MIRAT DI NERIDE

Formations

Cybersécurité, nouvel enjeu des décideurs.

Votre intervenant

Didier SPELLA

Dirigeant de MIRAT DI NERIDE

Expert en stratégie des entreprises et en cybercriminalité

Co-fondateur de CMCS

Responsable Bureau CLUSIR - Nouvelle Aquitaine Ouest

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

DATADOCKÉ

MIRAT DI NERIDE

Coordonnées Administratives

48 rue Antoine Chanzy 17300 ROCHEFORT
SIRET: 51768965900012
TVA Intracom: FR49517689659
MIRAT DI NERIDE SAS au capital de10 000 €
RCS LA ROCHELLE 517 689 659 - N° de Gestion 2009 B 968
Email : didier.spella@mirat-di-neride.com
Enregistrée sous le numéro 54 17 01396 17
Cet enregistrement ne vaut pas agrément de l'Etat

DATADOCKÉ

SecNumedu
Formation continue
ANSSI

MIRAT DI NERIDE

My business's Your Success

SecNum*edu*-FC

Cybersécurité, nouvel enjeu des décideurs.

SecNumedu
Formation continue
ANSSI

Attestation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Attestation de conformité au référentiel SecNum*edu*-Formation Continue

visant à labelliser les formations continues en sécurité du numérique

attribuée à :

MIRAT DI NERIDE

Pour la formation continue

« *CYBERCRIMINALITE : Virus, intrusion des systèmes d'information, piratage de données, usurpation d'identité bancaire, ransomware. Chef d'entreprise, face à ces risques, êtes-vous prêt ?* »

Référence de l'attestation : ANSSI-20-009

Valide jusqu'en avril 2023

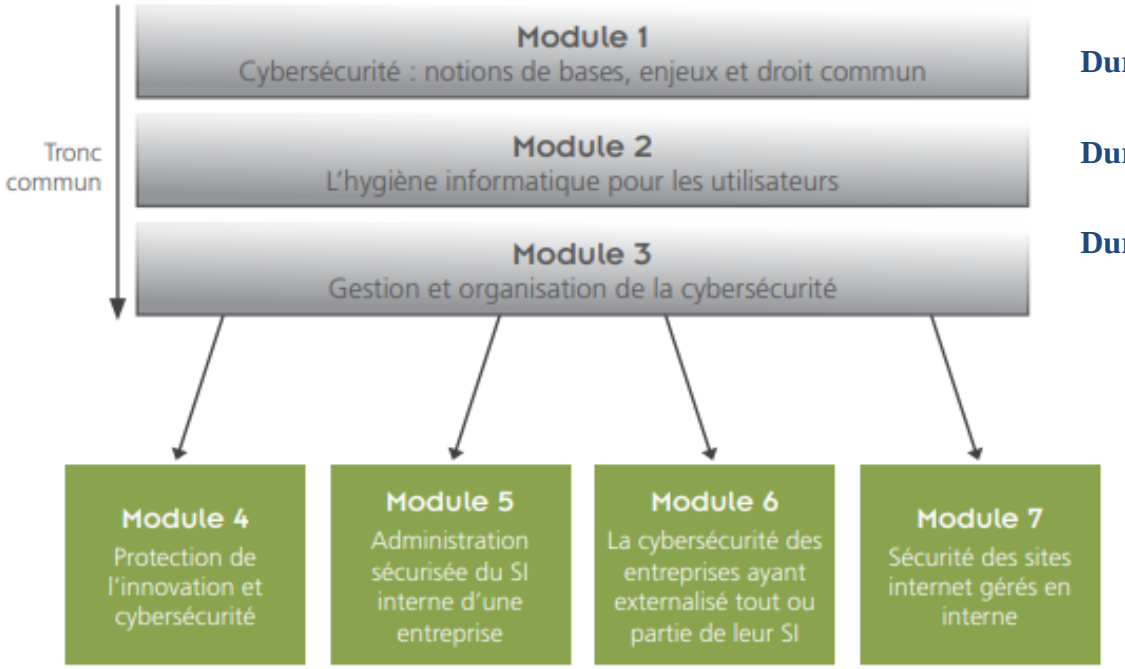
Paris, le 19/03/2020

Guillaume Poupard

Directeur général de l'Agence nationale
de la sécurité des systèmes d'information

Cette attestation est émise conformément au référentiel SecNumedu disponible sur le site www.ssi.gouv.fr
Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information, 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Cursus SecNum*Edu*-FC



Durée : 3 heures

Durée : 3 heures

Durée : 3 heures

Durée : 3 heures **Durée** : 7 heures **Durée** : 3 heures **Durée** : 10h5 heures

DGE DIRECTION GÉNÉRALE DES ENTREPRISES — ANSSI — SISSE Service de l'Information Stratégique et de la Sécurité Économiques

Les trois modules du tronc commun, sont complétés par des modules complémentaires. Ils permettent ainsi de proposer une offre globale correspondant au mieux aux problématiques que peut rencontrer le chef d'entreprise.

