

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Responsable en cybersécurité

RNCP37300 · Certification RNCP · Niveau 6

Ce parcours de 440 heures prépare au titre de Responsable en cybersécurité (RNCP37300, niveau 6) en couvrant intégralement ses quatre blocs : pilotage de la cyberprotection, audit, supervision et investigation numérique. Construit autour d'un fil rouge réaliste dans un environnement de défense, il fait progresser l'apprenant du rôle d'appui au RSSI jusqu'à la conduite d'investigations inforensiques et au pilotage d'un centre de supervision.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	4

01 · PRÉSENTATION

La formation en bref

Intitulé	Responsable en cybersécurité
Code	RNCP37300
Type	Certification RNCP
Niveau	Niveau 6
Certificateur	MINISTERE DES ARMEES
Durée	440 h, 20 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026
Fin d'enregistrement de la certification	26/08/2027

Le métier et les compétences visées

Le Responsable en cybersécurité conduit des actions défensives, et le cas échéant offensives, pour garantir la continuité et l'efficacité des activités d'une organisation, notamment au sein des forces armées. Il appuie le RSSI ou le DSI dans la gouvernance de la sécurité, administre la sécurité des systèmes et des réseaux, et prépare les unités à faire face aux incidents. Il audite les systèmes d'information, réalise des tests d'intrusion et propose des plans de remédiation. Il dirige des équipes de techniciens en centre de supervision, améliore les dispositifs de détection et pilote la réponse à incident. Enfin, il mène des investigations numériques, capitalise les retours d'expérience et forme les utilisateurs aux bonnes pratiques.

Public visé

- Militaires des armées (Terre, Marine nationale) occupant un poste du domaine des systèmes d'information et de communication décrit en cybersécurité
- Techniciens veilleurs de cybersécurité titulaires d'une certification de niveau 5 souhaitant évoluer vers des fonctions de responsabilité
- Administrateurs systèmes et réseaux expérimentés souhaitant se spécialiser en cybersécurité
- Analystes SOC ou CSIRT souhaitant accéder à des fonctions de supervision, d'audit ou d'investigation numérique
- Professionnels en reconversion ou en évolution interne, sous réserve de satisfaire aux conditions d'accès fixées par le certificateur

Prérequis

- Détenir une certification de niveau 5 dans le domaine, par exemple le titre de Technicien veilleur de cybersécurité (RNCP36164), ou une qualification militaire équivalente listée par le référentiel (FS2 Cyber, QAP 2 CYS, BS SITEL, BS SYNUM, BS RECOM, FSI, C CAPSI selon l'armée)
- Justifier d'une expérience professionnelle dans le domaine : au moins 5 années après le brevet militaire de 2e degré sur un poste SIC décrit en cybersécurité pour l'armée de Terre, au moins 2 années d'expérience en cybersécurité pour la Marine nationale
- Justifier d'un niveau d'anglais équivalent au niveau B1 du CECRL (score TOEIC de 550 points ou profil linguistique standardisé 2222)
- Pour l'exercice de l'emploi au sein du ministère des Armées : statut militaire et habilitation « Secret Défense » exigés par la réglementation

Objectifs pédagogiques

À l'issue du parcours, l'apprenant est capable de :

- Appuyer le RSSI ou le DSI dans l'élaboration des moyens, procédures et documents réglementaires de cybersécurité d'une entité
- Conduire une analyse des risques sur un périmètre défini et préparer une entité à l'homologation de son système d'information
- Sécuriser les architectures réseaux, l'administration des systèmes et la gestion des droits d'accès, et proposer des solutions de chiffrement adaptées
- Auditer la conformité organisationnelle et technique d'un système d'information au regard d'un référentiel défini
- Réaliser un test d'intrusion et rédiger le rapport technique associé
- Formaliser les non-conformités et construire un plan d'action de remédiation argumenté selon l'interlocuteur
- Diriger une équipe de techniciens en centre de supervision et qualifier les incidents de sécurité détectés
- Rédiger des règles de détection et maintenir un catalogue d'indicateurs de compromission à partir de la connaissance des modes opératoires adverses
- Mener une investigation inforensique et une analyse dynamique de code malveillant en garantissant l'intégrité des preuves

- Capitaliser le résultat des investigations et concevoir des actions de formation et d'entraînement des équipes

02 · FIL ROUGE PÉDAGOGIQUE

Valcorde Systèmes de Défense

CF

Camille Ferrand

Référente cybersécurité promue Responsable en cybersécurité, rattachée au RSSI

Industrie de défense : conception et maintien en condition opérationnelle de systèmes de communication et de commandement pour les forces armées

Valcorde Systèmes de Défense est une entreprise de taille intermédiaire implantée à Brest et à Toulon, qui conçoit et maintient des systèmes de communication embarqués et des infrastructures réseau pour des unités militaires. Elle héberge des données sensibles, gère un réseau industriel sur ses sites de production et doit faire homologuer plusieurs systèmes d'information. Après une tentative d'hameçonnage ciblé visant son bureau d'études, la direction décide de structurer sa cybersécurité : renforcement de la gouvernance, campagne d'audits, montée en puissance de son centre de supervision interne et création d'une capacité d'investigation numérique. Camille Ferrand, ancienne technicienne veilleuse de cybersécurité, est nommée Responsable en cybersécurité. Elle travaille aux côtés de Bertrand Lemaire, RSSI, et encadre une petite équipe de quatre techniciens SOC.

