυο από το υπόλοιπο σύστημα πληροφοριών		
24	Προστατέψτε την επαγγελματική σας αλληλογραφία		
25	Ασφάλιση των αποκλειστικών διασυνδέσεων δικτύου με τους συνεργάτες		
26	Έλεγχος και προστασία της πρόσβασης στους χώρους των διακομιστών και στα τεχνικά δωμάτια		

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΣΧΕΔΙΟ ΔΡΑΣΗΣ

VI	Ασφάλεια της διοίκησης		
27	Απαγόρευση της πρόσβασης στο Διαδίκτυο από τους σταθμούς εργασίας ή τους διακομιστές που χρησιμοποιούνται για τη διαχείριση του συστήματος πληροφοριών		
28	Χρήση ενός αποκλειστικού και διαχωρισμένου δικτύου για τη διαχείριση του συστήματος πληροφοριών		
29	Περιορίστε τα δικαιώματα διαχείρισης των σταθμών εργασίας στις απολύτως απαραίτητες λειτουργικές ανάγκες		
VII	Διαχείριση της κινητικότητας		
30	Λήψη μέτρων για τη φυσική ασφάλεια των κινητών τερματικών		
31	Κρυπτογράφηση ευαίσθητων δεδομένων, ιδίως σε εξοπλισμό που ενδέχεται να χαθεί		
32	Ασφάλιση της σύνδεσης δικτύου των τερματικών που χρησιμοποιούνται σε κινητές εφαρμογές		
33	Υιοθέτηση πολιτικών ασφάλειας ειδικά για κινητές συσκευές		
VIII	Διατήρηση του συστήματος πληροφοριών σε καλή κατάσταση		
34	Καθορισμός πολιτικής ενημέρωσης των στοιχείων του συστήματος πληροφοριών		
35	Προβλέψτε τη λήξη της συντήρησης του λογισμικού και των συστημάτων και περιορίστε τις προσκολλήσεις λογισμικού		
IX	Εποπτεία, έλεγχος, αντίδραση		
36	Ενεργοποίηση και διαμόρφωση των αρχείων καταγραφής των πιο σημαντικών στοιχείων		
37	Ορισμός και εφαρμογή πολιτικής δημιουργίας αντιγράφων ασφαλείας για κρίσιμα στοιχεία		
38	Διενέργεια τακτικών ελέγχων και επιθεωρήσεων ασφάλειας και εφαρμογή των σχετικών διορθωτικών μέτρων		
39	Ορίστε έναν υπεύθυνο για την ασφάλεια των συστημάτων πληροφοριών και ενημερώστε το προσωπικό σχετικά		
40	Καθορισμός διαδικασίας διαχείρισης περιστατικών ασφάλειας		
X	Για να προχωρήσετε περαιτέρω		
41	Διενέργεια επίσημης ανάλυσης κινδύνων		
42	Προτίμηση στη χρήση προϊόντων και υπηρεσιών που έχουν πιστοποιηθεί από την ANSSI		