Source : https://www.ssi.gouv.fr/uploads/2015/04/formation_cybersecurite_tpe_pme_mars_2017_sisse.pdf

MIRAT DI NERIDE

CYBERSECURITE : Notions de bases, enjeux, et droit commun Module 1

SecNumedu
Formation continue
ANSSI

Programme de formation

± **D**éfinitions :
• Intelligence économique, sécurité économique globale
• Cybersécurité, Sécurité des SI, Cyberdéfense, Cybercriminalité, Cybersécurité

± **L**es enjeux de la sécurité des SI
• La nouvelle économie de la cybercriminalité
• Panorama des menaces selon une typologie
• Les vulnérabilités (exemples, détermination, veille)
• Focus sur l'ingénierie sociale

± **L**es propriétés de sécurité
• Présentation du principe de défense en profondeur
• Identification et évaluation des actifs et des objectifs de sécurité

± **A**spects juridiques et assurantiels
• Responsabilités
• Préservation de la preuve
• L'offre assurantielle

± **L**e paysage institutionnel de la cybersécurité
• La prévention
• Le traitement des cyberattaques et la réponse judiciaire
• Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers

MIRAT DI NERIDE

CHARENTE-MARITIME CYBER SÉCURITÉ CMCS

CYBERSECURITE : L'hygiène informatique pour les utilisateurs Module 2

SecNumedu
Formation continue
ANSSI

Programme de formation

± **P**résentation du Guide d'hygiène

± **Con**naître le système d'information et ses utilisateurs

- Faire une cartographie des SI de l'entreprise.

± **I**dentifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes …) et de son système informationnel

± **M**aîtriser le réseau de partage de documents (en interne ou sur internet)

± **M**ettre à niveau les logiciels

± **A**uthentifier l'utilisateur

- Présentation des différentes méthodes permettant d'authentifier les utilisateurs
- Evoquer les bonnes pratiques pour les mots/phrases de passe (conception, fréquences d'utilisation, etc.).

± **N**omadisme – Problématiques liées au BYOD (Bring your Own Devices)

MIRAT DI NERIDE

CYBERSECURITE : Gestion et organisation de la cybersécurité Module 3

SecNumedu
Formation continue
ANSSI

Programme de formation

± **P**résentation des publications / recommandations
• Guides de l'ANSSI
• Recommandations de la CNIL
• Club de la Sécurité de l'information Français, Club des experts de la sécurité de l'information et du numérique (CLUSIF / CESIN), etc
• Observatoires zonaux de la Sécurité des systèmes d'information (SSI)
• Les CERTs (Computer Emergency Response Team)

± **P**résentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.)

± **M**éthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)

± **M**aîtriser le rôle de l'image et de la communication dans la cybersécurité
• Surveillance de l'e-réputation
• Communication externe
• Usage des réseaux sociaux, professionnel et personnel

± **M**éthodologie d'évaluation du niveau de sécurité

± **A**ctualisation du savoir du référent en cybersécurité

± **G**érer un incident / Procédures judiciaires

MIRAT DI NERIDE

CYBERSERCURITÉ : Protection de l'innovation et cybersécurité

Module 4

SecNumedu
Formation continue
ANSSI

Programme de formation

±Les modalités de protection du patrimoine immatériel de l'entreprise Intelligence économique, sécurité économique globale
L'objectif est de présenter les différentes mesures et éventuelles obligations en la matière.

± Les Droit de la propriété intellectuelle lié aux outils informatiques
L'objectif est de donner les moyens nécessaires aux entreprises ayant des données importantes pour connaitre les tenants et les aboutissants des contrats.

± Cyber-assurances
L'objectif est de donner les clés nécessaires à une entreprise dans le cas où elle souhaiterait souscrire à une offre de cyber-assurance.

± Cas pratiques
Présentation de cas de cyber-attaques avérés

MIRAT DI NERIDE

CYBERSERCURITÉ : Administration sécurisée du système d'information (SI) interne d'une entreprise

Module 5

SecNumedu
Formation continue
ANSSI

Programme de formation

± Analyse de risque (Expression des besoins et identification des objectifs de sécurité -EBIOS / Méthode harmonisée d'analyse des risques - MEHARI)

± Principes et domaines de la SSI afin de sécuriser les réseaux internes.

