Catalogue des prestations et services liés à la SSI

SURTYMAR

Audits des SI des navires et des installations portuaires conformément aux circulaires : MSC/Circ,428(98) & MSC-FAL.1/Circ.3 du 05 juillet 2017.

A partir du 01 Janvier 2021, la résolution MSC.428 (98) de l'OMI « encourage les administrations à s'assurer que les cyber risques sont correctement pris en compte dans les systèmes de gestion de la sécurité existants (tels que définis dans l'ISM Code) au plus tard lors de la première vérification annuelle du document de conformité de l'entreprise.

Formation

SURTYMAR

Sensibilisation Equipage à la cyber sécurité – Niveau 1

Public Concerné	La formation « Sensibilisation à la cyber sécurité – Niveau 1 », s'adresse aux équipages à bord des navires, aux personnels des compagnies maritimes à terre et ceux d'entreprises ou organismes publics et/ou privés.
Objectif	Accroître la prise de conscience des membres des équipages des navires et ceux des organismes à terre sur les risques de la cyber sécurité. Accroître la vigilance des utilisateurs des systèmes d'information.
Prérequis	Aucun pré requis pour cette formation n'est demandé.
Méthode pédagogique	La session de formation se dérouler en présentiel ; La session de formation pourrait se dérouler en ligne, (Online – FOAD) avec un référent formateur SURTYMAR dédié et via un Learning Management System (LMS)
Durée	1,5 heure.
Auditoire	1 accès par agent.
Formateur	L'animation et l'encadrement de cette formation est assurée par un formateur ayant l'expertise et l'expérience de la mise en œuvre des savoirs et concepts enseignés. Le CV du formateur est disponible sur demande.
Dates et Lieux	A convenir avec le donneur d'ordre.

PROGRAMME ET CONTENU DE LA FORMATION

- Sensibilisation à la cyber sécurité maritime
- But de la SSI
- Quelles sont les menaces sur les SI
- Vulnérabilités pour un SI
- Impacts lors d'attaque d'un SI
- Risque sur un SI
- Recommandations

REFERENTIEL

- OMI MSC.428(98) / ISM

Information des participants :
Pour assurer une bonne efficacité de cette formation, le stagiaire aura, avant le début de la formation, pris connaissance des conditions de réalisation de cette session de formation, définies dans ce descriptif de formation ainsi que dans le Livret d'accueil du stagiaire (Modalités de réalisation, Règles d'hygiène applicables, Règles disciplinaires et sanctions applicables.)

Moyens et Supports pédagogiques :
La session de formation se déroule en ligne (Online – FOAD) avec un référent formateur SURTYMAR dédié et via un Learning Management System (LMS)

Sensibilisation Officiers à la cyber sécurité – Niveau 2

Public Concerné	La formation « Sensibilisation officiers à la cybersécurité – Niveau 2 », s'adresse aux officiers, aux personnes de niveau « Responsables » à bord des navires et au sein des compagnies à terre et d'entreprises et organismes publics et/ou privés.
Objectif	Rappeler l'importance des systèmes d'information pour les industries maritimes et offshore en raison de la transformation numérique rapide Accroître la prise de conscience des officiers des navires et ceux des organismes à terre quant aux risques de la cyber sécurité. Accroître la vigilance des utilisateurs des systèmes d'informations.
Prérequis	Avoir une connaissance assez suffisante dans l'exploitation des systèmes d'informations.
Méthode pédagogique	La session de formation se dérouler en présentiel ; La session de formation pourrait se dérouler en ligne, (Online – FOAD) avec un référent formateur SURTYMAR dédié et via un Learning Management System (LMS)
Durée	3 heures.
Auditoire	1 accès par agent.
Formateur	L'animation et l'encadrement de cette formation est assurée par un formateur ayant l'expertise et l'expérience de la mise en œuvre des savoirs et concepts enseignés. Le CV du formateur est disponible sur demande.
Dates et Lieux	A convenir avec le donneur d'ordre.

PROGRAMME ET CONTENU DE LA FORMATION

- Sensibilisation à la cyber sécurité maritime
- But de la SSI
- Quelles sont les menaces sur les SI
- Vulnérabilités pour un SI
- Impacts lors d'attaque d'un SI
- Risque sur un SI
- Politique de sécurité des SI et gestion du risque

REFERENTIEL

- OMI MSC.428(98) / ISM

Information des participants :

Pour assurer une bonne efficacité de cette formation, le stagiaire aura, avant le début de la formation, pris connaissance des conditions de réalisation de cette session de formation, définies dans ce descriptif de formation ainsi que dans le Livret d'accueil du stagiaire (Modalités de réalisation, Règles d'hygiène applicables, Règles disciplinaires et sanctions applicables.)