ΑΠΟΣΤΟΛΕΣ – ΑΛΛΕΣ ΑΝΤΙΠΡΟΣΩΠΕΥΣΕΙΣ



Μελλοντικό επιχειρησιακό σχέδιο της Πολεμικής Αεροπορίας

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ - **PHISHING**

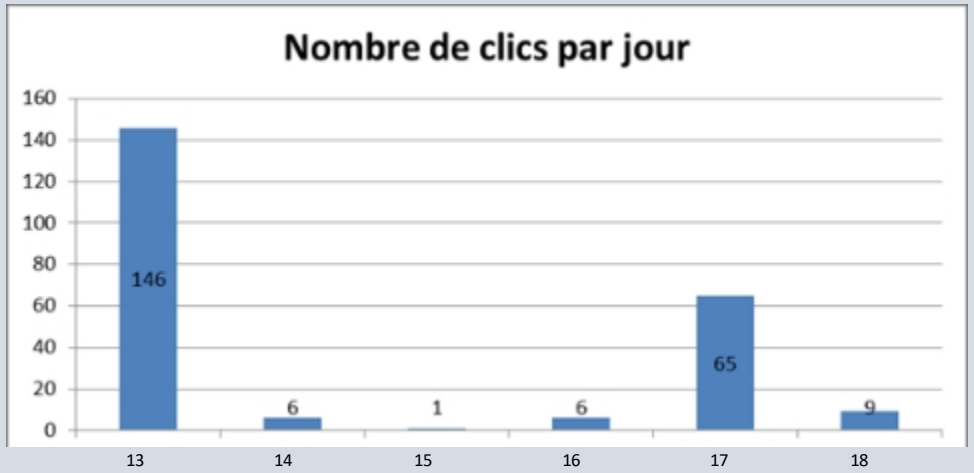
ΟΝΟΜΑ	**PHISHING – HAMECONNAGE**		
ΟΡΙΣΜΟΣ	Τεχνική που χρησιμοποιείται από απατεώνες απατεώνες για να προσωπικές προσωπικές πληροφορίες. Να κάνουν το θύμα να πιστέψει ότι επικοινωνεί με έναν αξιόπιστο τρίτο.	**ΣΤΟΧΟΣ**	Υποκρισία ταυτότητας.
		ΠΩΣ	Ηλεκτρονικό ταχυδρομείο.
ΠΩΣ **ΠΩΣ**	Για κάθε μήνυμα που λαμβάνετε,	➢ Μην ανοίγετε τα συνημμένα αρχεία ➢ Μην κάνετε ποτέ κλικ στους υπερσυνδέσμους ➢ Ελέγξτε τη διεύθυνση του αποστολέα ➢ Ελέγξτε την ώρα και την ημερομηνία αποστολής ➢ Ελέγξτε το θέμα του μηνύματος. ➢ Ελέγξτε ότι το μήνυμα δεν ζητά ασυνήθιστες/προσωπικές πληροφορίες ➢ Δώστε προσοχή στα μηνύματα προειδοποίησης που εμφανίζονται στο ηλεκτρονικό σας ταχυδρομείο	
ΣΕ ΠΕΡΙΠΤΩΣΗ ΑΜΦΙΒΟΛΙΑΣ	➢ Μην ανοίγετε τα συνημμένα αρχεία	➢ Μην κάνετε κλικ σε κανέναν από τους προτεινόμενους συνδέσμους	➢ Μην απαντήσετε στο μήνυμα
	Ειδοποιήστε τον RSSI		
ΣΥΓΚΕΚΡΙΜΕΝΗ ΠΕΡΙΠΤΩΣΗ	**ΑΣΚΗΣΗ PHISHING ΣΕ ΜΕΓΑΛΟ ΟΜΙΛΟ**		

Μια εκστρατεία phishing είχε ως στόχο 1000 υπαλλήλους του ομίλου.

Σε **6 ημέρες**, ο «κακόβουλος» διακομιστής συγκέντρωσε **233 κλικ**. **ΣΗΜΕΙΩΣΗ:** Στις 14 και 15 (Σαββατοκύριακο), 16 αργία.

Τελικά, **178 άτομα (18%) έκαναν κλικ** σε έναν από τους συνδέσμους του ηλεκτρονικού μηνύματος-παγίδα.

Σε περίπτωση πραγματικής επίθεσης, ένα μόνο κλικ θα μπορούσε να θέσει σε κίνδυνο ολόκληρη την εταιρεία.



Ευαισθητοποίηση **SSI - Ransomware Locky**

ΟΝΟΜΑ	**LOCKY**	**ΤΥΠΟΣ**	RANSOMWARE	**ΗΜΕΡΟΜΗΝΙΑ ΕΜΦΑΝΙΣΗΣ**	ΦΕΒ 2016
		ΣΥΣΤΗΜΑ ΠΟΥ ΕΠΗΡΕΑΖΕΤΑΙ	ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ WINDOWS	**ΤΟΠΟΘΕΣΙΑ**	ΕΥΡΩΠΗ

