Definizioni dei concetti di sicurezza e protezione

UE7- e A1 Sicurezza e protezione, due ambiti distinti ma di pari importanza

UE7 – D1 Le fasi dell'azione: anticipare e monitorare, reagire e combattere, ripristinare (Parte)

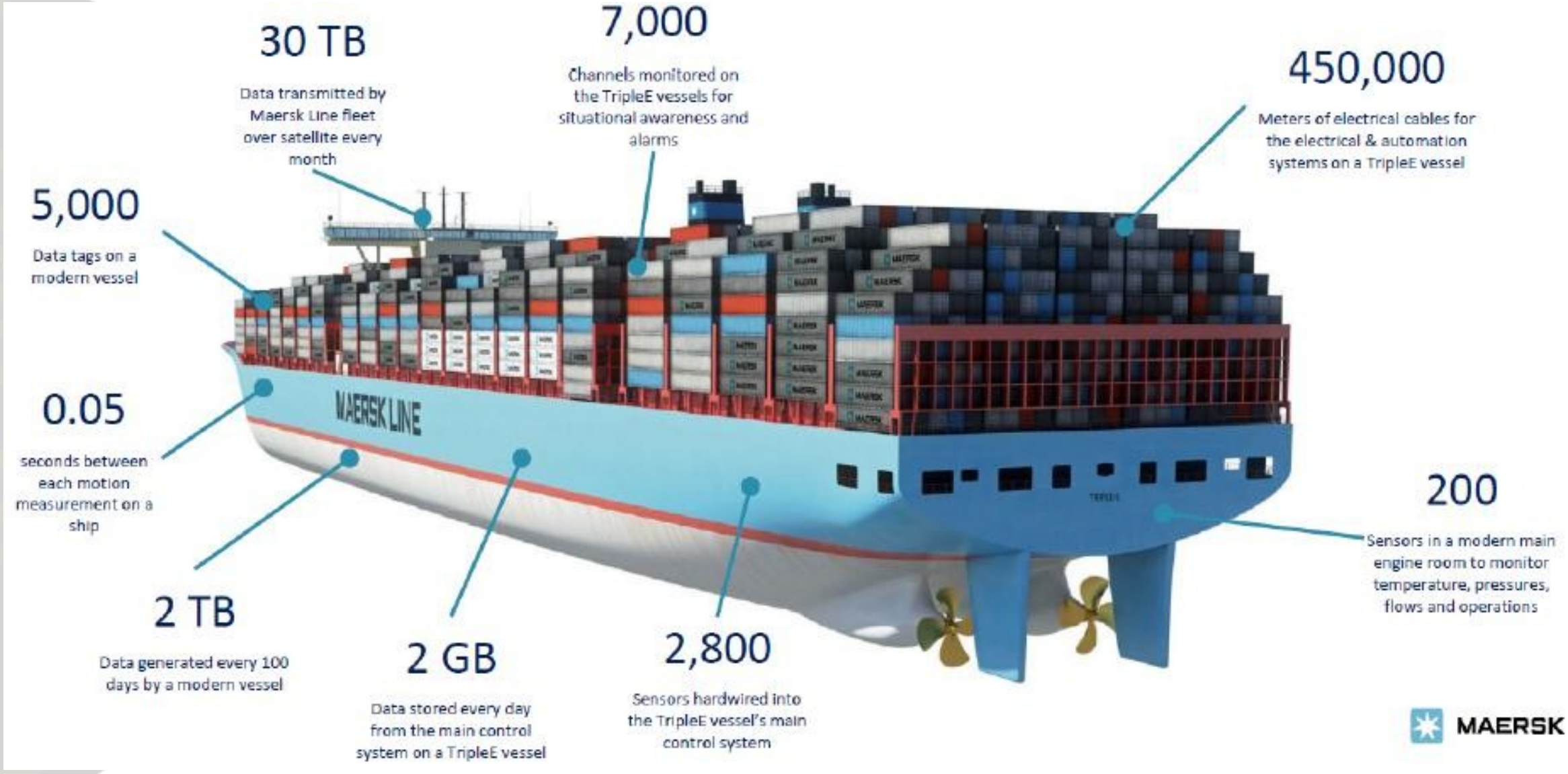
Sicurezza e protezione

SEMESTRE 10					
UE 7 - Attuare una politica di sicurezza informatica efficace		**BC 3**	**45**	*6*	**6**
UE7-A - Definizioni dei concetti di sicurezza e protezione			**15**	**2**	**2**
UE7-A-1	Sicurezza e protezione, due ambiti distinti ma di pari importanza				
UE7-A-2	Cybersicurezza: una visione condivisa tra utenti, progettisti di apparecchiature, reti di trasmissione, servizi di gestione dei dati				
UE7-C - Assicurare il rischio legato agli attacchi informatici			**15**	*2*	**2**
UE7-C-1	Identificare i settori funzionali, mapparli e garantirne l' interoperabilità sicura - Esigenze, constatazioni, analisi				
UE7-C-2	Assicurazione per coprire i costi causati dagli attacchi informatici ai sistemi informativi				
UE7-D - Organizzare i processi per garantire la sicurezza informatica dell'azienda e del suo ambiente			**15**	*2*	**2**
UE7-D-1	Le fasi dell'azione: anticipare e monitorare, reagire e combattere, ripristinare				
UE7-D-2	Gestire la comunicazione interna ed esterna verso i collaboratori, i fornitori, i clienti				

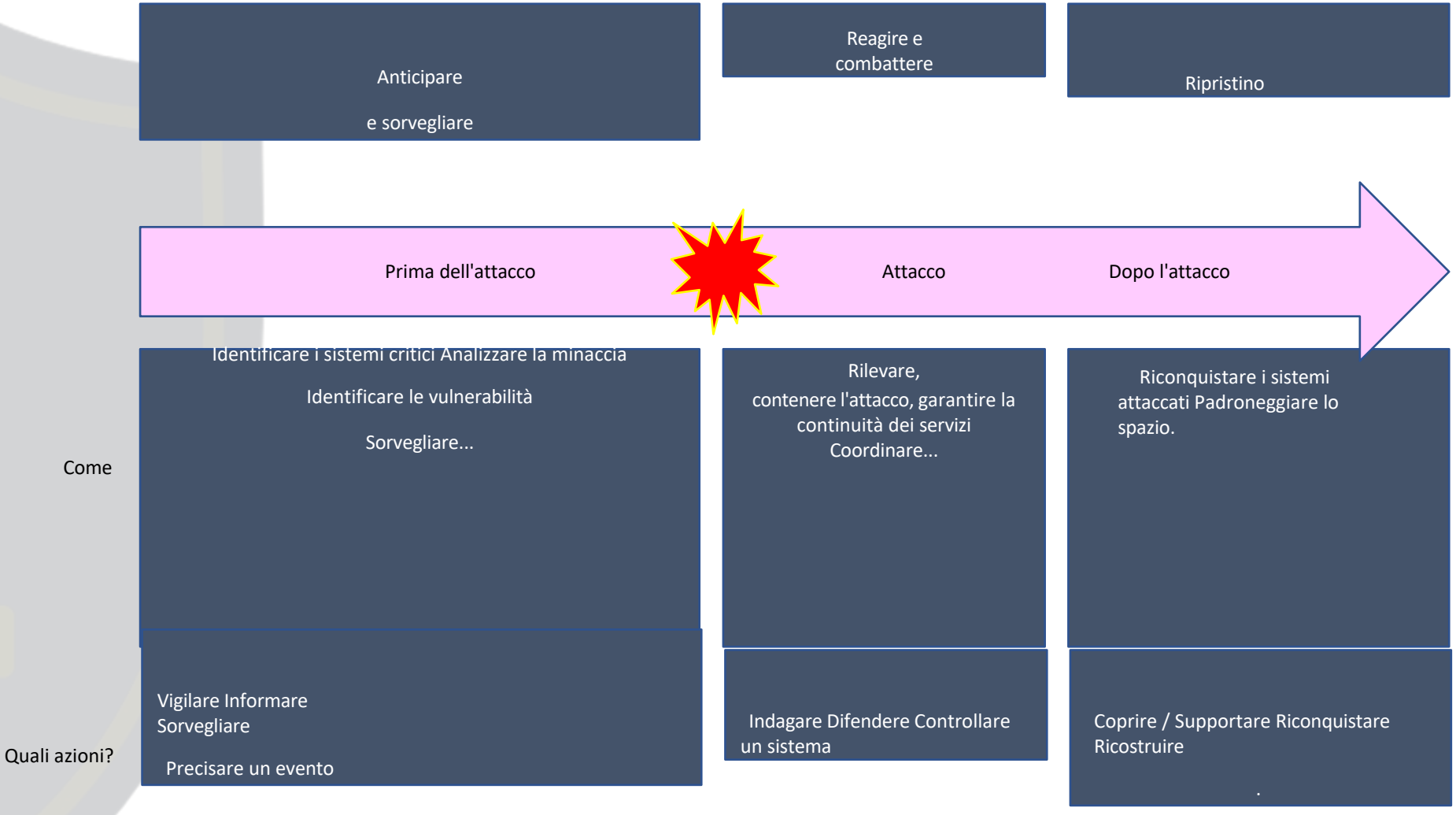
Definizioni dei concetti di sicurezza e protezione