- Politique et stratégie de sécurité,
- Gestion des flux, notamment réseaux sans fil / architecture réseaux (cloisonnement du réseau),
- Gestion des comptes, des utilisateurs, des privilèges selon le besoin d'en connaître,
- Gestion des mots de passe, des mises à jour,
- Journalisation et analyse,
- Gestion des procédures,
- Plan de continuité d'activité (PCA) / Plan de reprise d'activité (PRA),
- Virtualisation / cloisonnement.

± Détecter un incident.

± Gestion de crise

± Méthodologie de résilience de l'entreprise

± Traitement et recyclage du matériel informatique en fin de vie (ordinateurs, copieurs, supports amovibles, etc.)

± Aspects juridique

- Responsabilité en l'absence de conformité des infrastructures,
- Cyber-assurances.

MIRAT DI NERIDE

CYBERSERCURITÉ : La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI.

Module 6

SecNumedu
Formation continue
ANSSI

Programme de formation

± Les différentes formes d'externalisation
- Les contrats de services « classiques »
- Enjeux du Cloud Computing
- Techniques de sécurité lors de l'externalisation (chiffrement des données…)

± Comment choisir son prestataire de service ?
- Présentation du référentiel de l'ANSSI Maîtriser les risques de l'infogérance
- Présentation de la qualification SecNumCloud applicable aux prestataires de services d'informatique en nuage

± Aspects juridiques et contractuels.
- Connaître les bases juridiques pour protéger son patrimoine économique lors de l'externalisation d'un SI
- Obligations en matière d'utilisation, de localisation et de transfert de données

MIRAT DI NERIDE

CYBERSERCURITÉ : Sécurité des sites internet gérés en interne.

Module 7

SecNumedu
Formation continue
ANSSI

Programme de formation

± Menaces propres aux sites internet

± Approche systémique de la sécurité (éviter l'approche par patches)

± Configuration des serveurs et services

± HTTPS et Infrastructure de gestion de clés (IGC)

± Services tiers

± Avantages et limites de l'utilisation d'un Content Management System (CMS ou Gestion des contenus) et / ou développement web

± Sécurité des bases de données

± Utilisateurs et sessions

± Obligations juridiques réglementaires

MIRAT DI NERIDE

CYBERSECURITE : Gestion et organisation de la cybersécurité Validation

Programme de formation

Devenir référent cybersécurité

Objectifs de la formation	Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques ; Connaître les obligations et responsabilités juridiques de la cybersécurité ; Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux Internet, réseaux privés d'entreprises, réseaux publics ; Mettre en œuvre les démarches de sécurité spécifiques à l'activité de son entreprise ; Savoir présenter les précautions techniques et juridiques pour faire face aux attaques.
Public visé	Public hétérogène parmi les salariés des entreprises: dirigeant, cadre, responsable informatique, etc.
Prérequis	Pas de prérequis exigé pour suivre cette formation
Méthodes pédagogiques et suivi	Pédagogie interactive impliquant largement chaque participant : • Adaptation des apports théoriques à l'expérience et aux besoins de chacun • Théorie – Cas pratiques -Mises en situation • Groupe d'une dizaine de participants Suivi : • Feuille d'émargement par demi-journée • Attestation de formation
Méthode d'évaluation des acquis	• QCM en fin de formation

MIRAT DI NERIDE

SecNum*edu*-FC – La méthode Ebios RM

Cybersécurité, nouvel enjeu des décideurs.

SecNumedu
Formation continue
ANSSI

MIRAT DI NERIDE

My business's Your Success

EBIOS *RISK MANAGER*

SecNumedu
Formation continue
ANSSI

Attestation

PREMIER MINISTRE

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Attestation de conformité au référentiel SecNum*edu*-Formation Continue

visant à labelliser les formations continues en sécurité du numérique

attribuée à :

MIRAT DI NERIDE

Pour la formation continue

« *Analyse de Risque*

Chefs d'Entreprise, appréhender mieux vos risques afin d'accroître la valeur de votre entreprise »

Référence de l'attestation : ANSSI-20-022

Valide jusqu'en octobre 2023

Paris, le 25/09/2020

Guillaume Poupard

Directeur général de l'Agence nationale de la sécurité des systèmes d'information

Cette attestation est émise conformément au référentiel SecNumedu disponible sur le site www.ssi.gouv.fr

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information, 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Présentation de la formation

Cette formation s'adresse en priorité aux dirigeants et responsables d'entreprises. Elle permet de comprendre l'analyse de risques au travers de la méthode EBios Risk Manager.