Moyens et Supports pédagogiques :

La session de formation se déroule en ligne (Online – FOAD) avec un référent formateur SURTYMAR dédié et via un Learning Management System (LMS)

Formation Cyber sécurité à l'attention des Broadcast Manager – Niveau 3

Public Concerné	La formation Cyber sécurité Niveau 3, s'adresse aux Broadcast Manager, aux gestionnaires et administrateurs des systèmes d'informations à bord des navires et au sein des compagnies à terre et d'entreprises ou organismes publics et/ou privés.
Objectif	Assurer la sécurité des systèmes d'informations. Veiller sur mise en place des moyens susceptibles de contrecarrer les risques liés à la cyber sécurité. Garantir la fiabilité des moyens mis en place. Accroître la prise de conscience des officiers des navires et ceux des organismes à terre quant aux risques de la cyber sécurité. Accroître la vigilance des utilisateurs des systèmes d'informations.
Prérequis	Avoir des compétences en matière d'administration des systèmes d'informations.
Méthode pédagogique	La session de formation se dérouler en présentiel ; La session de formation pourrait se dérouler en ligne, (Online – FOAD) avec un référent formateur SURTYMAR dédié et via un Learning Management System (LMS)
Durée	7 heures.
Auditoire	1 accès par agent.
Formateur	L'animation et l'encadrement de cette formation est assurée par un formateur ayant l'expertise et l'expérience de la mise en œuvre des savoirs et concepts enseignés. Le CV du formateur est disponible sur demande.
Dates et Lieux	A convenir avec le donneur d'ordre.

PROGRAMME ET CONTENU DE LA FORMATION

- Sensibilisation à la cyber sécurité maritime
- Sensibilisation et Prévention aux logiciels malveillants
- Sensibilisation et Prévention des menaces internes
- Sensibilisation et Prévention à l'ingénierie sociale
- Sensibilisation et Prévention des à l'informatique mobile
- Navigation WEB sécurisée
- But de la SSI
- Quelles sont les menaces sur les SI
- Vulnérabilités pour un SI
- Impacts lors d'attaque d'un SI
- Risque sur un SI
- Politique de sécurité des SI et gestion du risque
- Recommandations

Information des participants :

Pour assurer une bonne efficacité de cette formation, le stagiaire aura, avant le début de la formation, pris connaissance des conditions de réalisation de cette session de formation, définies dans ce descriptif de formation ainsi que dans le Livret d'accueil du stagiaire (Modalités de réalisation, Règles d'hygiène applicables, Règles disciplinaires et sanctions applicables.)

Moyens et Supports pédagogiques :

La session de formation se déroule en ligne (Online – FOAD) avec un référent formateur SURTYMAR dédié et via un Learning Management System (LMS)

REFERENTIEL

- OMI MSC.428(98) / ISM

Audit

SURTYMAR

SURTYMAR
AGENCE DE SÛRETÉ MARITIME ET PORTUAIRE

Centre de Formation Maritime CFM Agréé pour la sûreté

Audit organisationnel et physique

La conduite de l'Audit est assurée par un auditeur expert en SSI ayant l'expertise et la mise en œuvre des savoirs et concepts en matière de SSI. Les domaines de compétences sont comme suit :

- Maîtrise des pratiques liées à l'audit organisationnel et physique :
  - Conduite d'entretien ;
  - Sondage par échantillon ;
  - Observation et récolte des preuves physiques ;
  - Analyse documentaire.

- Domaines relatifs à l'audit organisationnel et physique :
  - Politiques de sécurité de l'information;
  - Organisation de la sécurité de l'information;
  - La sécurité des ressources humaines;
  - Gestion des actifs Contrôle d'accès;
  - Cryptographie;
  - Sécurité physique et environnementale;
  - Sécurité liée à l'exploitation;
  - Sécurité des communications;
  - Acquisition, développement et maintenance des systèmes d'information;
  - Relations avec les fournisseurs;
  - Gestion des incidents liés à la sécurité de l'information;
  - Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité;
  - Conformité…

CADRE NORMATIF, JURIDIQUE ET RÉGLEMENTAIRE

- Directive Nationale de la sécurité des systèmes d'information ;
- Normes ISO 27001 et ISO 27002 ;
- Textes juridiques et réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes …

SURTYMAR
AGENCE DE SÛRETÉ MARITIME ET PORTUAIRE

Centre de Formation Maritime CFM Agréé pour la sûreté

Audit de configuration

La conduite de l'Audit est assurée par un auditeur expert en SSI ayant l'expertise et la mise en œuvre des savoirs et concepts en matière de SSI. Les domaines de compétences sont comme suit :

- Equipements de sécurité :
  - Pare-feu ;
  - Système de sauvegarde ;
  - Système de stockage mutualisé ;
  - Logiciels de sécurité côté poste client.

- Equipements réseau et protocoles :
  - Protocoles réseau et infrastructures ;
  - Protocoles applicatifs courants et service d'infrastructure ;
  - Configuration et sécurisation des principaux équipements réseau du marché ;
  - Réseaux de télécommunications ;
  - Technologie sans fil ;
  - Téléphonie.

-Couche applicative :
- Guides et principes de développement sécurisé ;
- Applications de type Web ou client/serveur ;
- Mécanismes cryptographiques (SSL, VPN, etc..) ;
- Socle applicatif :
  * Serveurs web,
  *Serveurs d'application,
  *Systèmes de gestion de bases de données.

- Systèmes d'exploitation :
  - Architectures Microsoft ;
  - Systèmes UNIX/Linux ;
  - Solution de virtualisation.

- - Environnements de virtualisation.

CADRE NORMATIF, JURIDIQUE ET RÉGLEMENTAIRE
- Directive Nationale de la sécurité des systèmes d'information ;
- Normes ISO 27001 et ISO 27002 ;
- Textes juridiques et réglementaires relatifs à la sécurité des systèmes d'i nformation, aux audits et aux sujets connexes ,

SURTYMAR
AGENCE DE SÛRETÉ MARITIME ET PORTUAIRE

Centre de Formation Maritime CFM Agréé pour la sûreté

Audit des architectures

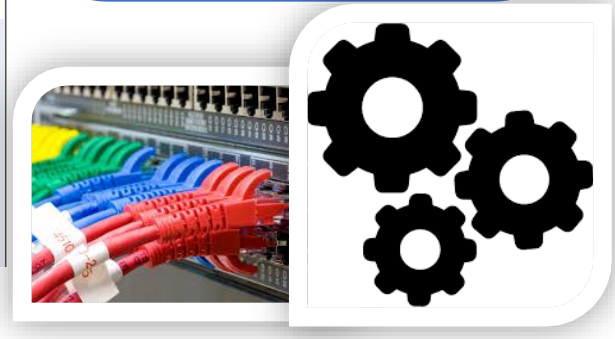
La conduite de l'Audit est assurée par un auditeur expert en SSI ayant l'expertise et la mise en œuvre des savoirs et concepts en matière de SSI. Les domaines de compétences sont comme suit :

- Equipements et logiciels de sécurité :
- Pare-feu ;
- Système de sauvegarde ;
- Système de stockage mutualisé ;
- Dispositifs de chiffrement des communications ;
- Serveurs d'authentification ; Serveurs mandataires inverses ;
- Solutions de gestion de la journalisation ;
- Équipements de détection et prévention d'intrusion.

-Réseaux et protocoles :
- Protocoles réseau et infrastructures ;
- Protocoles applicatifs courants et service d'infrastructure ;
- Configuration et sécurisation des principaux équipements réseau du marché ;
- Réseaux de télécommunications ;
- Technologie sans fil ;

-Techniques et outils pour établir des :
- Cartographies fonctionnelles, techniques et applicatives ;
- Schémas d'architecture ;
- Architectures hautement disponibles et redondantes ;
- Mécanismes de défense en profondeur.
- Téléphonie.

CADRE NORMATIF, JURIDIQUE ET RÉGLEMENTAIRE
- Directive Nationale de la sécurité des systèmes d'information ;
- Normes ISO 27001 et ISO 27002 ;
- Textes juridiques et réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes ,



SURTYMAR
AGENCE DE SÛRETÉ MARITIME ET PORTUAIRE

Centre de Formation Maritime CFM Agréé pour la sûreté

Tests d'intrusion

La conduite de l'Audit est assurée par un auditeur expert en SSI ayant l'expertise et la mise en œuvre des savoirs et concepts en matière de SSI. Les domaines de compétences sont comme suit :

- Equipements de sécurité :
  - Pare-feu ;
  - Dispositif de chiffrement des communications ;
  - Serveur d'authentification ;
  - Solution de gestion de la journalisation ;
  - Equipement de détection et prévention d'intrusion ;
  - logiciels de sécurité côté poste client.