Cybersicurezza - Garanzia delle informazioni

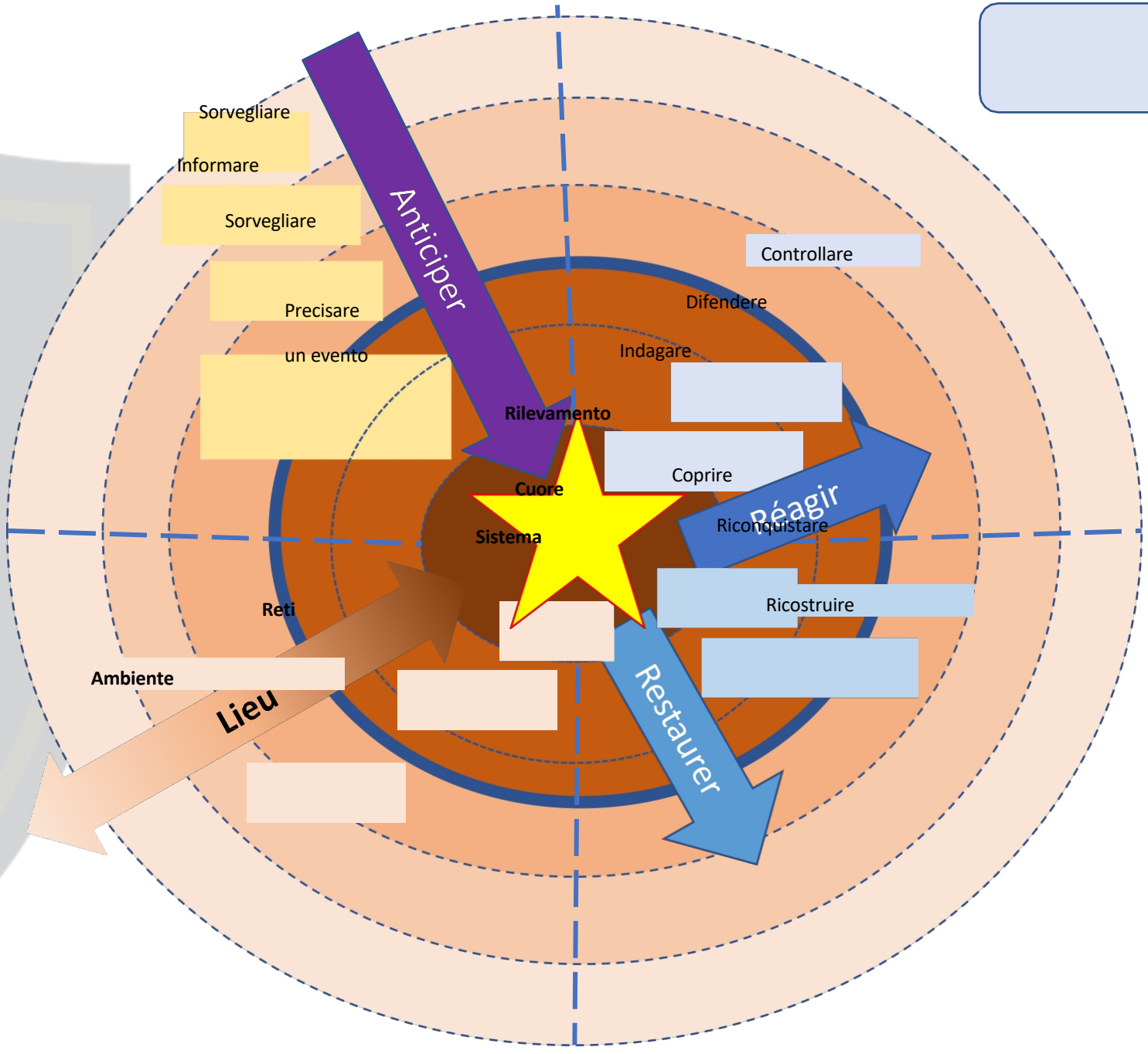
Confidentiality	Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information	KY
Integrity	The property whereby an entity has not been modified in an unauthorized manner.	ACCESS CTRL / RIGHT
Availability	Being accessible and useable upon demand by an authorized entity.	PCA/PRA
Non-Repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.	D.SIGN
Authentication	Verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.	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
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 LINE
MAERSK

Sicurezza – Protezione: le fasi della lotta



DIFENDERE IN PROFONDITÀ



Prevenzione: organizzare la sicurezza informatica

Governance

- Condivisione delle informazioni (ISAC)
- Regolamentazione
  - Navi (IMO)
  - Ecosistema portuale (NIS/LPM)
- Audit
- Notifica degli incidenti

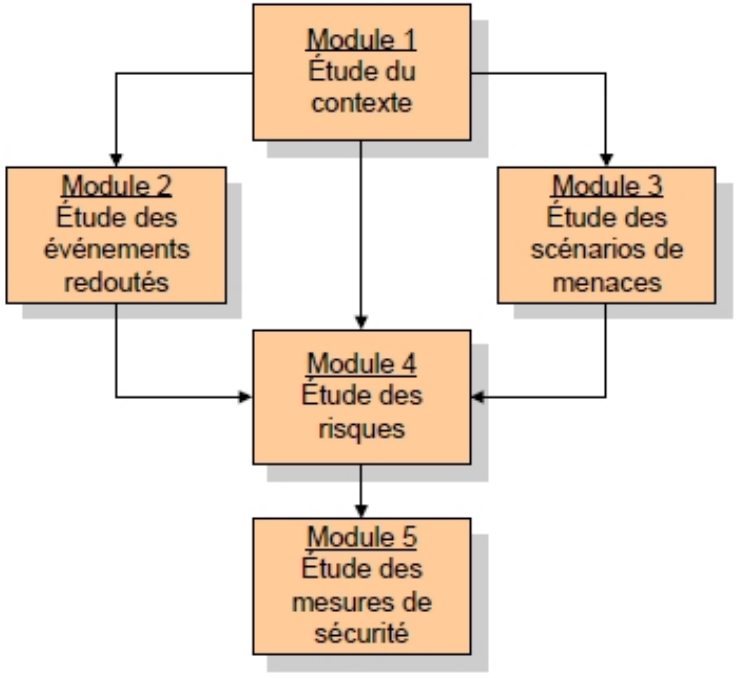
Protezione

- Sensibilizzazione e formazione
- Sicurezza fin dalla progettazione
- Valutazioni informatiche (BV, DNV-GL)
- Sicurezza della catena di approvvigionamento chain"

Difesa

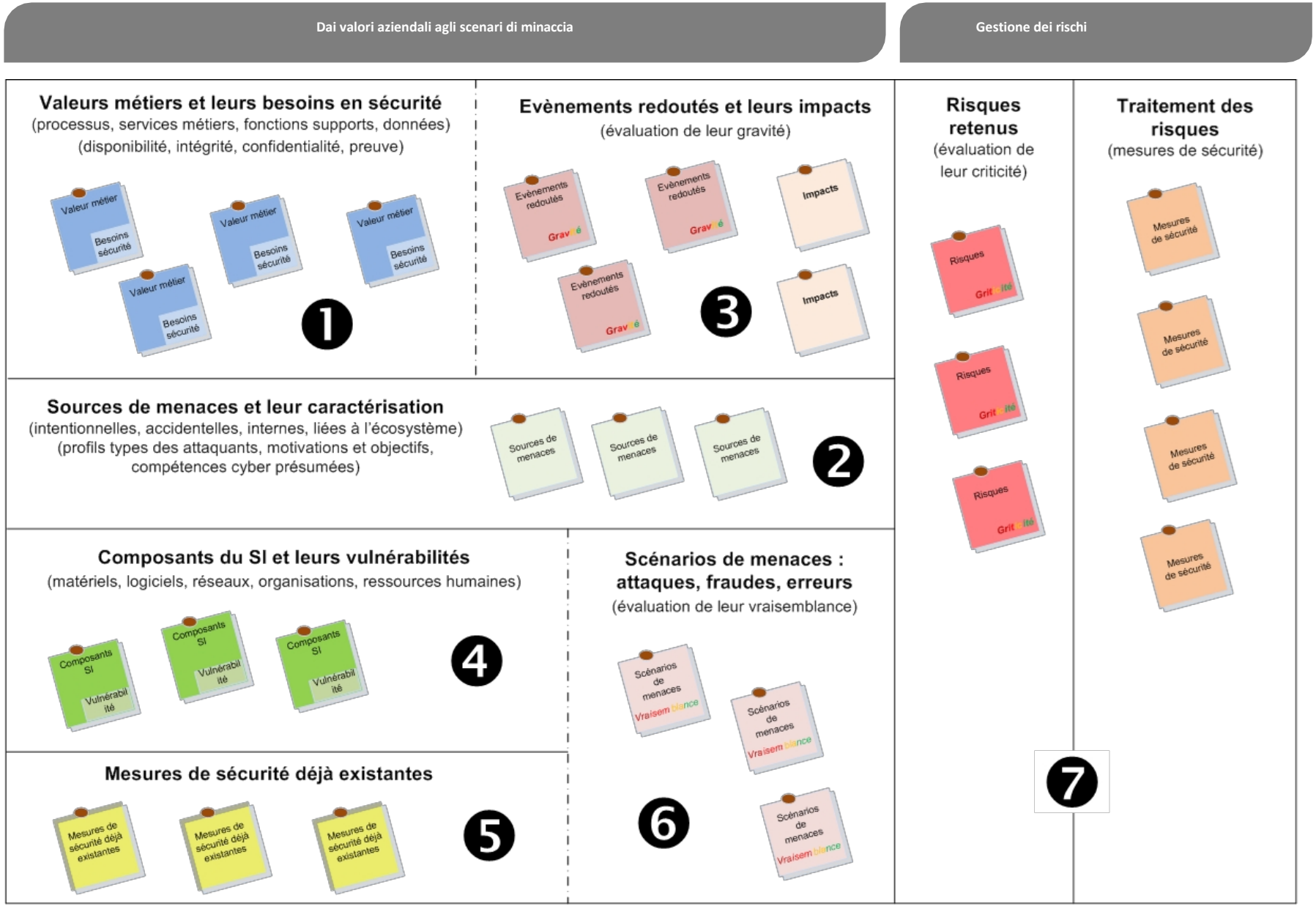
- M-CERT
- Gestione degli allarmi
- SOC Marittimo
- Piano di gestione delle crisi settoriale ed esercitazioni