Chaque cours se termine par une mise en situation dans cette entreprise : l'apprenant accompagne Camille dans des situations professionnelles réalistes, de plus en plus complexes, jusqu'à la préparation des épreuves.

La progression

1. Bloc 1 : Camille structure la gouvernance cyber de Valcorde, conduit l'analyse des risques du bureau d'études, prépare l'homologation du réseau de production et durcit l'administration des systèmes.
2. Bloc 2 : Camille pilote la campagne d'audit du site de Toulon, réalise un test d'intrusion sur l'extranet client et présente un plan de remédiation au comité de direction.
3. Bloc 3 : Camille prend la tête du centre de supervision, enrichit les règles de détection face à un mode opératoire adverse identifié et dirige la réponse à un incident de rançongiciel.
4. Bloc 4 : Camille mène l'investigation inforensique de l'incident, analyse le code malveillant en environnement isolé et capitalise les enseignements dans un retour d'expérience partagé avec les partenaires.

03 · ARCHITECTURE

Organisation du parcours

Le parcours est construit sur les blocs de compétences du référentiel officiel : chaque bloc regroupe les cours qui préparent à son évaluation.

N°	Bloc et cours	Durée
RNCP37300BC01 · Piloter la cyberprotection des systèmes et réseaux informatiques		**132 h**
1	Gouvernance de la cybersécurité et appui au RSSI et au DSI	22 h
2	Analyse des risques et préparation à l'homologation	22 h
3	Sensibilisation et développement des compétences cyber des utilisateurs et des administrateurs	22 h
4	Veille technologique et évaluation de la sécurité technique du SI	22 h
5	Sécurisation des architectures, administration sécurisée et chiffrement	22 h
6	Journalisation et lutte informatique défensive de premier niveau	22 h
RNCP37300BC02 · Contrôler et auditer le niveau de cybersécurité d'un système d'information		**110 h**
7	Référentiels et méthodologie de l'audit de sécurité	22 h
8	Audit technique d'un système d'information	22 h
9	Tests d'intrusion	22 h
10	Rapport d'audit, non-conformités et plan d'action	22 h
11	Remédiation technique, sécurité applicative et restitution d'audit	22 h
RNCP37300BC03 · Superviser la cybersécurité des systèmes d'information		**110 h**
12	Organisation et pilotage d'un centre de supervision	22 h
13	Chasse aux menaces et qualification des incidents	22 h
14	Ingénierie de détection et connaissance de la menace	22 h
15	Pilotage de la réponse à incident dans un centre de supervision	22 h
16	Formation et entraînement des équipes de supervision	22 h
RNCP37300BC04 · Conduire une investigation numérique dans le domaine de la cybersécurité		**88 h**
17	Collecte et préservation des preuves numériques	22 h
18	Analyse inforensique post mortem	22 h
19	Analyse de codes malveillants et évaluation des impacts	22 h
20	Capitalisation, retour d'expérience et renforcement durable	22 h
Total du parcours		**440 h**

Répartition des modalités pédagogiques

Chaque sous-chapitre s'ouvre sur une vidéo de 3 à 5 minutes. La vidéo représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies, des études de cas, des mises en situation et des QCM.



- Vidéos : 132 h
- Cours texte et infographies : 138 h 30
- Études de cas et mises en situation : 108 h
- QCM et évaluations : 61 h 30

04 · PROGRAMME DÉTAILLÉ

Contenu des cours

RNCP37300BC01 · 132 h

Piloter la cyberprotection des systèmes et réseaux informatiques

Cours 1 · Gouvernance de la cybersécurité et appui au RSSI et au DSI

22 h

OBJECTIFS

- Contribuer à l'élaboration des moyens et procédures cyber au profit des autorités qualifiées et d'emploi
- Rédiger les documents réglementaires d'organisation et de conduite de la cybersécurité d'une entité
- Organiser, conduire et contrôler la mise en œuvre des mesures locales et conseiller la direction

ÉVALUATION FORMATIVE

QCM de validation des acquis et rédaction commentée d'une procédure de sécurité locale

CONTENUS

- Organisation de la cybersécurité : rôles du RSSI, du DSI, des autorités qualifiées et des autorités d'emploi
- Cadre réglementaire et normatif : protection des informations sensibles, PSSI, référentiels de l'ANSSI, famille ISO 27000
- Rédiger une politique de sécurité et ses documents d'application
- Décliner et contrôler les mesures locales de cybersécurité
- Tableaux de bord et indicateurs de pilotage de la cyberprotection
- Conseiller la direction : formuler une recommandation et un arbitrage de cyberprotection

Fil rouge · Bertrand Lemaire confie à Camille la refonte de la PSSI de Valcorde : elle doit rédiger les procédures applicables au site de Brest et présenter au directeur général trois actions prioritaires de cyberprotection.

Cours 2 · Analyse des risques et préparation à l'homologation

22 h

OBJECTIFS

- Conduire l'analyse des risques pesant sur un périmètre informatique défini
- Préparer une unité à l'homologation ou au contrôle d'un système d'information
- Évaluer et rendre compte du niveau de sécurité organisationnel du périmètre

ÉVALUATION FORMATIVE

Étude de cas notée : analyse de risques simplifiée et plan de préparation à l'homologation

CONTENUS

- Fondamentaux de la gestion des risques numériques
- Méthode EBIOS Risk Manager : ateliers, sources de risque, scénarios stratégiques et opérationnels
- Traitement du risque et risques résiduels
- Démarche d'homologation : acteurs, dossier, décision et suivi
- Préparer un contrôle ou une inspection de sécurité
- Évaluer le niveau de sécurité organisationnel et en rendre compte

Fil rouge · Le réseau de production de Toulon doit être homologué avant la livraison d'un système à un client militaire : Camille anime les ateliers EBIOS RM et constitue le dossier d'homologation.

Cours 3 · Sensibilisation et développement des compétences cyber des utilisateurs et des administrateurs

22 h

OBJECTIFS

- Concevoir et animer des séances de sensibilisation adaptées aux utilisateurs et aux administrateurs
- Construire un plan de développement des compétences en cybersécurité

ÉVALUATION FORMATIVE

Conception d'un déroulé de séance de sensibilisation et QCM

CONTENUS

- Facteur humain et ingénierie sociale : comprendre les comportements à risque
- Identifier les besoins de sensibilisation selon les publics
- Concevoir une séance de sensibilisation : objectifs, supports, messages clés
- Animer une séance et gérer un groupe
- Campagnes de simulation d'hameçonnage : conception, éthique et exploitation
- Plan de montée en compétences des administrateurs
- Mesurer l'efficacité des actions de sensibilisation

Fil rouge · Suite à la tentative d'hameçonnage visant le bureau d'études, Camille conçoit une séance de sensibilisation pour les ingénieurs et un parcours de bonnes pratiques pour les administrateurs.

Cours 4 · Veille technologique et évaluation de la sécurité technique du SI

22 h

OBJECTIFS

- Assurer une veille technologique et le suivi des études amont du domaine cyber
- Anticiper et proposer les nouveaux besoins cyber de son périmètre
- Évaluer et rendre compte du niveau de sécurité technique du périmètre

ÉVALUATION FORMATIVE

Note de synthèse de veille évaluée sur grille et QCM

CONTENUS

- Organiser une veille : sources institutionnelles, bulletins CERT, publications techniques, études amont
- Outils de collecte, de tri et de diffusion de la veille
- Traduire la veille en besoins cyber pour son périmètre
- Cartographie technique du SI et inventaire des actifs
- Indicateurs et outils d'évaluation de la sécurité technique
- Rendre compte : note de synthèse technique à destination du RSSI

Fil rouge · Camille met en place une veille hebdomadaire pour Valcorde et propose au RSSI une évolution de la protection des postes du bureau d'études à la suite d'une vulnérabilité critique publiée.

Cours 5 · Sécurisation des architectures, administration sécurisée et chiffrement

22 h

OBJECTIFS

- Proposer ou développer les outils et procédures de sécurisation des architectures réseaux et des services associés
- Définir et appliquer les règles d'administration sécurisée et la politique de gestion des droits d'accès
- Proposer des solutions de chiffrement adaptées au niveau de sécurité attendu

ÉVALUATION FORMATIVE

Mise en situation sur laboratoire virtuel : durcissement d'une configuration et justification écrite des choix

CONTENUS

- Principes de sécurisation des architectures : cloisonnement, défense en profondeur, filtrage
- Durcissement des systèmes et des éléments actifs réseau
- Administration sécurisée : postes dédiés, bastions, recommandations de l'ANSSI
- Gestion des identités et des droits d'accès : moindre privilège, revues de droits, comptes à privilèges
- Fondamentaux de la cryptographie : symétrique, asymétrique, fonctions de hachage, PKI
- Choisir une solution de chiffrement selon la sensibilité des données
- Automatiser et documenter les procédures de sécurisation

Fil rouge · Camille redéfinit l'architecture d'administration du réseau de Toulon, met en place une politique de droits d'accès et recommande une solution de chiffrement pour les échanges avec les clients militaires.

Cours 6 · Journalisation et lutte informatique défensive de premier niveau

22 h

OBJECTIFS

- Exploiter et préserver les journaux d'événements des systèmes
- Appliquer les mesures prioritaires de lutte informatique défensive et apporter un soutien technique à la résolution d'incident
- Établir et diffuser un compte rendu d'incident précis

ÉVALUATION FORMATIVE

Étude de cas chronométrée : analyse de journaux et rédaction d'un compte rendu d'incident

CONTENUS

- Politique de journalisation : sources, rétention, horodatage, intégrité
- Centraliser et exploiter les journaux
- Organisation et processus de lutte informatique défensive
- Mesures prioritaires en réaction à un incident : confinement, isolement, sauvegarde des éléments
- Soutien technique aux équipes de résolution
- Rédiger et diffuser un compte rendu d'incident

Fil rouge · Un poste du bureau d'études présente un comportement suspect : Camille exploite les journaux, applique les premières mesures de confinement et rédige le compte rendu transmis au RSSI.

RNCP37300BC02 · 110 h

Contrôler et auditer le niveau de cybersécurité d'un système d'information

Cours 7 · Référentiels et méthodologie de l'audit de sécurité

22 h

OBJECTIFS

- Constituer et maintenir à jour les référentiels techniques et organisationnels d'audit
- Assurer une veille active sur les risques pesant sur les systèmes audités
- Mener une investigation liée à l'environnement organisationnel d'un SI

ÉVALUATION FORMATIVE

Construction d'une grille d'audit et QCM

CONTENUS

- Typologie des audits : organisationnel, architecture, configuration, code, intrusion
- Référentiels d'audit : normes, guides de l'ANSSI, référentiels internes
- Construire et maintenir une grille d'audit
- Cadrage d'une mission : convention, périmètre, règles d'engagement
- Veille sur les risques et les vulnérabilités applicables au périmètre audité
- Audit organisationnel : entretiens, revue documentaire, collecte de preuves

Fil rouge · La direction mandate Camille pour auditer le site de Toulon : elle construit le référentiel d'audit et conduit les entretiens avec les responsables d'exploitation.

Cours 8 · Audit technique d'un système d'information

22 h

OBJECTIFS

- Mener seul ou en équipe une investigation technique sur un périmètre défini et son environnement
- Conduire sur plateforme des tests et études de produits de sécurité

ÉVALUATION FORMATIVE

Mise en situation en laboratoire : audit de configuration et relevé de constats

CONTENUS

- Audit d'architecture : flux, cloisonnement, points d'interconnexion
- Audit de configuration des systèmes et des équipements réseau
- Outils de scan de vulnérabilités et d'analyse de configuration
- Investigation sur l'environnement technique : sites, sous-traitants, interconnexions
- Tests et évaluations de produits de sécurité sur plateforme
- Conduire un audit en équipe : répartition, coordination, traçabilité

Fil rouge · Camille et deux techniciens auditent la configuration des pare-feu et des serveurs du site de Toulon, puis testent sur plateforme une sonde de détection envisagée par le RSSI.

Cours 9 · Tests d'intrusion

22 h

OBJECTIFS

- Réaliser un test d'intrusion sur un système informatique dans un cadre légal et contractuel
- Rédiger un rapport de test d'intrusion technique

ÉVALUATION FORMATIVE

Exercice pratique en laboratoire isolé et rapport de test d'intrusion évalué

CONTENUS

- Cadre juridique et éthique du test d'intrusion
- Méthodologie : reconnaissance, énumération, exploitation, post exploitation
- Tests d'intrusion sur infrastructures et annuaires
- Tests d'intrusion sur applications web
- Cotation des vulnérabilités et preuves d'exploitation
- Structure et rédaction d'un rapport de test d'intrusion

Fil rouge · Camille réalise un test d'intrusion autorisé sur l'extranet client de Valcorde et documente une chaîne d'exploitation permettant d'accéder à des données de projet.

Cours 10 · Rapport d'audit, non-conformités et plan d'action

22 h

OBJECTIFS

- Élaborer les synthèses et rédiger les rapports d'audit et de contrôle
- Identifier et formaliser les non-conformités au regard d'un référentiel défini
- Proposer les évolutions de mise en conformité et concevoir les tableaux de suivi

ÉVALUATION FORMATIVE

Rédaction d'une synthèse d'audit et d'un tableau de suivi évalués sur grille

CONTENUS

- Qualifier un constat et formaliser une non-conformité
- Hiérarchiser les écarts selon le risque
- Rédiger un rapport d'audit : synthèse managériale et détail technique
- Construire un plan d'action de mise en conformité
- Concevoir un tableau de suivi des actions : responsables, échéances, indicateurs
- Suivre et clôturer les actions après audit

Fil rouge · À partir des constats de Toulon, Camille rédige le rapport d'audit, formalise douze non-conformités et livre au RSSI un tableau de suivi des actions.

Cours 11 · Remédiation technique, sécurité applicative et restitution d'audit

22 h

OBJECTIFS

- Proposer des évolutions de code et de configuration pour accroître le niveau de sécurité
- Communiquer et argumenter de manière adaptée selon l'interlocuteur

ÉVALUATION FORMATIVE

Oral simulé de restitution d'audit et exercice de correction de code

CONTENUS

- Vulnérabilités applicatives courantes et bonnes pratiques de développement sécurisé
- Proposer des corrections de code et des revues de sécurité
- Évolutions de paramétrage et de configuration des équipements
- Prioriser la remédiation selon le coût et le risque
- Préparer une restitution adaptée : direction, équipes techniques, développeurs
- Argumenter et gérer les objections

Fil rouge · Camille présente le plan de remédiation au comité de direction puis accompagne l'équipe de développement de l'extranet dans la correction des failles identifiées.

RNCP37300BC03 · 110 h

Superviser la cybersécurité des systèmes d'information

Cours 12 · Organisation et pilotage d'un centre de supervision

22 h

OBJECTIFS

- Exploiter des systèmes de cybersurveillance et de détection d'événements de sécurité
- Diriger l'action d'une équipe de techniciens et compléter leurs travaux

ÉVALUATION FORMATIVE

QCM et étude de cas sur l'organisation d'une équipe de supervision

CONTENUS

- Missions et organisation d'un SOC : niveaux d'analyse, rotations, interfaces
- Architecture de détection : SIEM, sondes réseau, EDR
- Exploiter une console de supervision au quotidien
- Répartir la charge et piloter l'activité de l'équipe
- Contrôler et compléter les analyses des techniciens
- Indicateurs de performance d'un centre de supervision

Fil rouge · Camille prend la responsabilité du SOC interne de Valcorde : elle réorganise les rotations des quatre techniciens et met en place une revue quotidienne des alertes.

Cours 13 · Chasse aux menaces et qualification des incidents

22 h

OBJECTIFS

- Conduire une recherche des éléments précurseurs d'une agression informatique
- Interpréter les détections et croiser les constats pour qualifier un incident

ÉVALUATION FORMATIVE

Exercice de qualification sur jeu de données d'alertes

CONTENUS

- Chaîne d'attaque et signaux précurseurs
- Démarche de chasse aux menaces fondée sur des hypothèses
- Interpréter une alerte : contexte, faux positifs, priorisation
- Croiser les constats avec d'autres sources d'information
- Qualifier un incident : gravité, périmètre, urgence
- Documenter une qualification d'incident

Fil rouge · Plusieurs connexions inhabituelles vers l'extérieur sont relevées la nuit : Camille mène une recherche de précurseurs, croise les journaux avec des sources de renseignement et qualifie l'incident.

Cours 14 · Ingénierie de détection et connaissance de la menace

22 h

OBJECTIFS

- Réaliser une veille sur les menaces et les vulnérabilités et caractériser les modes opératoires adverses
- Rédiger des règles de détection et maintenir le catalogue des indicateurs de compromission

ÉVALUATION FORMATIVE

Rédaction et test de règles de détection en laboratoire

CONTENUS

- Renseignement sur la menace : sources, niveaux stratégique, opérationnel et tactique
- Modes opératoires d'attaquants et cadre MITRE ATT&CK
- Indicateurs de compromission : types, durée de vie, qualité
- Rédiger des règles de détection : signatures, corrélations, formats Sigma et YARA
- Tester et ajuster une règle de détection
- Maintenir un catalogue d'indicateurs de compromission

Fil rouge · Un bulletin signale un mode opératoire ciblant l'industrie de défense : Camille l'analyse, rédige trois règles de détection et met à jour le catalogue d'indicateurs du SOC.

Cours 15 · Pilotage de la réponse à incident dans un centre de supervision

22 h

OBJECTIFS

- Faire appliquer les procédures de réaction, d'alerte et les ordres techniques de lutte informatique défensive
- Caractériser la menace et préserver les traces et preuves
- Transmettre de façon rigoureuse les éléments aux analystes et aux organismes tiers

ÉVALUATION FORMATIVE

Exercice de gestion de crise simulée avec débriefing

CONTENUS

- Cycle de réponse à incident : préparation, détection, confinement, éradication, rétablissement
- Procédures de réaction et d'alerte
- Faire appliquer les ordres techniques de lutte informatique défensive
- Caractériser la menace pendant la crise
- Préserver les traces et les preuves pendant la réponse
- Transmettre les éléments aux analystes et aux organismes tiers
- Communication et coordination en situation de crise

Fil rouge · Un rançongiciel chiffre plusieurs serveurs du site de Brest : Camille déclenche les procédures d'alerte, dirige le confinement, préserve les preuves et transmet les éléments aux autorités compétentes.

Cours 16 · Formation et entraînement des équipes de supervision

22 h

OBJECTIFS

- Concevoir et rédiger des scénarios d'entraînement adaptés aux équipes de supervision
- Former et évaluer les techniciens et opérateurs du centre de supervision

ÉVALUATION FORMATIVE

Conception d'un scénario d'entraînement et d'une grille d'évaluation

CONTENUS

- Analyse des besoins de formation d'une équipe SOC
- Concevoir un scénario d'entraînement : objectifs, injections, critères de réussite
- Exercices sur plateforme et entraînements sur table
- Animer une séquence de formation technique
- Évaluer les compétences : grilles, observations, retours
- Construire un plan de progression individuel

Fil rouge · Après l'incident, Camille conçoit un scénario d'entraînement inspiré de l'attaque subie, l'anime avec son équipe et évalue chaque technicien.

RNCP37300BC04 · 88 h

Conduire une investigation numérique dans le domaine de la cybersécurité

Cours 17 · Collecte et préservation des preuves numériques

22 h

OBJECTIFS

- Exploiter les éléments recueillis par des sondes de supervision des réseaux
- Collecter les traces, codes et preuves en garantissant leur intégrité et leur recevabilité juridique

ÉVALUATION FORMATIVE

Travaux pratiques de collecte en laboratoire et QCM juridique

CONTENUS

- Cadre juridique de la preuve numérique
- Exploiter les données des sondes gouvernementales et commerciales
- Ordre de volatilité et stratégie de collecte
- Acquisition de mémoire vive et de supports
- Intégrité des preuves : empreintes, scellés numériques
- Chaîne de traçabilité et documentation de la collecte

Fil rouge · Camille organise la collecte sur les serveurs chiffrés de Brest : acquisition mémoire, copies de disques, calcul d'empreintes et tenue du registre de traçabilité.

Cours 18 · Analyse inforensique post mortem

22 h

OBJECTIFS

- Réaliser l'analyse post mortem d'un système ayant subi un incident
- Analyser les traces et preuves collectées pour reconstituer l'incident

ÉVALUATION FORMATIVE

Étude de cas inforensique sur image disque fournie

CONTENUS

- Démarche d'analyse inforensique
- Artefacts des systèmes Windows et Linux
- Analyse de la mémoire vive
- Analyse des journaux et des traces réseau
- Reconstitution d'une chronologie d'attaque
- Outils d'analyse inforensique et validation des résultats

Fil rouge · Camille reconstitue la chronologie de l'attaque : premier accès par un compte VPN compromis, mouvement latéral, puis déploiement du rançongiciel.

Cours 19 · Analyse de codes malveillants et évaluation des impacts

22 h

OBJECTIFS

- Réaliser une analyse dynamique d'un code malveillant dans un environnement sécurisé
- Déterminer les stratégies d'attaque et de propagation
- Évaluer les impacts avérés et potentiels en tenant compte de contextes sensibles

ÉVALUATION FORMATIVE

Rapport d'analyse dynamique évalué sur grille

CONTENUS

- Familles de codes malveillants et techniques d'évasion
- Mettre en place un environnement d'analyse isolé
- Analyse statique de premier niveau
- Analyse dynamique : comportement, persistance, communications
- Identifier les mécanismes de propagation
- Évaluer les impacts : données, opérations, partenaires, contexte de défense

Fil rouge · Camille analyse l'échantillon de rançongiciel dans un laboratoire isolé, identifie son mécanisme de propagation et évalue l'exposition des données de programmes classés.

Cours 20 · Capitalisation, retour d'expérience et renforcement durable

22 h

OBJECTIFS

- Rédiger et transmettre les rapports d'incident et d'analyse
- Construire un référentiel de retour d'expérience et maintenir les bases d'indicateurs de compromission
- Proposer des solutions de renforcement à long terme

ÉVALUATION FORMATIVE

Rapport d'incident complet et soutenance simulée devant un jury fictif

CONTENUS

- Rédiger un rapport d'incident et d'analyse selon le destinataire
- Transmettre et partager l'information de façon maîtrisée
- Conduire un retour d'expérience
- Construire un référentiel de connaissances exploitable
- Maintenir les bases d'indicateurs de compromission
- Élaborer une feuille de route de renforcement à long terme
- Synthèse du parcours : du pilotage à l'investigation

Fil rouge · Camille rédige le rapport final de l'incident, anime le retour d'expérience avec la direction et propose une feuille de route de sécurité sur trois ans pour Valcorde.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

Correspondance entre les compétences du référentiel France Compétences et les cours du parcours.

Compétence	Bloc	Cours
Contribuer à l'élaboration des moyens et procédures cyber	RNCP37300BC01	1
Concourir à la rédaction des documents réglementaires de cybersécurité	RNCP37300BC01	1
Organiser, conduire et contrôler les mesures locales cyber	RNCP37300BC01	1
Préparer son unité à une homologation ou un contrôle	RNCP37300BC01	2
Évaluer et rendre compte du niveau de sécurité organisationnel	RNCP37300BC01	2
Conduire l'analyse des risques d'un périmètre	RNCP37300BC01	2
Réaliser et animer des séances de sensibilisation	RNCP37300BC01	3
Conseiller le directeur de l'entité sur la cyberprotection	RNCP37300BC01	1
Assurer une veille technologique et le suivi des études amont	RNCP37300BC01	4
Anticiper et proposer les nouveaux besoins cyber	RNCP37300BC01	4
Évaluer et rendre compte du niveau de sécurité technique	RNCP37300BC01	4
Développer les compétences cyber des administrateurs et utilisateurs	RNCP37300BC01	3
Proposer les solutions de chiffrement adaptées	RNCP37300BC01	5
Proposer ou développer les outils et procédures de sécurisation des architectures réseaux	RNCP37300BC01	5
Définir et mettre en œuvre les règles et outils d'administration sécurisés	RNCP37300BC01	5
Définir et appliquer la politique de gestion des droits d'accès	RNCP37300BC01	5
Exploiter et préserver les journaux d'événements	RNCP37300BC01	6
Appliquer les mesures prioritaires de lutte informatique défensive	RNCP37300BC01	6
Établir et diffuser un compte rendu d'incident	RNCP37300BC01	6
Apporter un soutien technique à la résolution des incidents	RNCP37300BC01	6
Concourir aux processus de lutte informatique défensive	RNCP37300BC01	6
Constituer et maintenir les référentiels d'audit	RNCP37300BC02	7
Assurer une veille active sur les risques pesant sur les systèmes	RNCP37300BC02	7
Mener une investigation technique sur un périmètre défini	RNCP37300BC02	8
Mener une investigation liée à l'environnement technique du SI	RNCP37300BC02	8
Mener une investigation liée à l'environnement organisationnel du SI	RNCP37300BC02	7
Conduire sur plateforme des tests de produits de sécurité	RNCP37300BC02	8
Élaborer les synthèses et rédiger les rapports d'audit	RNCP37300BC02	10
Réaliser des tests d'intrusion	RNCP37300BC02	9
Rédiger un rapport de test d'intrusion	RNCP37300BC02	9
Identifier et formaliser les non-conformités	RNCP37300BC02	10
Proposer les évolutions de mise en conformité	RNCP37300BC02	10
Concevoir les tableaux de suivi des actions post audit	RNCP37300BC02	10
Proposer les évolutions de code pour la sécurité applicative	RNCP37300BC02	11
Proposer des évolutions de paramétrage et de configuration	RNCP37300BC02	11
Communiquer et argumenter selon l'interlocuteur	RNCP37300BC02	11
Exploiter des systèmes de cybersurveillance et de détection	RNCP37300BC03	12

Rechercher les éléments précurseurs d'une agression	RNCP37300BC03	13
Interpréter les détections pour qualifier un incident	RNCP37300BC03	13
Compléter les travaux des techniciens en cybersécurité	RNCP37300BC03	12
Croiser les constats avec d'autres sources	RNCP37300BC03	13
Réaliser une veille sur les menaces et vulnérabilités	RNCP37300BC03	14
Rédiger des règles de détection	RNCP37300BC03	14
Maintenir le catalogue des indicateurs de compromission	RNCP37300BC03	14
Caractériser la menace à partir des modes opératoires adverses	RNCP37300BC03	14
Faire appliquer les procédures de réaction et d'alerte	RNCP37300BC03	15
Faire appliquer les ordres techniques de lutte informatique défensive	RNCP37300BC03	15
Caractériser la menace cyber	RNCP37300BC03	15
Transmettre les éléments pertinents aux organismes tiers	RNCP37300BC03	15
Préserver les traces et preuves à des fins d'analyse	RNCP37300BC03	15
Transmettre les éléments de façon rigoureuse aux analystes	RNCP37300BC03	15
Concevoir et rédiger des scénarios d'entraînement	RNCP37300BC03	16
Former les techniciens et opérateurs du centre de supervision	RNCP37300BC03	16
Évaluer les techniciens et opérateurs du centre de supervision	RNCP37300BC03	16
Exploiter les éléments des sondes de supervision des réseaux	RNCP37300BC04	17
Collecter les traces, codes et preuves lors d'un incident	RNCP37300BC04	17
Réaliser l'analyse post mortem (inforensique) d'un système	RNCP37300BC04	18
Analyser les traces, codes et preuves collectés	RNCP37300BC04	18
Garantir la préservation et l'intégrité juridique des éléments collectés	RNCP37300BC04	17
Réaliser une analyse dynamique d'un code malveillant	RNCP37300BC04	19
Évaluer les impacts avérés et potentiels d'incidents	RNCP37300BC04	19
Déterminer les stratégies d'attaque et de propagation	RNCP37300BC04	19
Construire et capitaliser un référentiel de retour d'expérience	RNCP37300BC04	20
Rédiger et transmettre les rapports d'incident et d'analyse	RNCP37300BC04	20
Proposer des solutions de renforcement à long terme	RNCP37300BC04	20
Maintenir les bases de connaissances des indicateurs de compromission	RNCP37300BC04	20

Évaluations formatives

Chaque cours intègre des évaluations formatives régulières : QCM de fin de sous-chapitre avec correction commentée, études de cas, exercices pratiques sur laboratoire virtuel isolé et productions écrites (procédures, rapports, règles de détection) évaluées sur grille critériée. Les mises en situation du fil rouge Valcorde Systèmes de Défense placent l'apprenant face aux décisions réelles du métier et lui permettent de mesurer sa progression. Les résultats sont tracés sur la plateforme, ce qui permet à l'organisme de formation d'assurer le suivi individuel, d'identifier les besoins de remédiation et de documenter les acquis conformément aux exigences Qualiopi.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP37300BC01	Par la voie de la formation : épreuves écrites et orales, mises en situation professionnelles. Par la voie de la VAE : étude du livret 2 et entretien avec le jury. Ces épreuves visent à démontrer la capacité du candidat à assurer la gouvernance de la sécurité des systèmes et réseaux informatiques.
RNCP37300BC02	Par la voie de la formation : épreuves écrites et orales, mises en situation professionnelles. Par la voie de la VAE : étude du livret 2 et entretien avec le jury. Ces épreuves visent à démontrer la capacité du candidat à évaluer et identifier les non-conformités et les vulnérabilités d'un système d'information et à proposer un plan de remédiation.

RNCP37300BC03	Par la voie de la formation : épreuves écrites et orales, mises en situation professionnelles. Par la voie de la VAE : étude du livret 2 et entretien avec le jury. Ces épreuves visent à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience à la suite d'un incident cyber.
RNCP37300BC04	Par la voie de la formation : épreuves écrites et orales, mises en situation professionnelles. Par la voie de la VAE : étude du livret 2 et entretien avec le jury. Ces épreuves visent à démontrer la capacité du candidat à caractériser une attaque et à adapter sa stratégie de gestion de crise en fonction des retours d'expérience.

Le parcours reproduit les formats des épreuves officielles : rédactions techniques et de synthèse pour préparer les épreuves écrites, restitutions et soutenances simulées pour les épreuves orales, exercices pratiques et gestion de crise simulée pour les mises en situation professionnelles. Le fil rouge fournit à l'apprenant un corpus cohérent de productions (analyse de risques, rapport d'audit, rapport de test d'intrusion, règles de détection, rapport d'incident) qu'il peut mobiliser pour s'entraîner. School For Mate fournit le contenu pédagogique : l'organisme de formation reste seul responsable de l'inscription des candidats, de l'organisation des épreuves et de la relation avec le certificateur, le ministère des Armées, dans le respect des conditions d'accès fixées par celui-ci.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning accessible en continu, avec suivi de progression et traçabilité des activités pour l'organisme de formation
- Une capsule vidéo de 3 à 5 minutes par sous-chapitre, le format vidéo représentant 30 % du volume horaire du parcours
- Cours texte enrichis, infographies et fiches de synthèse téléchargeables
- Études de cas et mises en situation professionnelles construites autour du fil rouge Valcorde Systèmes de Défense
- Laboratoires virtuels isolés pour les exercices de durcissement, d'audit, de test d'intrusion, de détection et d'inforensique
- QCM et grilles d'évaluation critériées pour chaque cours
- Modèles de documents professionnels : procédures, dossier d'homologation, rapport d'audit, rapport de test d'intrusion, rapport d'incident

Débouchés et évolutions

- Superviseur ou analyste cyberdéfense au sein du ministère des Armées
- Auditeur de systèmes d'information ou contrôleur en cyberprotection
- Responsable du SOC (Security Operation Center)
- Responsable du CSIRT (Computer Security Incident Response Team)
- Analyste réponse aux incidents de sécurité ou analyste de la menace cybersécurité
- Responsable de la cybersécurité et de la gestion de crise

Accessibilité

Contenus sous-titrés en français, contrastes conformes WCAG AA, navigation au clavier sur les écrans interactifs. L'organisme de formation qui diffuse le parcours adapte les modalités d'accompagnement aux personnes en situation de handicap avec son référent handicap.

Livrables fournis à l'organisme de formation

- Package SCORM 1.2 / 2004 et xAPI, compatible avec les principaux LMS
- Sources éditables des cours, scripts vidéo et banques de QCM
- Livret apprenant et grilles d'évaluation
- Licence marque blanche à vie, stagiaires illimités, maintenance 24 mois

School For Mate
On crée vos formations, vous n'avez plus qu'à les diffuser.
contact@schoolformate.com · catalogue-2026-sfm.netlify.app

Référentiel RNCP37300 consulté sur francecompetences.fr (export officiel du 4 novembre 2026). La délivrance de la certification relève exclusivement du certificateur et de l'organisme de formation habilité. Document non contractuel, susceptible d'évoluer avec le référentiel.