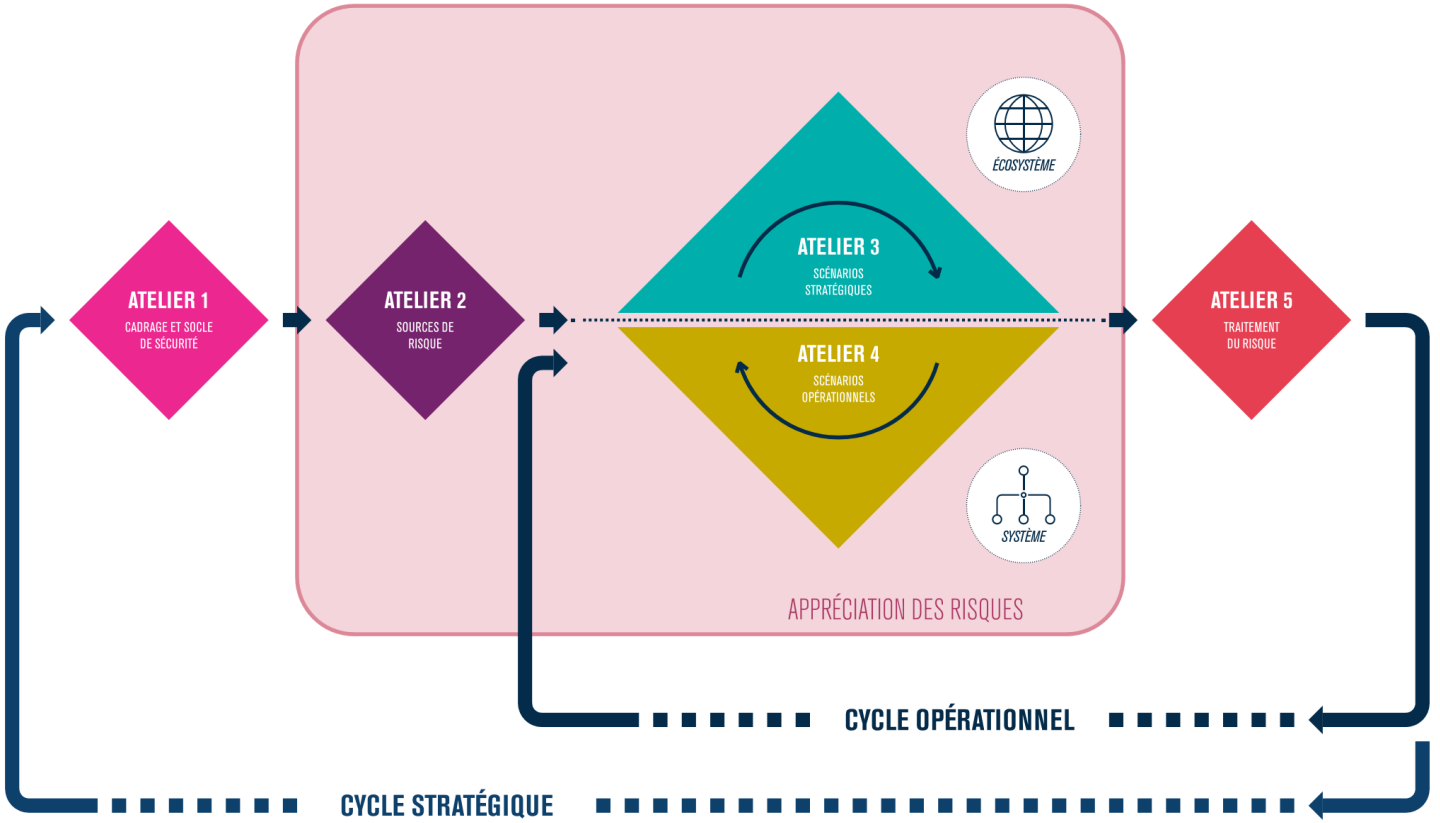
D'un côté pratique, elle présente les 5 ateliers qui structurent la méthode (voir page suivante). Ceux-ci permettent ainsi aux apprenants de se familiariser avec la méthode. Ils seront orientés sur leurs domaines d'activité. Ils se complètent en final par une analyse grandeur nature.

Elle se déroule sur 2 jours soient 14 heures de formation.
Le premier jour permet d'étudier le déroulement des 3 premiers ateliers.
Le deuxième jour permet de poursuivre cette étude sur les ateliers 4 & 5 complété par une étude de cas.