ΕΠΙΠΤΩΣΗ	ΟΜΗΡΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΣΑΣ ΔΕΔΟΜΕΝΩΝ ΜΕΣΩ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ	
ΣΤΟΧΟΣ	ΑΙΤΗΣΗ ΛΥΤΡΩΝ ΓΙΑ ΤΗΝ ΑΝΑΚΤΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ	
ΔΙΑΔΟΣΗ	ΔΙΑΔΙΔΕΤΑΙ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΑΠΟ **BOTNET** (Βλ. ορισμό)	
	ΜΕΣΩ ΜΗΧΑΝΗΜΑΤΟΣ	
ΜΕΘΟΔΟΣ ΕΠΙΘΕΣΗΣ	ΛΗΨΗ E-MAIL ΜΕ ΜΟΛΥΝΘΕΝ ΣΥΝΗΜΜΕΝΟ:	ΘΕΜΑ (προς το παρόν): ΠΡΟΣ: Τιμολόγιο J-XXXXXXX
		ΚΥΡΙΑ ΚΕΙΜΕΝΟΥ: ΣΩΣΤΗ ΣΥΝΤΑΞΗ, ΣΥΝΗΜΜΕΝΟ ΣΕ ΜΟΡΦΗ .DOC (ΣΥΝΗΘΩΣ, ΑΛΛΑ ΟΧΙ ΠΑΝΤΑ…)
		ΑΠΟΣΤΟΛΕΑΣ: ΠΟΤΕ Ο ΙΔΙΟΣ
	ΚΑΤΑ ΤΗΝ ΕΝΑΡΞΗ ΤΗΣ PJ, ΤΑ ΕΓΓΡΑΦΑ ΤΟΥ ΘΕΣΗΣ ΚΡΥΠΤΟΓΡΑΦΟΥΝΤΑΙ (ΜΟΡΦΗ .LOCKY)	
	ΤΟ ΣΗΜΕΙΩΜΑΤΑΡΙΟ ΑΝΟΙΓΕΙ ΚΑΙ ΕΜΦΑΝΙΖΕΙ ΜΙΑ ΑΙΤΗΣΗ ΛΥΤΡΟΥ	
	ΟΙ ΣΥΝΔΕΣΜΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΘΑ ΔΕΙΧΝΟΥΝ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΓΙΑ ΤΗΝ ΑΝΑΚΤΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΗ ΒΟΗΘΕΙΑ ΕΝΟΣ ΑΠΟΚΡΥΠΤΟΓΡΑΦΟΥ (ΟΝΟΜΑΖΟΜΕΝΟΥ LOCKY DECRYPTOR PRO, Η ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ ΟΠΟΙΟΥ ΔΕΝ ΕΧΕΙ ΑΠΟΔΕΙΧΘΕΙ)	
ΛΥΣΗ	**ΚΑΜΙΑ ΜΈΧΡΙ ΣΗΜΕΡΑ – ΠΛΉΡΗΣ ΑΠΩΛΕΙΑ ΤΩΝ ΔΕΔΟΜΈΝΩΝ**	
ΣΥΣΤΑΣΕΙΣ	ΜΗΝ ΠΛΗΡΩΝΕΤΕ ΤΟ ΛΥΤΡΑ ΣΤΟΥΣ ΚΛΕΦΤΕΣ ΕΠΕΙΔΗ:	Η ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΕΝ ΕΧΕΙ ΑΠΟΔΕΙΧΘΕΙ
		ΧΑΜΗΛΟΣ ΚΟΣΤΟΣ
		ΕΝΘΑΡΡΥΝΕΙ ΤΟΥΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΙΕΣ ΝΑ ΣΥΝΕΧΙΣΟΥΝ
ΤΡΕΧΟΥΣΑ ΠΡΟΛΗΠΤΙΚΗ ΜΕΤΡΑ	ΠΡΟΣΘΗΚΗ ΣΤΟ ΑΡΧΕΙΟ ΕΓΓΡΑΦΩΝ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ WINDOWS ΕΝΟΣ ΑΡΧΕΙΟΥ .LOCKY ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΤΡΟΠΟΠΟΙΗΣΗΣ ΑΥΤΗ Η ΜΕΘΟΔΟΣ, ΣΕ ΠΕΡΙΠΤΩΣΗ ΑΝΟΙΓΜΑΤΟΣ ΕΝΟΣ ΜΟΛΥΝΘΕΝΤΟΣ ΠΑΡΑΡΤΗΜΑΤΟΣ, ΕΜΠΟΔΙΖΕΙ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ LOCKY ΚΑΙ, ΣΥΝΕΠΩΣ, ΤΗΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ	

ΟΡΙΣΜΟΣ BOTNET	ΈΝΑ **BOTNET** (ΑΠΟ ΤΗΝ ΑΓΓΛΙΚΗ ΣΥΝΘΕΣΗ ΤΩΝ ΛΕΞΕΩΝ «ROBOT» ΚΑΙ «NETWORK») ΕΙΝΑΙ ΕΝΑ ΔΙΚΤΥΟ ΠΡΟΓΡΑΜΜΑΤΩΝ ΣΥΝΔΕΔΕΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΠΟΥ ΕΠΙΚΟΙΝΩΝΟΥΝ ΜΕ ΑΛΛΑ ΠΑΡΟΜΟΙΑ ΠΡΟΓΡΑΜΜΑΤΑ ΓΙΑ ΤΗΝ ΕΚΤΕΛΕΣΗ ΟΡΙΣΜΕΝΩΝ ΕΡΓΑΣΙΩΝ.

ΤΕΛΟΣ