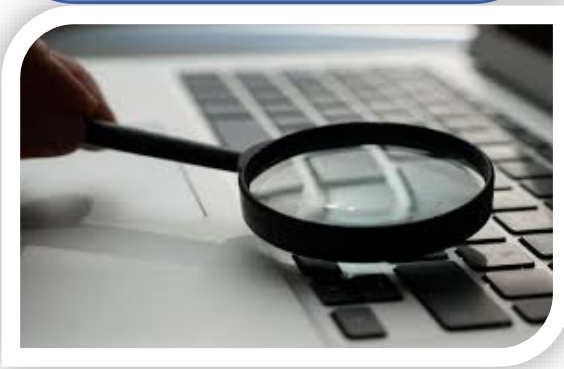
- Réseau et protocoles :
  - Protocoles réseau et infrastructures ;
  - Protocoles applicatifs courants et service d'infrastructure ;

- Systèmes d'exploitation :
  - Systèmes Microsoft;
  - Systèmes UNIX/Linux ;
  - Solutions de virtualisation.
  - Technologie sans fil.

- Couche applicative :
  - Applications de type Web ou client/serveur;
  - Langages de programmation utilisés pour la configuration (ex : scripts, filtres WMI, etc.) ;
  - Mécanismes cryptographiques (SSL, VPN, etc..);
    - ✓ Socle applicatif :
    - ✓ Serveurs web,
    - ✓ Serveurs d'application,
  - Systèmes de gestion de bases de données. - techniques d'intrusion.

CADRE NORMATIF, JURIDIQUE ET RÉGLEMENTAIRE

- Directive Nationale de la sécurité des systèmes d'information ;
- Normes ISO 27001 et ISO 27002 ;
- Textes juridiques et réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes ,



SURTYMAR
AGENCE DE SÛRETÉ MARITIME ET PORTUAIRE

Centre de Formation Maritime CFM Agréé pour la sûreté

Audit du code source

La conduite de l'Audit est assurée par un auditeur expert en SSI ayant l'expertise et la mise en œuvre des savoirs et concepts en matière de SSI. Les domaines de compétences sont comme suit :

- attaques :
  - Principes et méthodes d'intrusion applicatives ;
  - Contournement des mesures de sécurité logicielles ;
  - Techniques d'exploitation de vulnérabilités et d'élévation de privilèges

- couche applicative :
  - Guides et principes de développement sécurisé ;
  - Architectures applicatives (client/serveur, n-tiers, etc.) ;
  - Langages de programmation ;
  - Mécanismes cryptographiques ;
  - Mécanismes de communication (internes au système et par le réseau) et protocoles associés ;
  - Socle applicatif :
    - ✓ serveurs web ;
    - ✓ serveurs d'application ;
    - ✓ systèmes de gestion de bases de données ;
    - ✓ progiciels ;

CADRE NORMATIF, JURIDIQUE ET RÉGLEMENTAIRE

- Directive Nationale de la sécurité des systèmes d'information ;
- Normes ISO 27001 et ISO 27002 ;
- Textes juridiques et réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes ,

SURTYMAR
AGENCE DE SÛRETÉ MARITIME ET PORTUAIRE

Centre de Formation Maritime CFM Agréé pour la sûreté

Audit des systèmes d'information Industriels

La conduite de l'Audit est assurée par un auditeur expert en SSI ayant l'expertise et la mise en œuvre des savoirs et concepts en matière de SSI ainsi que d'autres qualités techniques . Les domaines de compétences sont comme suit :

- architectures fonctionnelles à base d'automates programmables industriels (PLC) ;

- réseaux et protocoles industriels :

- Topologie des réseaux industriels ;
- Cloisonnement des réseaux industriels vis-à-vis des autres systèmes d'information ;
- Protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850) ;
- Technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la couche 802.15.4).
- Equipements :
- Configuration et sécurisation des principaux automates et équipements industriels du marché.

CADRE NORMATIF, JURIDIQUE ET RÉGLEMENTAIRE

- Directive Nationale de la sécurité des systèmes d'information ;
- Normes ISO 27001 et ISO 27002 ;
- Textes juridiques et réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes ,