Analyste et gestionnaire de la cybersécurité des systèmes industriels et urbains (CRISIS)

Intitulé officiel : Licence professionnelle Sciences, technologies, santé mention Métiers de l'informatique : administration et sécurité des systèmes et des réseaux parcours Cybersécurité et réponse à incident pour les systèmes d'information, indust. et urbains (CRISIS)

Présentation

Publics / conditions d'accès

- Être titulaire d'un diplôme de niveau 5 en informatique : BTS SN, SIO, FED ;
- DUT 2ième année ou BUT informatique, GEII ;
- DPCT informatique ; diplôme analyste programmeur du Cnam ;
- certains titres Afpa homologués au niveau 5.
- Être titulaire d'un diplôme qui dispense des niveaux L1 et L2.

Objectifs

L'objectif de la formation est de former des spécialistes en cyber sécurité en mesure de comprendre et d'intervenir sur les infrastructures IT/OT/IoT/IIoT d'opérateurs d'importance vitale (OIV).

Ces infrastructures sont complexes, elles concernent tout aussi bien les capteurs (Cyber Physiqical Systems) en lien direct avec les entités physiques (vannes, ...), les automates (PLC,...) pour réaliser des opérations techniques, et enfin, plus global, le shysteme de contrôle et d'acquisition des données (SCADA)destiné au controle de tous ces équipements et des processus métier. Les SCADA collectent également les données relevées par les netités physiques, en temps réel, même auprès de sites distants.

Ces infrastructures sont sujettes à de nombreuses vulnérabilités, il n'est pas toujours possible de réaliser des mises à jour sur les installations en production continue ou encore en dehors des fenetres de maintenance dont le cycle est parfois de deux ans ! Par ailleurs, la cybersécurité n'a pas été pensée dès la conception, d'autant que les pièces informatiques ont été intégrées plus tard. Pendant longtemps, la cybersécurité de ces ensembles informatiques et physiques ont concerné les grands groupes industriels, avec la transformation numérique, ce sont les petites et moyennes entreprises du secteur de l'industrie qui deviennent exposées aux cyberattaques.

Selon l'ANSSI, le maintien des conditions de sécurité des systèmes industriels et urbains est une condition majeure du maintien de la sécurité globale, de notre pays mais également au niveau mondial, ces systèmes industriels sont actuellement la cible de nombreuses attaques informatiques.

Modalités de validation

Devoir final avec jury, contrôle continu par matière avec examen sur table, projet, mise en situation simulée, évaluation individuelle écrite et orale.

Travaux pratiques notés.

Mise en situation simulée d'une cyberattaque sur une ligne de production fonctionnelle equipée de composants industriels (PLC, IoT,....).

Compétences

La déployabilité du cursus est soumise à validation avec la présence et l'agrément

Mis à jour le 15-10-2024

Arrêté du 13 mai 2025. Accréditation jusque fin 2029-2030. le 13-05-2025

Fin d'accréditation au 31-08-2030

Code : LP15401A

60 crédits

Licence professionnelle

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Niveau CEC d'entrée requis : Niveau 5 (ex Niveau III)

Niveau CEC de sortie : Niveau 6 (ex Niveau II)

Mention officielle : Arrêté du 13 mai 2025. Accréditation jusque fin 2029-2030.

Mode d'accès à la certification :

- Validation des Acquis de l'Expérience
- Formation continue
- Contrat de professionnalisation
- Apprentissage

NSF : Analyse informatique, conception d'architecture de réseaux (326n)

Métiers (ROME) : Analyste en cybersécurité (M1805)

Code répertoire : RNCP40102

Contact national :

EPN05 - Informatique
2 rue Conté
accès 33.1.13B
75003 Paris
01 40 27 28 21
Mmadi Hamida
hamida.mmadi@lecnam.net

d'un enseignant chercheur dans la responsabilité opérationnelle.

BLOC 1 : Maintien des conditions opérationnelles de sécurité (MCS) et gestion des incidents de sécurité des infrastructures IT OT IoT IIoT
(installer, configurer, superviser, développer)

- Participer à la supervision du MCS de moyens techniques en lien avec le RSSI, le CERT et le SOC
- Participer au traitement des incidents de sécurité en lien avec le SOC et le CERT
- Assurer la mise en place des techniques de sécurité (ségrégation réseau, mot de passe, patch management, droits d'accès physiques et logiques, ...) dans les systèmes informatiques virtualisés ou non (réseaux, postes de travail, serveurs, Active Directory,...) ou dans lesinfratsructures OT (operational technology) d'une entreprise (Automates industriels, Machines de maintenance, supervision SCADA, protocoles industriels, etc.).
- Assurer une veille technologique sur les menaces et techniques d'attaques (CERT, TTP,...) et spéicfiques aux systèmes industriels (CISA, ANSSI,...)
- Intervenir sur la sécurité des systèmes d'information de production ou de maintenance (GMAO/MES/ERP)
- Installer, intégrer, paramétrer des dispositifs de de collecte et de détection (sondes IDS, SIEM, EDR de type SentinelOne,...) dans les centres de sécurité opérationnelle (SOC) ou de supervision des OT
- Appliquer les bonnes pratiques selon les référentiels informatiques (ISO27002, RGS,...) ou industriels (CEI 61508, IEC 61508, ISO 26262,...)
- Réaliser des scripts d'automatisation sur les dispositifs de sécurité ou sécurisés
- Reprogrammer des automates (PLC,...) en respectant les critères de cybersécurité.

BLOC 2 : Analyse et audit de sécurité des infrastructures IT OT IoT IIoT
(Vérifier, corriger)

- Analyser les vulnérabilités des systemes informatiques à l'aide d'outils de gestion de vulnérabilités (Nessus Tenable,...)
- Analyser les codes malveillants
- Analyser les alertes cybersécurité, investiguer et effectuer le diagnostic technique de ces alertes
- Veiller à l'application
- Assurer une veille technologique sur les solutions de « sécurité »
- Participer à l'évaluation de conformité des systemes d'informatiques ou des projets de développemens (applications, réseaux, systèmes et données)au regard de normes globales en vigueur (NIST, ANSSI,...)
- Participer à l'élaboration des recommandations suite à un audit de sécurité (Mise en place de Firewall, VLAN)

BLOC 3 : Management de projet et conception d'architecture de sécurité de base de la sécurité des infrastructures IT OT IoT IIoT
(Planifier, diffuser, travailler en équipe, rédiger)

- Participer à la conception de projet en prenant en compte les exigences de sécurité spécifique (politique interne, classification des données, etc)
- Préparer et suivre les travaux de sécurisation
- Rédiger, analyser puis suivre les marchés liés aux missions de sécurité informatique des systèmes industriels,
- Participer à toutes les démarches visant à améliorer la sécurité des infrastructure IT ou OT.
- Participer à la définition des procédures qualité et documents internes (RGPD, charte informatique) et de sécurité en lien avec les IT/OT/IoT/IIoT.
- Recenser les besoins de sécurité des utilisateurs, assurer le suivi et proposer

des arbitrages (via ticketing, plateforme de pilotage),

- S'impliquer dans les projets en lien avec l'architecture du système d'information et la sécurité,
- Former les collaborateurs du service technique sur les matériels et logiciels choisis
- Aider dans le choix des solutions de sécurité matérielles et logicielles

Enseignements

60 ECTS

Modélisation et Ingénierie des systèmes : besoin, exigences, conception et architecture	USRS3N 4 ECTS
Système d'exploitation : principes, virtualisation, introduction aux automates et systèmes embarqués	USRS3P 4 ECTS
Réseaux et protocoles, réseaux industriels	USRS3Q 4 ECTS
Architectures SCADA et CPS	USRS3R 4 ECTS
Base de données et structures de données des SI, ERP, des systèmes industriels, SCADA et MES	USRS3S 4 ECTS
Développement, algorithmie, langages et programmation Java, Web	USRS3T 4 ECTS
Développement, algorithmie, langages et programmation d'automate, systèmes embarqués	USRS3U 4 ECTS
Analyse des enjeux principes, doctrines de sécurité : description de la menace, attaques, vulnérabilités	USRS3V 4 ECTS
Analyse de la menace, des attaques et des vulnérabilités des CPS et SCADA	USRS3W 4 ECTS
Dispositifs de sécurité : DMZ, Pare-feu, IDS, principes généraux et configuration du SI	USRS3X 4 ECTS
Dispositifs de sécurité appliqués au systèmes industriels et embarqués	USRS3Y 4 ECTS
Mathématiques générales et appliquées à l'algorithmie et la cryptographie	USRS3Z 4 ECTS
Anglais et SHS en anglais/français : compréhension écrite, géopolitique, droit et criminologie, éthiques	USRS40 2 ECTS
Projet et mémoire	UARS0R 10 ECTS

Blocs de compétences

Code, N° et intitulé du bloc	Liste de compétences
LP154B11 RNCP40102BC01 Usage numérique	-Utiliser les outils numériques de référence et oles règles de sécurité informatique pour acquérir, traiter, produire et diffuser l'information ainsi que pour collaborer en interne et en externe -Rédiger un sur une étude de cas pratique avec les outils de la bureautique -Utiliser les outils de planification pour la gestion des projets (par exemple Excel, MSProject,...) -Réaliser un ou plusieurs schémas d'architecture avec un outil informatique (par exemple visio, Powerpoint,...) -Rédiger en introduction des documents et rapports les règles de bonnes pratiques vis-à-vis de la propriété intellectuelle et industrielle, des éléments de sécurité constitutifs du document vis-à-vis des propriétés de vie privée, DIC, ainsi que les éléments de traçabilité du document (cycle de vie, archivage, ...) -Maîtriser les outils de navigation et de recherche vis-à-vis des questions de confidentialité
LP154B21 RNCP40102BC02 Exploitation de données à des fins d’analyse	-Identifier, sélectionner et analyser avec esprit critique diverses ressources dans son domaine de spécialité pour documenter un sujet et synthétiser ces données en vue de leur exploitation -Analyser et synthétiser des données en vue de leur exploitation -Développer une argumentation avec un esprit critique -Traduire de façon intelligible la nature du problème traité à l'aide des données issues du système d'information IT/OT -Identifier les données produites par les composants informatiques ainsi que leurs finalités (supervision, analyse, traçabilité, ...), on mettra à disposition des logs d'incident, de fonctionnement normal ou d'incident de sécurité pour chacune des typologies des composants informatiques (logs routeurs, pare feux, système d'exploitation, hardware, etc...) -Identifier les différents référentiels des équipementiers de sécurité (CISCO, Microsoft Windows, Active Directory, ...) et publics du domaine de la cybersécurité (CVE, ...) permettant l'analyse de ces données -Positionner les données dans le cycle de vie du processus étudié -Identifier le ou les phénomène(s) ayant produit des données, en particulier les données en lien avec la vulnérabilité et leurs évaluations -Restituer sous forme d'une synthèse les différents traitements statistiques effectués sur des données issues de ces composants à partir de jeux de données produits en lien avec un comportement ou un incident

	-Identifier la source des données analysées (internes ou ouvertes) -Présenter une vision synthétique du problème résolu (par exemple en présentant la situation avant et après phénomène) -Obtenir de l'information contradictoire sur des analyses obtenues à partir d'échanges avec des communautées d'expérience du domaine des IT/OT -Identifier des informations contradictoires d'une recherche bibliographique dans le champs disciplinaire
LP154B31 RNCP40102BC03 Expression et communication écrites et orales	-Se servir aisément des différents registres d'expression écrite et orale de la langue française -Communiquer par oral et écrit, de façon claire et non ambigüe, dans au moins une langue étrangère -Participer à des réunions de projet en langue anglaise -Résoudre un problème technique faisant appel à un support technique de niveau 3 en anglais -Rédiger un rapport d'incident de sécurité en anglais
LP154B41 RNCP40102BC04 Positionnement vis à vis d’un champ professionnel	-Identifier et situer les champs professionnels potentiellement en relation avec les acquis de la mention ainsi que les parcours possibles pour y accéder -Caractériser et valoriser son identité, ses compétences et son projet professionnel en fonction d'un contexte -Identifier le processus de production, de diffusion et de valorisation des savoirs -Connaître les différents composants informatiques d'un SI It (réseaux (TCPIP, HTTOS, SSL, ...), systèmes d'exploitation (MS, Linux, Android, ...) données, applications, SI), ainsi que leurs règlement de conception et d'assemblage, d'interprobabilité et d'architectures incluant leur fonctionnement et caractéristiques (normes, OSI X.200/IETF), client-serveur, WIFI (802,11), algorithme, ... -Connaître les différents composants d'une infrastructure pour les opérations techniques industrielles OT (réseaux (Modbys, ...), normes d'architectures et et d'interprobabilité (modèle de Péra, ISA99, ISA-95/IEC 62264, ...), programmation (Graphet, PLC), interafces IHM, ...) -Situer le champs de la cybersécurité en identifiant les différentes vulnérabilités d'un composant informatique et industriel lors des modes de conceptionou d'utilisation -Concevoir une architecture SIU à partir d'un cahier des charges -Concevoir une application informatique à partir d'un cahier des charges -Identifier les différents composants étudiés en C041

	-Restituer l'architecture IT/OT et ses composants, puis la rapprocher de l'une des normes abordées ou encore une nougvelle, qui sera expliquée -Installer et configurer les éléments d'une architecture -Tester l'inconnexion et les échanges de données -Lister les vulérabilités (surface d'exposition) corrigées ou à corriger
LP154B51 RNCP40102BC05 Action en responsabilité au sein d’une organisation professionnelle	-Situer son rôle et sa mission au au sein d'une organisation pour s'adapter et prendre des initiatives -Respecter les principes d'éthique, de déontologie et de responsabilité environnementale -Travailler en équipe et en réseau ainsi qu'en autonomie et responsabilité au service d'un projet -Analyser ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique -Relater une situation d'activité industrielle IT/OT en lien avec le métier de l'organisation (conception, fabrication ou logistique) -Décrire le processus lié à son organisation à l'aide d'une méthodologie et du formalisme du domaine (par exemple l'analyse des processus métiers du PLM(Product Lifecycle Management)) -Décrire le processus du métier de la cybersécurité (norme ISO27x) lié à son organisation, sa gouvernance et les points de décision identifiés -Décrire les principes d'éthiques rencontrés dans l'organisation, les aspects saillants de la culture de la convergence IT/OT -Modéliser un indicateur d'impact écologique d'un composant informatique ou numérique IoT et son mode de calcul -Relater et formaliser une situation vulnérable ou d'incident de sécurité (réponse à incident) à l'aide d'outils de normes ISO 22301 (gestion de crise) -Caractériser le mode de capitalisation de la connaissance utilisé prendra par exemple le cas d'une fiche REFLEX de son choix -Rédiger une analyse réflexive de la mission situant la mission en situation de crise, en analysant les axes d'amélioration
	-Maîtriser les outils du génie logiciel -Maîtriser le déploiment de service -Garantir la sécurité, l'authenticité et la confidentialité des données -Maîtriser les outils d'administration informatique -Conception et développement sécurisé d'une application microservice back-end et front-end en langage par exemple nodejs et javascript utilisée dans le domaine de la fabrication

LP154B61

RNCP40102BC06

Développement et mise en œuvre d'outils de conception et d'analyse

d'outils (assemblage, désassemblage, ...)

-Conception et mise en place de dispositifs de sécurité informatiques offensifs : test d'intrusion KALI, Cyberrange, Bug bounty (plateforme)

-Conception et mise en place de dispositifs de sécurité informatiques défensifs (sondes IDS, parefeux, zones et conduits)(Zone démilitarisé , IDS snort, scanner de vulnérabilité)

-Conception d'un centre de gestion de réponse à un incident de système industrels et urbains (SOC, CSIRT, ...)(après avoir mis en oeuvre le système de défenses et d'attaques)

-Evaluation de la sécurité de l'application à l'aide d'outillage OWASP, mener une analyse statique et dynamique d'un code malveillant lancé par le formateur pendant l'évaluation à l'aide d'outils forensiques mis à la disposition du candidat

-Rédiger un rapport technique intégrant les fichiers de configuration réalisés en langue anglaise

-Déploiment d'un SIEM (Splunk, ELK, ...) et des sondes remontées d'incidents (IDS, ...) pour les systèmes industriels et urbains

-Intégration au sein du SIEM des composants déployés en environnements industriel, a mise en place des règles d'agrégation et des corrélations d'évènements

-Validation de la solution à l'aiede d'une plateforme de simulatyion d'attaque avec l'évacuatioàn des outils (faux positifs, ...)