Prevenzione: Documentare i rischi

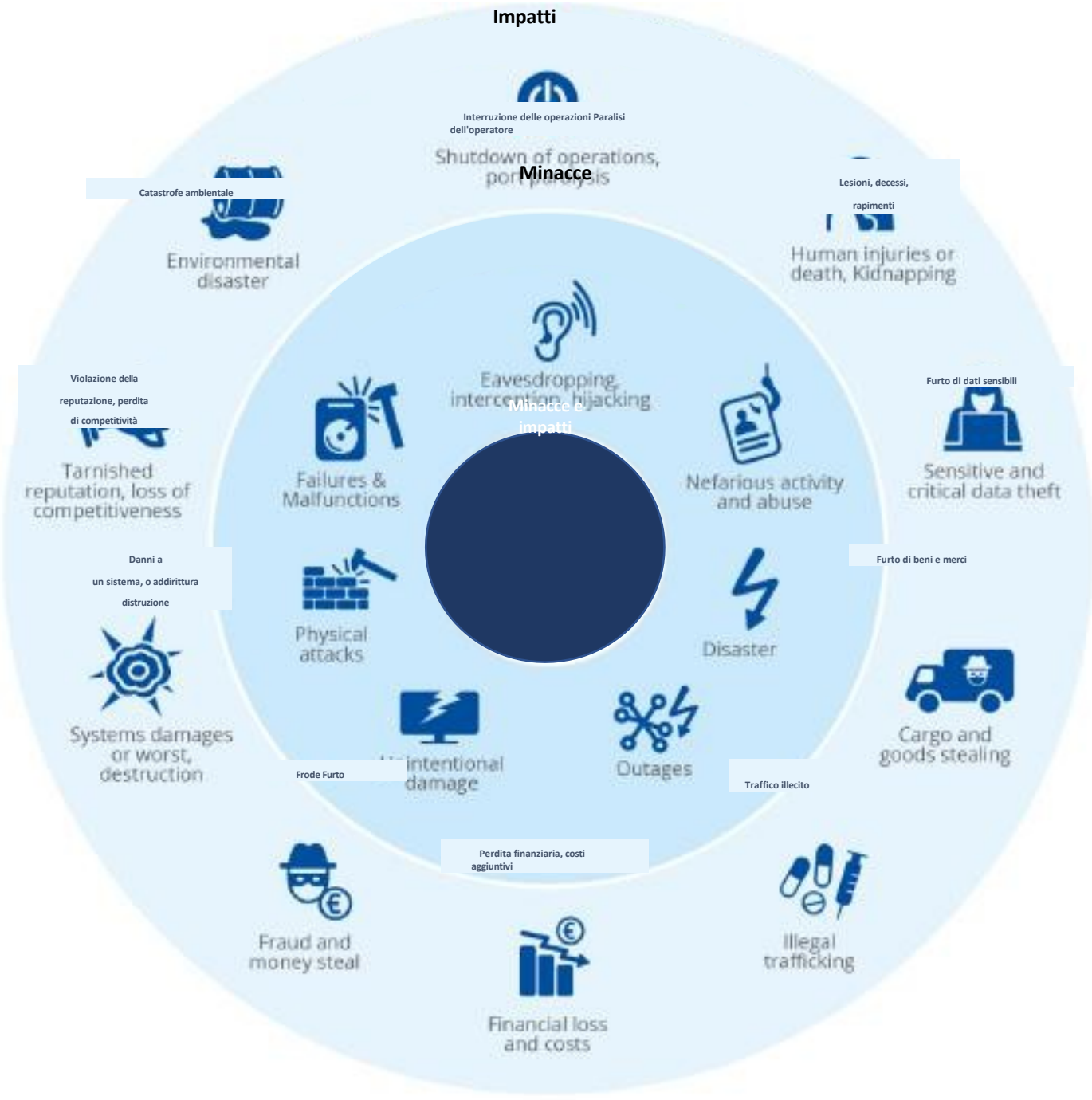


SABSA: Sherwood Applied Business Security Architecture **SSRS:** Dichiarazione dei requisiti di sicurezza specifici del sistema **SECOPS**: Procedure operative di sicurezza

Prevenzione: rischi e trattamento



Minacce / Impatti



Prevenzione: esempio

Analisi dell'impatto sul business (BIA)

Scenario di minaccia	Vulnerabilità	Classificazione
Corruzione dei dati, Abuso di diritti, Falsificazione di diritti, Negazione di azioni	Password di accesso deboli	Alta
Spionaggio "Intercettazioni"	Password di accesso cambiata raramente	Molto Alta

SSRS

Gestione delle password

sistema

Implementazione SSRS

Il sistema di gestione utenti XXX Network impone la creazione di password di adeguata complessità:

Piano di implementazione

Sviluppare una politica relativa alle password. Da trattare nell'ambito di SSRS e SecOPs.

SECopS

Gestione degli accessi

Implementazione SecOPs

Il sistema di gestione utenti della rete XXX richiede password di

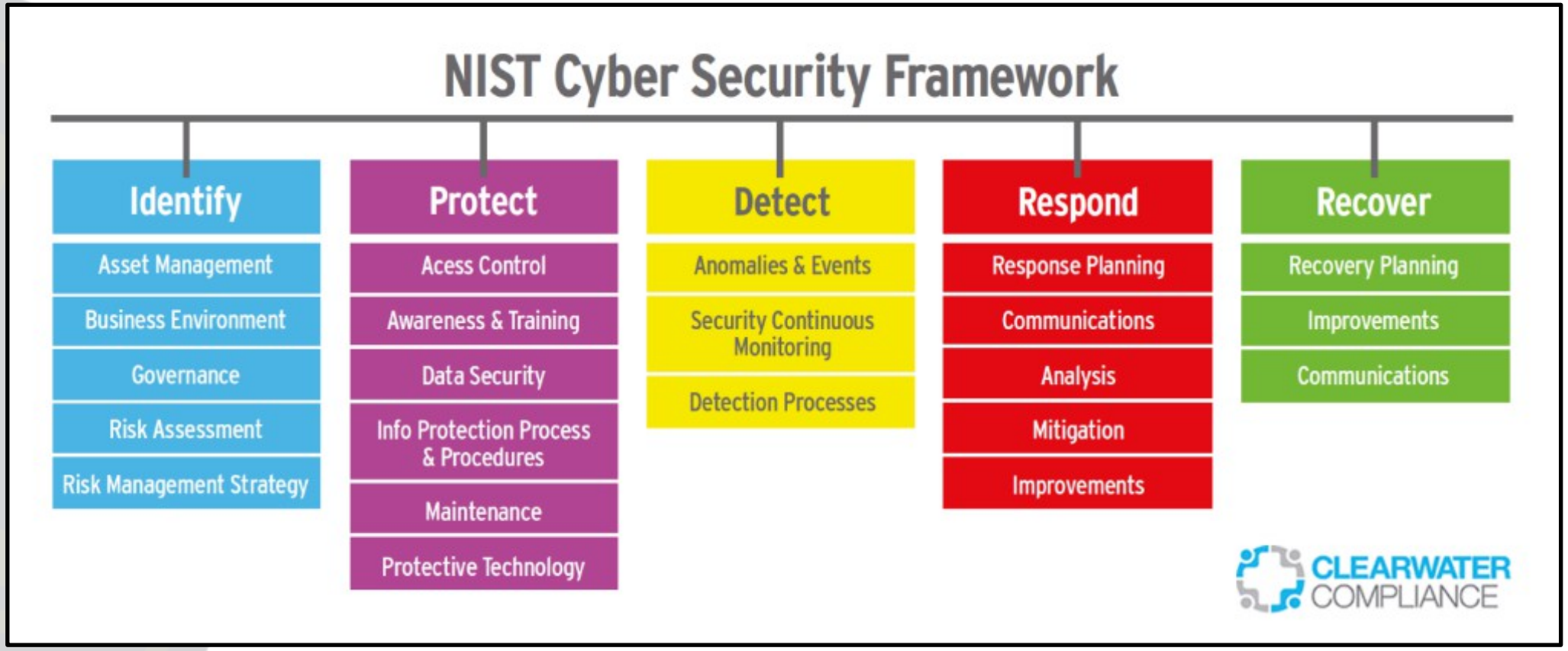
adeguata complessità:

- almeno 10 caratteri;
- Password amministratore: almeno 12 caratteri;
- Deve rispettare 3 dei 4 gruppi di caratteri:
  - almeno una lettera minuscola (da a a z);
  - almeno una lettera maiuscola (da A a Z);
  - almeno una cifra (da 0 a 9) o almeno un carattere speciale

    (ad es.! @ # $% & *, ecc.);
- Cambia ogni 90 giorni.

La password di un nuovo utente o amministratore deve essere diversa dalle ultime 20 password utilizzate.