Ces formations s'adressent à des promotions de 6 à 8 stagiaires.

Présentation de la formation

Comme pour la méthode, cette formation suit le déroulement de la méthode afin de faire comprendre son côté récursif, basé sur le même principe de la boucle d'amélioration continue plus connue sous le terme de PDCA.



Introduction et Atelier 1 – Cadrage et socle de sécurité (J1-2h30)

Introduction

Objectif : obtenir l'accord des apprenants sur le cadre de la formation..

- Accueil des apprenants
- Recueil des attentes des apprenants
- Règles et programme

Objectif : Faire comprendre comment réunir les éléments nécessaires pour adapter la gestion des risques au contexte particulier du sujet de l'étude.

- Présentation du déroulement de l'atelier
- Valeurs métier et biens supports
- Événements redoutés (ER), impacts et gravité
- Socle de sécurité
- Mesures issues de l'atelier
- Exercice(s)

Cet atelier vise à identifier l'objet de l'étude, les participants aux ateliers et le cadre temporel. Au cours de cet atelier, nous recensons les missions, de valeurs métier et biens supports relatifs à l'objet étudié. Nous identifions événements redoutés associés aux valeurs métier et évaluez la gravité de leurs impacts. Nous définissons également le socle de sécurité et les écarts.

Atelier 2 –Sources de risque (J1-2h)

Objectif : Faire comprendre comment identifier et analyser l'origine des risques : les couples sources de risques (SR) / objectifs visés (OV)

- Présentation du déroulement de l'atelier
- Couples sources de risques (SR) / objectifs visés (OV)
- Mesures issues de l'atelier
- Exercice(s)

Dans ce deuxième atelier, nous identifions et caractérisons les sources de risque (SR) et leurs objectifs de haut niveau, appelés objectifs visés (OV). Les couples SR/OV jugés les plus pertinents sont retenus au terme de cet atelier. Les résultats seront formalisés dans une cartographie des sources de risque.

Atelier 3 – Scénarios stratégiques (J1-2h30)

Objectif : Expliquer comment élaborer les scénarios stratégiques.

- Présentation du déroulement de l'atelier
- Parties prenantes : identification
- Parties prenantes : évaluation
- Scénarios stratégiques
- Mesures issues de l'atelier
- Exercice(s)

Dans ce troisième atelier 3, nous vous faisons acquérir une vision claire de l'écosystème et établir une cartographie de menace numérique de celui-ci vis-à-vis de l'objet étudié. Ceci va vous permettre de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ils représentent les chemins d'attaque qu'une source de risque est susceptible d'emprunter pour atteindre son objectif. Ces scénarios se conçoivent à l'échelle de l'écosystème et des valeurs métier de l'objet étudié. Ils sont évalués en termes de gravité. À l'issue de cet atelier, vous pouvez déjà définir des mesures de sécurité sur l'écosystème.

Atelier 4 – Scénarios opérationnels (J2-1h45)

Objectif : Expliquer comment élaborer les scénarios opérationnels.

- Présentation du déroulement de l'atelier
- Scénarios opérationnels
- Mesures issues de l'atelier
- Exercice(s)

Le but de ce quatrième atelier est de construire des scénarios techniques reprenant les modes opératoires susceptibles d'être utilisés par les sources de risque pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l'atelier précédent mais se concentre sur les biens supports critiques. Nous évaluons ensuite le niveau de vraisemblance des scénarios opérationnels obtenus.

Atelier 5 – Traitement du risque (J2-1h45)

Objectif : Expliquer comment choisir les traitements appropriés des risques, les planifier et suivre leur mise en œuvre.

- Présentation du déroulement de l'atelier
- Mesures pour traiter les risques
- Suivi des risques

Le dernier atelier consiste à réaliser une synthèse de l'ensemble des risques étudiés en vue de définir une stratégie de traitement du risque. Cette dernière est ensuite déclinée en mesures de sécurité inscrites dans un plan d'amélioration continue. Lors de cet atelier, nous établirons la synthèse des risques résiduels et définissez le cadre de suivi des risques.

Étude de cas (J2- 3h30)

Objectif : S'assurer de la bonne appropriation de la logique globale.

- Mise en pratique des concepts
- Déroulé des 5 ateliers dans le cadre d'un cas concret

A l'issue de cette formation, après s'être approprié la méthode l'apprenant sera en mesure de l'appliquer dans son entreprise ou organisation.

N.B. En cas de formation intra-entreprise, cette formation pourra être adaptée au contexte spécifique de l'organisme ou de l'entreprise