prevenzione/Azione

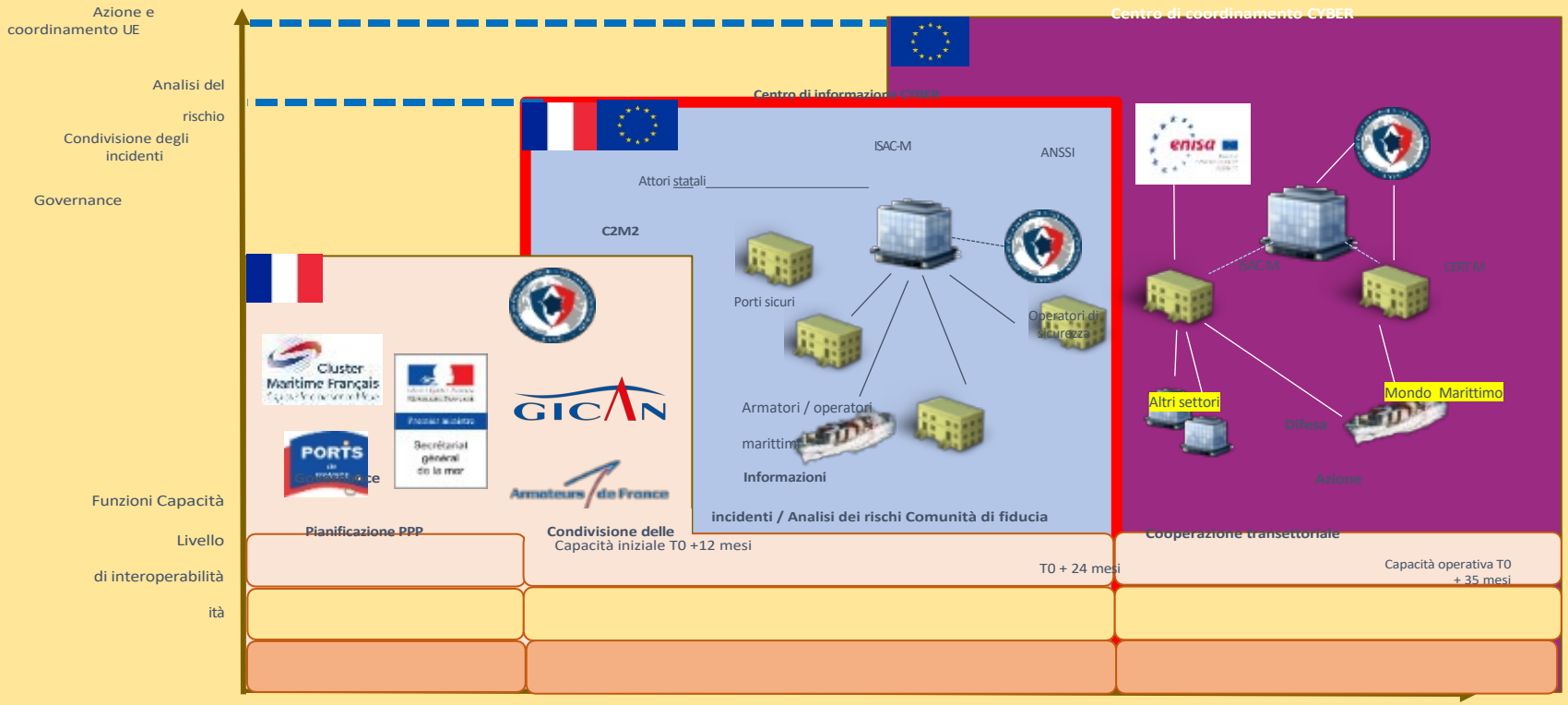


Sicurezza

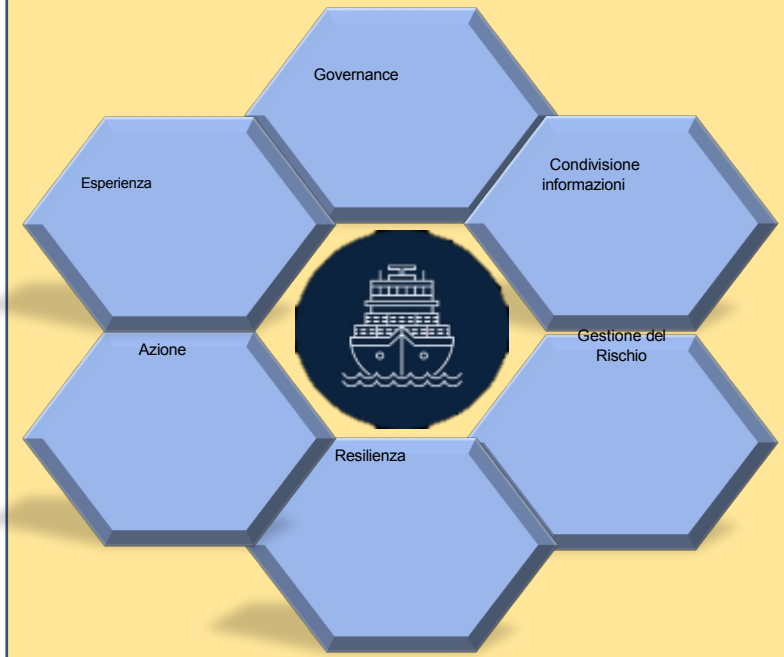
Sicurezza

L'iniziativa avviata dal Comitato France Maritime (2018)

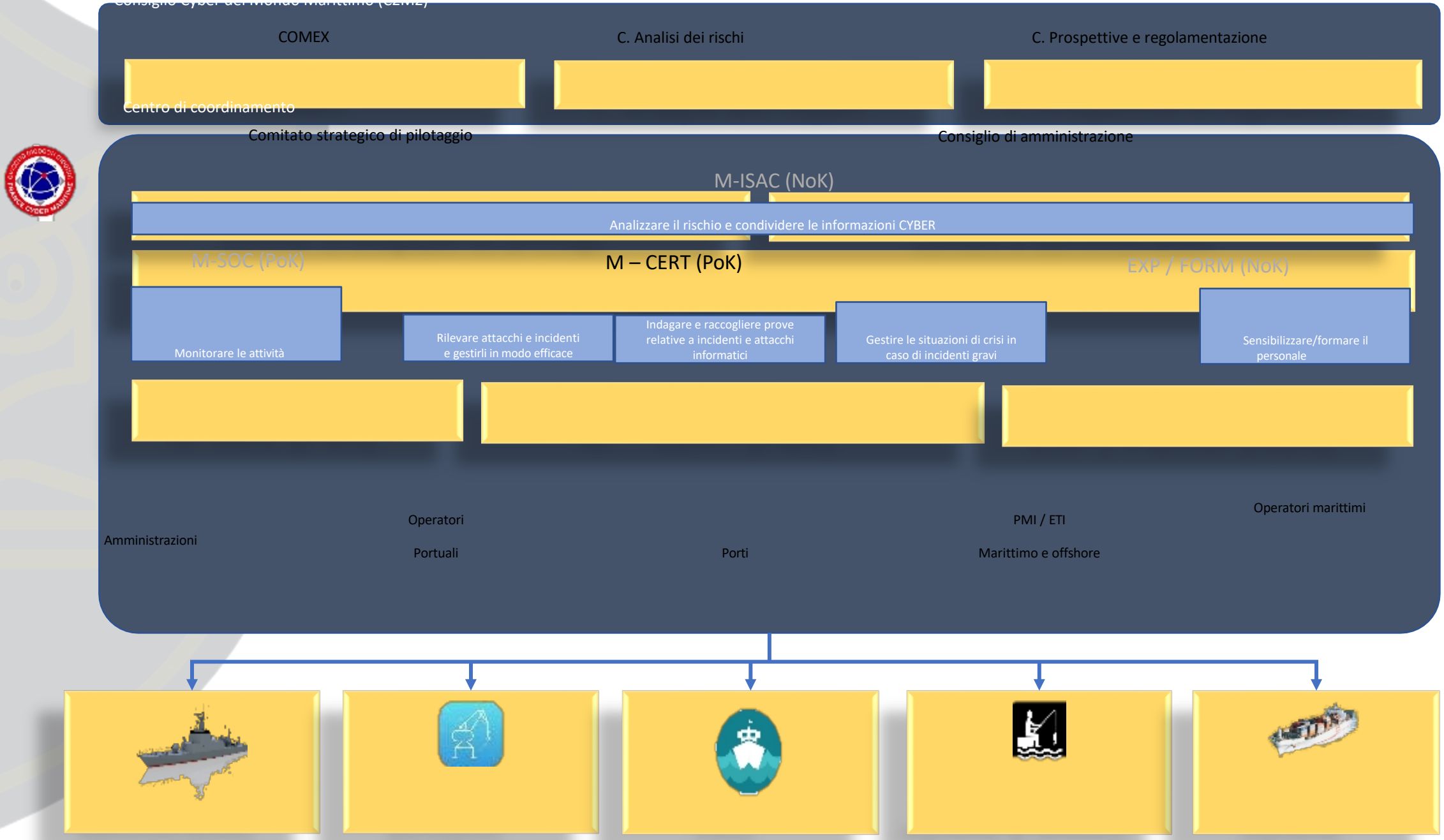
3 FASI



6 LINEE GUIDA



Governance informatica nel settore marittimo: a che punto siamo?



CERT / C-SIRT

Missioni

PREVENZIONE E THREAT INTEL (monitoraggio, sorveglianza e allerte)

- Analisi delle minacce e condivisione delle informazioni
- Avvisi di sicurezza e informazioni informatiche
- Riferimento agli indicatori di compromissione e alle firme
- Pubblicazione di allerte
- Prevenzione, formazione, addestramento.

GESTIONE E COORDINAMENTO DEGLI INCIDENTI

Gestione tecnica e organizzativa degli incidenti.

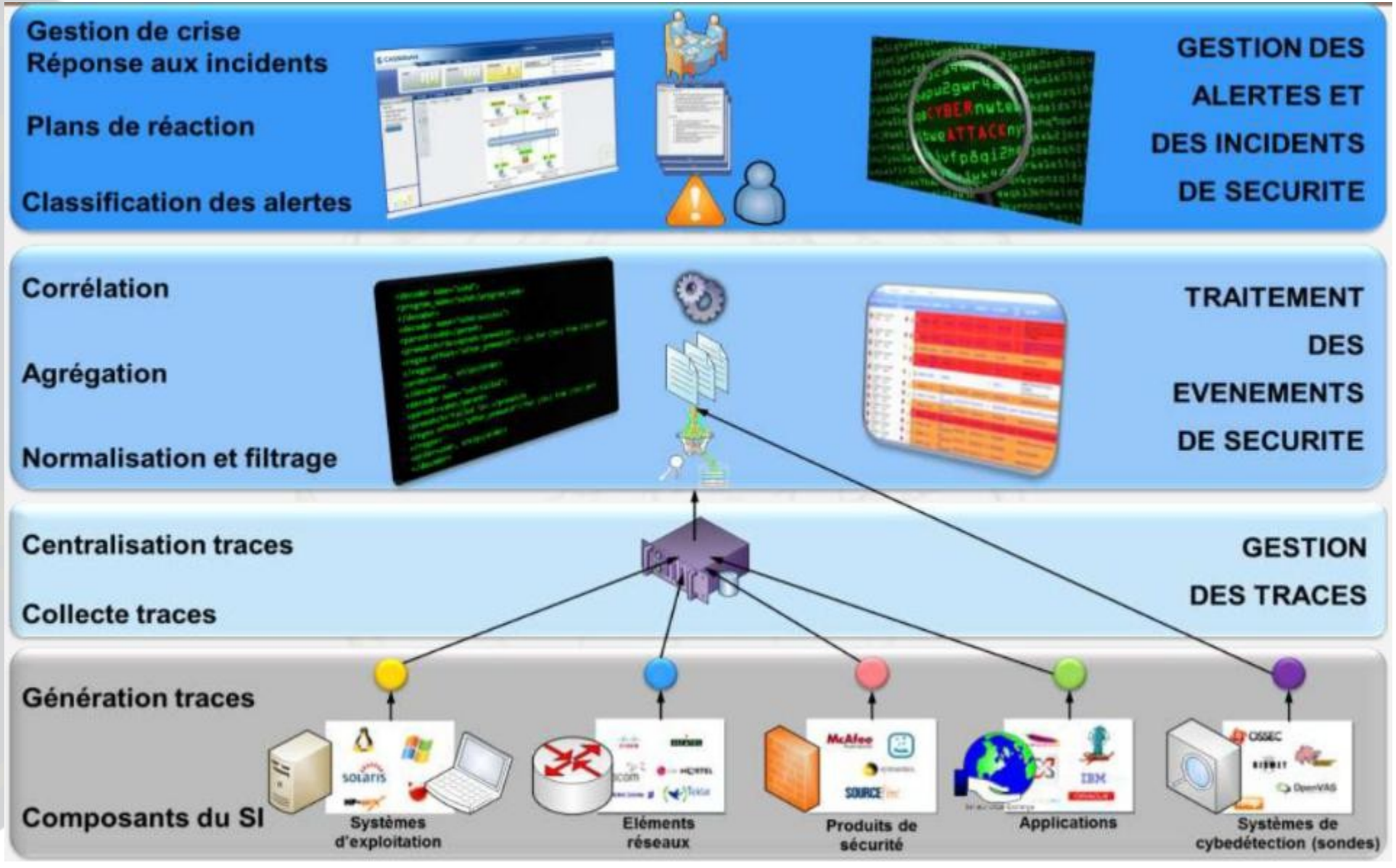
TRIAGE

- Raccolta di informazioni sugli incidenti,
- Associazione Incidente / membri del CERT
- Valutazione della gravità dell'incidente

COORDINAMENTO

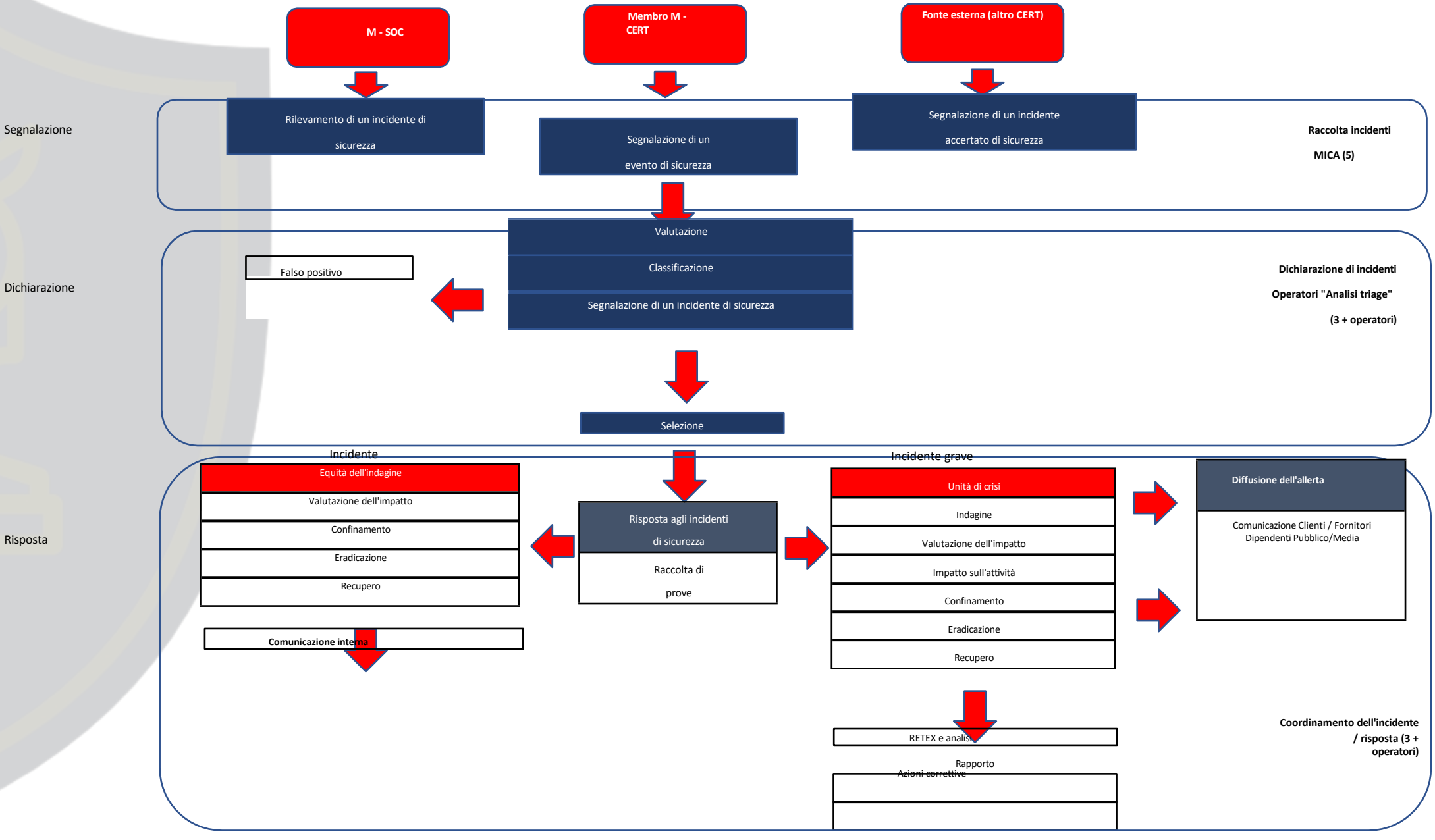
Coordinamento (ente segnalante, partner coinvolti nella risoluzione dell'incidente). Contenimento

Organizzazione tecnica di un CERT



Funzionamento di un CERT marittimo

Organigramma di gestione degli incidenti



Rischi e capacità

Sei tipi di minacce

Malware: software dannoso la cui diffusione è incontrollabile

Script kiddy (adolescente disoccupato o, più in generale, aggressore solitario e opportunista):

- Mezzi molto limitati (< 100 €)
- Il gioco (ed eventualmente il profitto) come motivazione
- Attacco opportunistico

Dipendente malintenzionato (rancore / avidità):

- Mezzi modesti (< 1.000 €)
- Motivazione principale: danneggiare il proprio datore di lavoro, evitando le vittime
- Discrezione quando possibile
- Facile accesso a tutte le parti della nave

Gruppo terroristico:

- Mezzi moderati (da 10 a 50.000 €)
- Ricerca di vittime umane, danni materiali, forte visibilità mediatica

Impresa criminale:

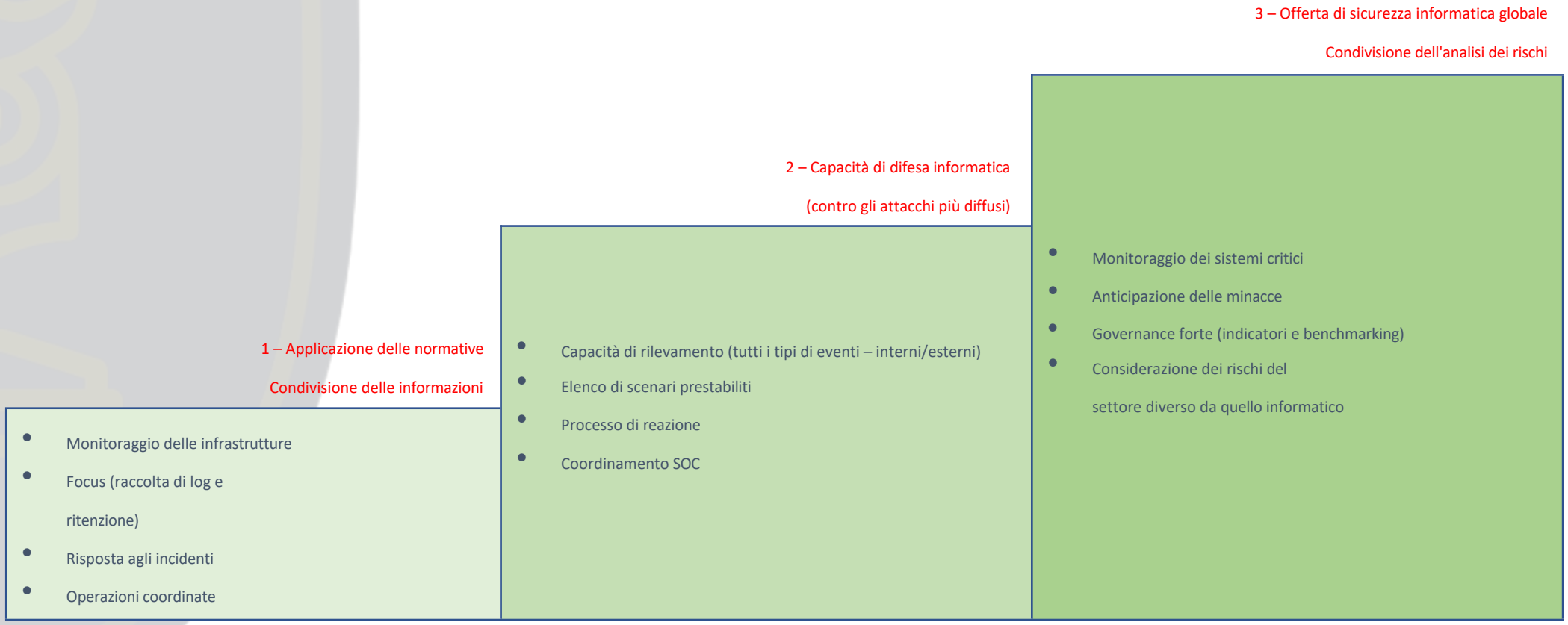
- Risorse elevate (dell'ordine di milioni di euro)
- Obiettivo di redditività
- Vincoli morali limitati
- Ricerca della discrezione

Stato:

- Risorse quasi illimitate
- Obiettivi di ogni tipo
- Assenza di vincoli morali
- Discrezione necessaria

Rilevare gli incidenti

SIEM



SIEM = SIM + SEM (Incidente + Evento)

Rif.: ETSI GS ISI 004 V1.1.1 (2013-12) - Indicatori di sicurezza delle informazioni (ISI); Linee guida per l'implementazione del rilevamento degli eventi

ETSI GS ISI 003 V1.1.2 (2014-06) - Indicatori di sicurezza delle informazioni (ISI); Indicatori chiave di prestazione della sicurezza (KPSI)

RISCHI

Scenari Nave civile

Attacco generalizzato tramite compromissione di un operatore satellitare Spionaggio

Scatenamento deliberato di una crisi di panico Saturazione delle reti

Modifica delle carte nautiche (compromissione di un editore)

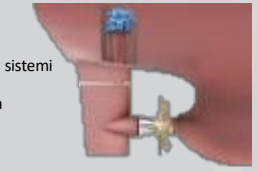
Compromissione del sistema informativo dell'armatore da una nave

Modifica dei riferimenti cartografici

Falso segnale GPS/radar

Paralisi dei sistemi

di manovra



Falsi allarmi incendio

Paralisi della nave (ransomware)

Blackout energetico

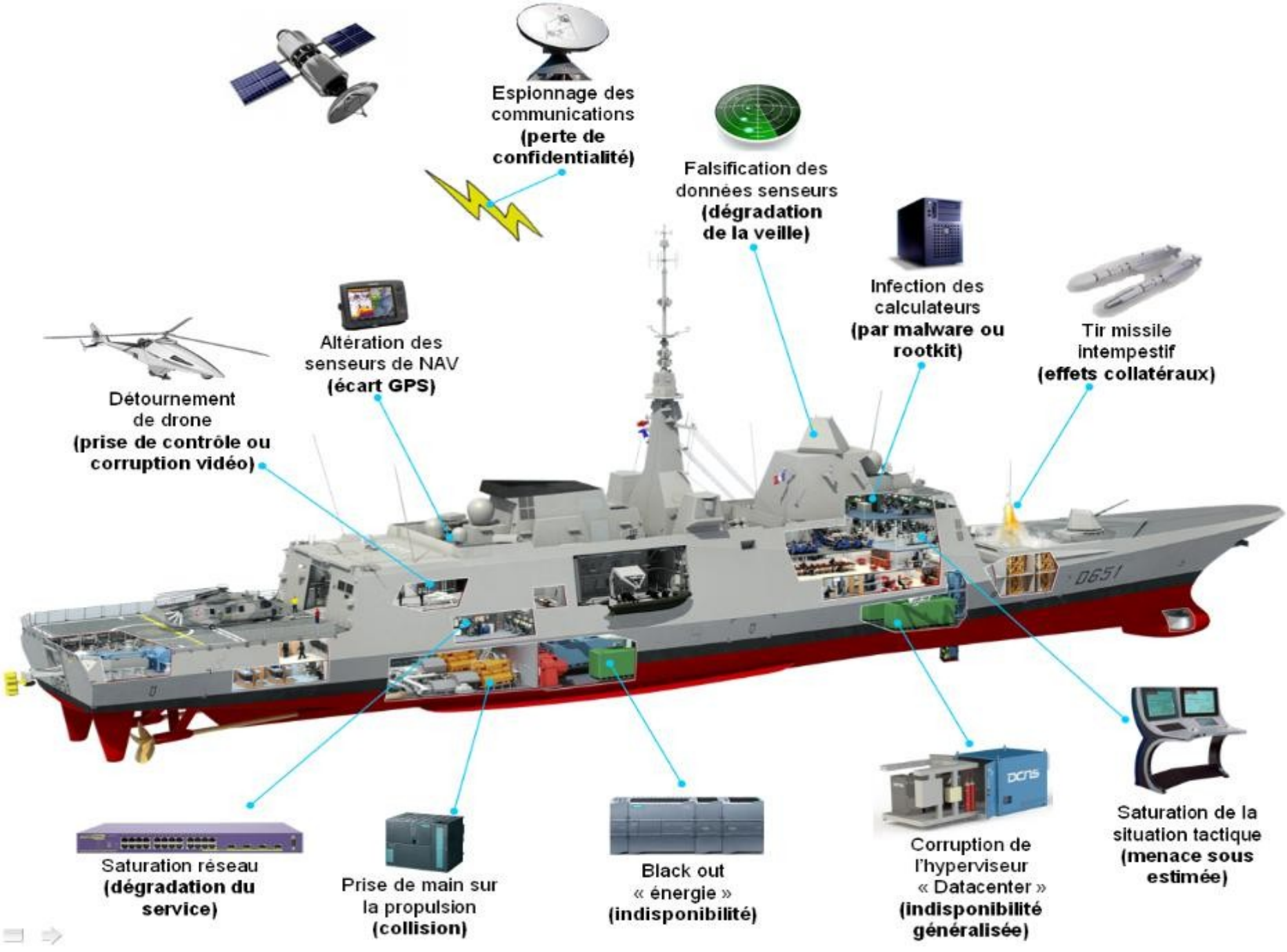
Sabotaggio di una nave / flotta (attacco mirato)

Compromissione della stabilità della nave

Rischio specifico di ciascun ambiente / sistema

RISCHI

Scenari Nave militare



STRATEGIE


ROYAUME DU MAROC
ADMINISTRATION DE
LA DEFENSE NATIONALE
LA STRATÉGIE NATIONALE
DE CYBERSÉCURITÉ
2030
DIRECTION GÉNÉRALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION


PREMIER
MINISTRE
Liberté
Égalité
Fraternité
STRATEGIE DE CYBERSECURITE
DES SECTEURS MARITIME ET PORTUAIRE
Lors du CIMER 2018, la France a décidé de mettre en avant les enjeux liés à la cybersécurité dans le domaine maritime, à la fois en termes de protection et en termes de développements économiques, en décidant la création d'un centre national de coordination de la cybersécurité où elle s'affirmera comme puissance maritime et comme nation en pointe dans le domaine de la cybersécurité.

Presentazione della strategia

Linee strategiche

LE GRANDI LINEE STRATEGICHE

Trasposizione al settore marittimo e portuale dei grandi principi della sicurezza informatica che sono stati definiti a livello transettoriale dalla LPM e dalla direttiva NIS su:

- ***La governance (politica generale di sicurezza informatica)***
- ***La protezione delle reti e dei sistemi informativi***
- ***La difesa delle reti e dei sistemi informativi***
- ***La resilienza delle attività***

Definizione di azioni e compiti

Tabella di monitoraggio delle azioni/indicatori

Presentazione della strategia

Piano d'azione (da 1.1 a 1.7)

Settore	N. Azione	Azione	Compito/i	Responsabile	Collaboratori	Scadenza	Commenti	Avanzamento ment
L1: GOVERNANCE	Azione 1.1	Implementare e promuovere la governance della sicurezza informatica marittima	Sviluppare e animare il consiglio per la sicurezza informatica del settore marittimo istituito nel 2019	Segreteria del C2M2	Comitati del C2M2	2019		Realizzato
			Creare e mantenere un quadro di monitoraggio delle azioni e dei relativi responsabili	Segreteria del C2M2	Comitati del C2M2	settembre 2021	Questatabella di marcia sarà rivista ogni riunione del COMEX	Da avviare
	Azione 1.2	Stabilire e mantenere una mappatura dei rischi del settore marittimo	Creare una mappa dei sistemi informativi utilizzati nel settore marittimo e portuale, preliminare alla mappatura dei rischi;	Comitato analisi delle rischi C2M2	Tutti gli attori rilevanti del mondo marittimo	Gennaio 2022	Definizione dell'ambito e approfondimento dell'analisi; condivisione delle informazioni.	avviata
			Produrre e aggiornare la mappatura dei rischi informatici del mondo marittimo.	Comitato di analisi dei rischi C2M2	Tutti gli attori del mondo marittimo	giugno 2022		Da avviare
	Azione 1.3	Mettere in atto e applicare per il settore marittimo delle indicatori nazionali di sicurezza informatica per il monitoraggio delle politiche e la valutazione della loro efficacia.	Sviluppare indicatori per il monitoraggio delle azioni del presente strategia	Comitati del C2M2	Comitati del C2M2	aprile 2022	Aggiungere una colonna di indicatori alla presente tabella	Da avviare
			Aggiornare il quadro di controllo dell'andamento degli indicatori	Comitati del C2M2	Comitati del C2M2	aprile 2022	Azione permanente	Da avviare
			Effettuare una revisione annuale degli indicatori ed esaminare le azioni da intraprendere di conseguenza	COMEX del C2M2	Comitati del C2M2	aprile 2022	Riunione del COMEX	Da avviare
	Azione 1.4	Coordinare le posizioni e l'azione della Francia presso dei suoi partner internazionali	Contribuire alla redazione di comunicazioni e proposte all'OMI	DGITM/DAM (navi) DGITM/DST (porti)	C2M2	Azione permanente	Il C2M2 coordina, ma il La convalida è interministeriale e RP presso l'OMI.	lanciato
			Contribuire ai lavori europei attraverso i gruppi di lavoro della CE (ad es. MARSEC, NIS Cooperation group, ECGFF Cybersecurity WG)	Comitati C2M2	SGMER, MIMER, MTE, ANSSI, Comitato Francia Marittima	Azione permanente		avviato
	Azione 1.5	Attuare azioni di sensibilizzazione alla sicurezza informatica e creare un quadro di formazione rivolto a tutti gli professioni del settore marittimo	Identificare le offerte esistenti e proporle al settore marittima (FR, UE)	France Cyber Marittimo	C2M2 DGITM/DAM (navi) DGITM/DST (porti)	marzo 2022	Aggiornare le guide delle buone pratiche pratiche esistenti	Da avviare
			Sviluppare una piattaforma di sensibilizzazione CYBER marittimo in relazione alle iniziative nazionali e esistenti	France Cyber Marittimo	C2M2 DGITM/DAM (navi) DGITM/DST (porti)	giugno 2022	In collaborazione con Cybermalveillance.gouv.fr	Da lanciare
	Azione 1.6	Organizzare e controllare il Condivisione di informazioni per tutti gli attori	Pubblicare una newsletter C2M2 cyber all'anno (generalità e attualità internazionale, progetti)	Segreteria del C2M2	Comitati C2M2	Trimestrale	Lanciato nel 2018; formalizzare il ambito di applicazione della presente lettera con FCM	Realizzato
			Sviluppare e pubblicare bollettini tecnici	France Cyber Marittimo	ANSSI (CERT-FR)		Secondo il programma da definire da France Cyber Maritime	Da avviare

Presentazione della strategia

Piano d'azione (2.1-2.4)

Settore	N. Azione	Azione	Compito/i	Responsabile	Collaboratori	Scadenza	Commenti	Avanzamento ment
L2: PROTEZIONE DELLE RETI E DEI SISTEMI INFORMATIVI	Azione 2.1	Analizzare le esigenze di evoluzioni legislative e regolamentari applicabili al settore marittimo	Trarre le conclusioni dall'analisi dei rischi, compresi i feedback sugli incidenti di sicurezza, al fine di definire le esigenze di evoluzione.	Comitato Prospettive e regolamentazione C2M2	France Cyber Maritime, Comitato Analisi dei rischi	Azione permanente		Da avviare
			Garantire il monitoraggio dell'evoluzione dei testi internazionali e delle norme che potrebbero giustificare una modifica dei testi nazionali	Comitato Prospettive e regolamentazione C2M2	DGITM/DAM (navi) DGITM/DST (porti) ANSSI	Azione permanente		avviata
	Azione 2.2	Contribuire a creare un quadro di certificazione/etichettatura dei prodotti e dei servizi che risponda alle esigenze del settore marittimo	Sostenere un approccio di certificazione/etichettatura dinanzi all'OMI in collaborazione con le amministrazioni e gli uffici di classificazione sulla base dei lavori esistente	MIMER / DAM	DGITM/DAM (navi) DGITM/DST (porti) ANSSI	2024	Annotare le azioni intraprese durante l'anno	Da avviare
	Azione 2.3	Definire un quadro di riferimento per la sistematica integrazione della sicurezza informatica nei progetti di progettazione e costruzione di navi e infrastrutture portuali	Sviluppare la "cybersecurity by design" presso gli attori industriali	Comitato Prospettive e regolamentazione C2M2	GICAN ANSSI	Azione permanente	Annotare le azioni intraprese durante l'anno	Da avviare
			Integrare la sicurezza informatica nelle riflessioni sullo sviluppo delle navi autonome	Comitato Prospettiva e regolamentazione C2M2	DGITM / DAM CLUSTER MARITIME ANSSI	Azione permanente	Sono in corso riflessioni presso l'OMI nei gruppi che lavorano sulle navi autonome;	Da avviare
	Azione 2.4	Condurre progetti specifici per la messa in sicurezza dei sistemi essenziali	Integrare i rischi di interferenza e disturbo del GNSS e le loro conseguenze su sistemi quali l'AIS o informazioni PNT	Comitato analisi dei rischi C2M2	DGITM CNES ANFR	settembre 2022	GT interministeriale - Interferenze AIS / GNSS	avviato
			Continuare a garantire la sicurezza dei sistemi di navigazione	Comitato analisi dei rischi C2M2	CNES CCTA	2024		Da avviare
			Contribuire a rendere più sicuri i sistemi portuali e di gestione delle merci	Grandi porti marittimi	Francia PCS	2024	Progetto PIA triennale	Da avviare
			Continuare a sviluppare la sicurezza delle reti elettriche dei porti	Grandi porti marittimi	Francia PCS	2024	Progetto PIA su 3 anni	Da avviare
			Promuovere l'implementazione di soluzioni di monitoraggio e rilevamento degli incidenti di sicurezza sui sistemi portuali	Grandi porti marittimi	Francia Cyber Maritime MICA	2024		Da avviare

Presentazione della strategia

Piano d'azione (azioni 3.1, 4.1 e 4.2)

Settore	N. Azione	Azione	Compito/i	Responsabile	Collaboratori	Scadenza	Commenti	Stato di avanzamento
L3: DIFESA DELLE RETI E DEI SISTEMI INFORMATIVI	Azione 3.1	Accompagnare gli attori del settore marittimo nell'attuazione di processi di sorveglianza, rilevamento e risposta agli incidenti di sicurezza informatica.	Promuovere la segnalazione degli incidenti da parte attori del settore marittimo	France Cyber marittimo	C2M2 MICA Center	dicembre 2021	Esistono già obblighi di segnalazione (LPM, NIS); nel 2018 la DAM ha diffuso una guida a tutti gli armatori	Da avviare
			Sviluppare e istituire meccanismi di raccolta degli incidenti	Francia Cyber marittimo	MICA Center ANSSI (CERT-FR)	Dicembre 2021		Da avviare
			Istituire un CERT marittimo	Francia Cyber Maritime	Centro MICA GENDARMERIA MARITTIMA ANSSI	dicembre 2023		Da lanciare
L4: RESILIENZA DELLE ATTIVITÀ	Azione 4.1	Organizzare la resilienza del settore	Implementare e testare i processi di gestione delle crisi;	Segreteria del C2M2	France Cyber Maritime ANSSI	dicembre 2021	Definizione di obiettivi, ambiti e interazioni con le esercitazioni esistenti	Da avviare
			Sviluppare il coordinamento tra gli attori e promuovere la condivisione delle buone pratiche.	Segreteria del C2M2	France Cyber Maritime ANSSI	Dicembre 2021		Da avviare
	Azione 4.2	In alternanza e con i settori marittimo e portuale, organizzare esercitazioni di crisi informatica	Mettere in atto una pianificazione delle esercitazioni per i settori marittimo e portuale, in collegamento con le grandi esercitazioni nazionali;	Segreteria del C2M2	France Cyber Maritime ANSSI	Ogni due anni	Attuazione di un programma di esercitazioni per le aree marittime e portuali.	Da avviare
			Diffondere a tutte le parti interessate l'analisi dei risultati delle esercitazioni e le azioni da intraprendere.	Segreteria del C2M2	France Cyber Maritime ANSSI	Ogni due anni		Da avviare

Posizione permanente di sicurezza informatica

Una necessaria rifondazione

- Ritorno alle origini: buone pratiche

Protezione: fin dalla progettazione

- A prova di tutto
- Tracciabilità e integrità del codice consegnato
- Mappatura e controllo dei flussi
- Pragmatismo a vantaggio dei punti di forza!

Difesa

- Supervisione dinamica della sicurezza:
- sonde e console

Continuità operativa – resilienza

- PCA / PRA
- MCS e piani di continuità e ripristino dopo un incidente

Posizione permanente di sicurezza informatica

Un aumento di potenza

- Quantitativa
- Qualitativa
- Comune

Formazione

- Sensibilizzazione
- Formazione universitaria
- CYBERSECPRO

Allenamenti

- Esercizi analoghi ai temi relativi alla sicurezza
- Canale ispirato alla lotta contro i sinistri
- Integrazione negli indicatori aziendali

Esempio di piano d'azione

SENSIBILIZZAZIONE – PIANO D'AZIONE

I	Sensibilizzare e formare	STANDARD	RINFORZATO
1	Formare i team operativi alla sicurezza dei sistemi informativi		
2	Sensibilizzare gli utenti alle buone pratiche di base in materia di sicurezza informatica		
3	Controllare i rischi dell'outsourcing informatico		
II	Conoscere il sistema informativo		
4	Identificare le informazioni e i server più sensibili e mantenere uno schema della rete		
5	Disporre di un inventario completo degli account privilegiati e mantenerlo aggiornato		
6	Organizzare le procedure di arrivo, partenza e cambio di funzione degli utenti		
7	Autorizzare la connessione alla rete dell'entità solo alle apparecchiature controllate		
III	Autenticare e controllare gli accessi		
8	Identificare nominalmente ogni persona che accede al sistema e distinguere i ruoli utente/amministratore		
9	Assegnare i diritti corretti sulle risorse sensibili del sistema informativo		
10	Definire e verificare le regole di scelta e dimensionamento delle password		
11	Proteggere le password memorizzate sui sistemi		
12	Modifica degli elementi di autenticazione predefiniti su dispositivi e servizi		
13	Privilegiare, quando possibile, un'autenticazione forte		

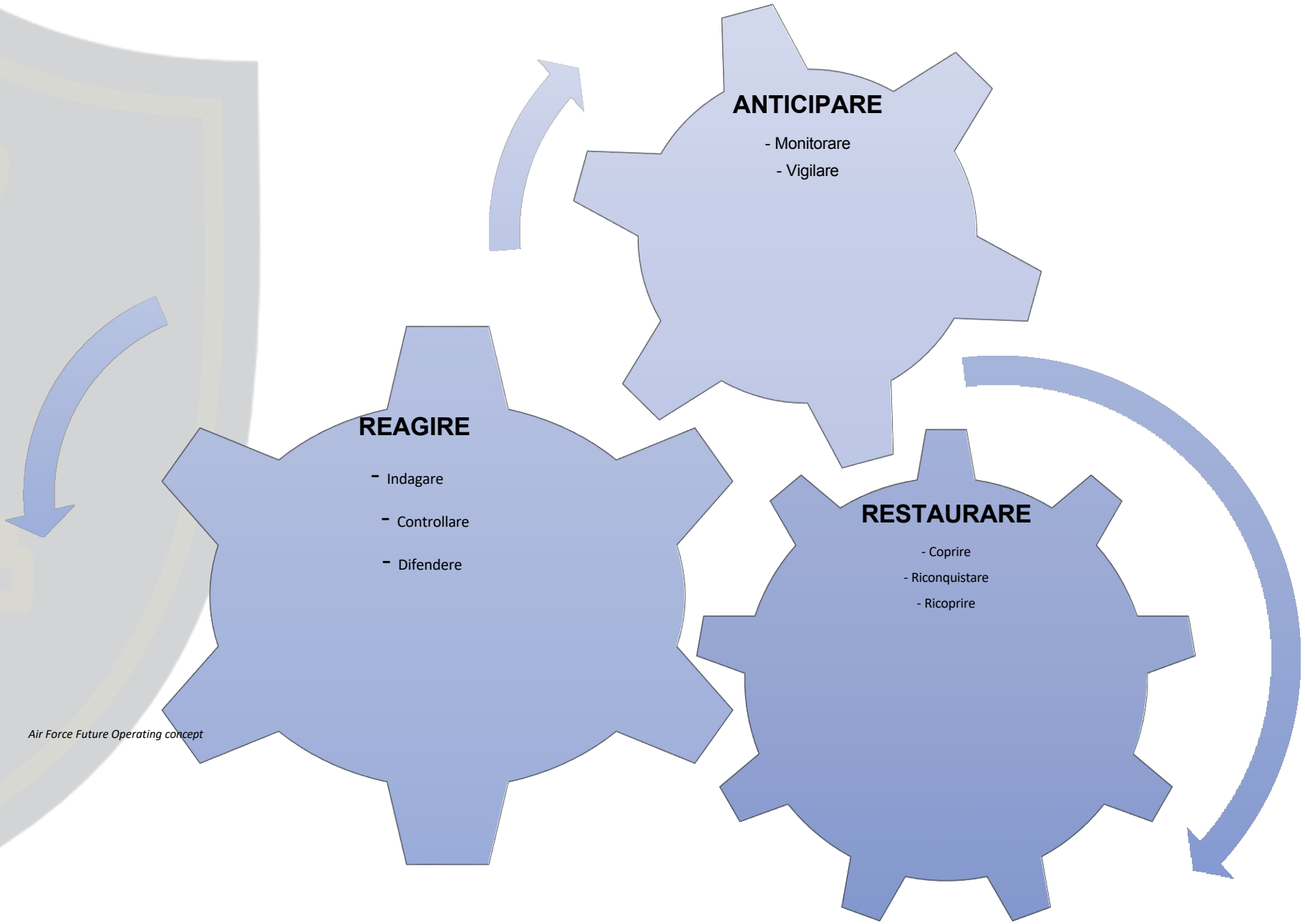
SENSIBILIZZAZIONE – PIANO D'AZIONE

IV	Proteggere le postazioni di lavoro		
14	Implementare un livello minimo di sicurezza su tutto il parco informatico		
15	Proteggersi dalle minacce relative all'uso di supporti rimovibili		
16	Utilizzare uno strumento di gestione centralizzata per uniformare le politiche di sicurezza		
17	Attivare e configurare il firewall locale dei computer		
18	Crittografare i dati sensibili trasmessi via Internet		
V	Proteggere la rete		
19	Segmentare la rete e creare una separazione tra queste zone		
20	Garantire la sicurezza delle reti Wi-Fi e la separazione degli utilizzi		
21	Utilizzare protocolli sicuri non appena disponibili		
22	Implementare un gateway di accesso sicuro a Internet		
23	Separare i servizi visibili da Internet dal resto del sistema informativo		
24	Proteggere la propria posta elettronica professionale		
25	Proteggere le interconnessioni di rete dedicate con i partner		
26	Controllare e proteggere l'accesso alle sale server e ai locali tecnici		

SENSIBILIZZAZIONE – PIANO D'AZIONE

VI	Rendere sicura l'amministrazione		
27	Vietare l'accesso a Internet dai computer o dai server utilizzati per l'amministrazione del sistema informatico		
28	Utilizzare una rete dedicata e separata per l'amministrazione del sistema informativo		
29	Limitare i diritti di amministrazione sulle postazioni di lavoro alle strette necessità operative		
VII	Gestire il nomadismo		
30	Adottare misure di sicurezza fisica dei terminali nomadi		
31	Crittografare i dati sensibili, in particolare quelli presenti su dispositivi che potrebbero andare persi		
32	Proteggere la connessione di rete dei dispositivi utilizzati in mobilità		
33	Adottare politiche di sicurezza dedicate ai dispositivi mobili		
VIII	Mantenere aggiornato il sistema informativo		
34	Definire una politica di aggiornamento dei componenti del sistema informativo		
35	Anticipare la fine della manutenzione dei software e dei sistemi e limitare le aderenze software		
IX	Supervisionare, controllare, reagire		
36	Attivare e configurare i registri dei componenti più importanti		
37	Definire e applicare una politica di backup dei componenti critici		
38	Effettuare controlli e audit di sicurezza regolari, quindi applicare le azioni correttive associate		
39	Designare un referente per la sicurezza dei sistemi informativi e comunicarlo al personale		
40	Definire una procedura di gestione degli incidenti di sicurezza		
X	Per approfondire		
41	Condurre un'analisi formale dei rischi		
42	Privilegiare l'uso di prodotti e servizi qualificati dall'ANSSI		

MISSIONI – ALTRA RAPPRESENTANZA



Air Force Future Operating concept

SENSIBILIZZAZIONE - PHISHING

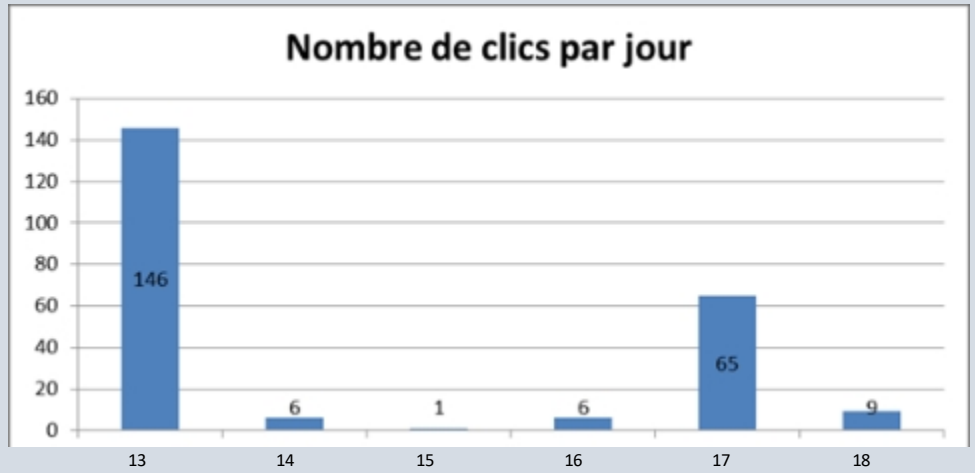
NOME	**PHISHING – HAMECONNAGE**		
DEFINIZIONE	Tecnica utilizzata da truffatori truffatori per ottenere informazioni informazioni personali. Far credere alla vittima di rivolgersi a una terza parte di fiducia.	**OBIETTIVO**	Usurpazione di identità.
		COME	Posta elettronica.
COME **COME REAGIRE**	Per qualsiasi messaggio ricevuto,	➢ Non aprire gli allegati ➢ Non cliccare mai sui link ipertestuali ➢ Verificare l'indirizzo del mittente ➢ Verificare l'ora e la data di invio ➢ Verificare l'oggetto del messaggio; ➢ Verificare che il messaggio non richieda informazioni insolite/personali ➢ Prestare attenzione ai messaggi di avviso visualizzati dalla propria casella di posta elettronica	
IN CASO DI DUBBIO	➢ Non aprire gli allegati	➢ Non cliccare su alcun link proposto	➢ Non rispondere al messaggio
	Avvisare il responsabile della sicurezza dei sistemi informativi		
CASO CONCRETO	**ESERCIZIO DI PHISHING CONDOTTO IN UN GRANDE GRUPPO**		

Una campagna di phishing ha preso di mira 1000 dipendenti del gruppo.

In **6 giorni**, il server "malintenzionato" ha raccolto **233 clic**. **NOTA:** il 14 e il 15 (fine settimana), il 16 giorno festivo.

Alla fine, **178 persone hanno cliccato (18%)** su uno dei link contenuti nell'e-mail trappola.

In caso di attacco reale, un solo clic avrebbe potuto compromettere l'intera azienda.



SENSIBILIZZAZIONE SSI - RANSOMWARE LOCKY

NOME	**LOCKY**	**TIPO**	RANSOMWARE	**DATA DI COMPARSA**	FEBBRAIO 2016
		SISTEMA INTERESSATO	SISTEMA OPERATIVO WINDOWS	**LUOGO**	EUROPA

IMPATTO	SEQUESTRO DEI VOSTRI DATI PERSONALI MEDIANTE CRITTOGRAFIA	
OBIETTIVO	RICHIESTA DI RISCATTO PER POTER RECUPERARE I DATI	
DIFFUSIONE	SI DIFFONDE TRAMITE E-MAIL TRAMITE **BOTNET** (vedi definizione)	
	ALLEGATO INFETTO CONTENUTO IN UN'E-MAIL	
METODO DI ATTACCO	RICEVIMENTO DI UN'E-MAIL CON UN ALLEGATO INFETTO:	OGGETTO (per ora): ATTN: Fattura J-XXXXXXX
		CORPO DEL MESSAGGIO: REDAZIONE CORRETTA, ALLEGATO IN FORMATO .DOC (IL PIÙ SPESSO, MA NON SEMPRE…)
		MITENTE: MAI LO STESSO
	ALL'APERTURA DEL PJ I DOCUMENTI DEL POSTO VENGONO CRITTOGRAFATI (FORMATO .LOCKY)	
	IL BLOCO NOTE SI APRIRÀ PER VISUALIZZARE UNA RICHIESTA DI RISCATTO	
	I LINK WEB INDICANO LA PROCEDURA PER RECUPERARE I DATI CON L'AIUTO DI UN DECODIFICATORE (CHIAMATO LOCKY DECRYPTOR PRO, LA CUI EFFICACIA NON È PROVATA)	
SOLUZIONE	**NESSUNA AL MOMENTO – PERDITA TOTALE DEI DATI**	
RACCOMANDAZIONI	NON PAGARE IL RISCATTO AI RICATTATORI PERCHÉ:	L'EFFICACIA DEL SOFTWARE DI DECODIFICA NON È PROVATA
		PERDITA DI DENARO
		INCORAGGIA I CRIMINALI INFORMATICI A CONTINUARE
MISURA PREVENTIVA ATTUALE	AGGIUNTA NEL REGISTRO DI SISTEMA DI WINDOWS DI UNA CARTELLA .LOCKY SENZA DIRITTO DI MODIFICA QUESTO METODO, IN CASO DI APERTURA DI UN ALLEGATO INFETTO, BLOCCA L'INSTALLAZIONE DI LOCKY E QUINDI LA CRITTOGRAFIA DEI DATI	

DEFINIZIONE BOTNET	UN **BOTNET** (DALL'INGLESE, CONTRATTURA DI "ROBOT" E "RETE") È UNA RETE DI PROGRAMMI CONNESSI A INTERNET CHE COMUNICANO CON ALTRI PROGRAMMI SIMILI PER L'ESECUZIONE DI ALCUNE ATTIVITÀ.

FINE