

DGA

Maîtrise de l'information à BRUZ près de RENNES (35)

Book de postes 2022/2023

Ingénieurs (F/H) Cybersécurité

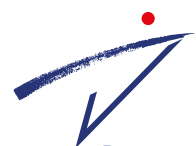


du 09 au 24 nov 2022
www.dghack.fr

DGA MAÎTRISE DE L'INFORMATION
136, La Roche Marguerite 35170 BRUZ
dga-mi-bruz.recrutement.fct@intra.def.gouv.fr



www.defense.gouv.fr/dga



DGA

DIRECTION GÉNÉRALE
DE L'ARMEMENT

Sommaire

› DGA	p.2
› DGA Maîtrise de l'information	p.3
› Un environnement dynamique	p.4
› Activités extra-professionnelles	p.5
› Venez à notre rencontre	p.6
› Comment postuler	p.7
› Les annonces	p.8
› Index par mots clés	... fin

Mention : Ce book est une liste des postes prévisionnels pour l'année 2023 pour les différents métiers à DGA Maîtrise de l'information.



MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

La DGA

Direction Générale de l'Armement
du ministère des Armées
est responsable de la
conception, de l'acquisition et de
l'évaluation des systèmes qui équipent
les forces armées.



DGA Techniques navales
BREST

DGA Maîtrise de l'information
RENNES

DGA Techniques terrestres
ANGERS

DGA Essais propulseurs
SACLAY

DGA Techniques hydrodynamiques
VAL DE REUIL

DGA Ingénierie des projets
PARIS

DGA Maîtrise NRBC
VERT LE PETIT

DGA Techniques terrestres
BOURGES

DGA Essais de missiles
SAINT MÉDARD

DGA Essais en vol
CAZAUX

DGA Essais de missiles
BISCARROSSE

DGA Techniques aéronautiques
TOULOUSE

DGA Essais en vol
ISTRES

DGA Techniques navales
Toulon

DGA Essais de missiles
Toulon - Ile du Levant

10118



2

Retrouvez notre actualité



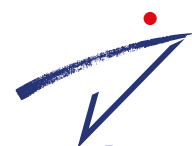
@dga

in

dga



dga



DGA

DIRECTION GÉNÉRALE
DE L'ARMEMENT



MINISTÈRE
DES ARMÉES

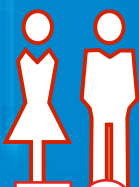
*Liberté
Égalité
Fraternité*

DGA

Maîtrise de l'information

Nos experts techniques travaillent dans les domaines innovants tels que les systèmes d'information et de communication, la cybersécurité, l'Intelligence Artificielle, la survivabilité des systèmes, la navigation, la guerre électronique et les systèmes de missiles.

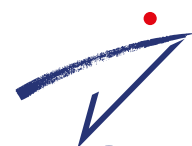



1700

DGA Maîtrise de l'information
Bruz 



3



DGA
DIRECTION GÉNÉRALE
DE L'ARMEMENT

Un environnement dynamique

- › Exercer un métier technique passionnant comme vous ne le trouverez nulle part ailleurs et développer vos compétences dans divers domaines.
- › Travailler sur un site de 100 hectares arboré où l'on peut se déplacer à vélo électrique et accessible par les transports en commun.



4



DGA
DIRECTION GÉNÉRALE
DE L'ARMEMENT



MINISTÈRE
DES ARMÉES

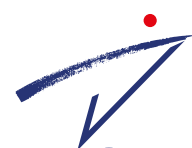
*Liberté
Égalité
Fraternité*

Activités extra- professionnelles



Multiples
activités de
cohésion,
sportives,
culturelles...

 5



DGA

DIRECTION GÉNÉRALE
DE L'ARMEMENT

Venez à notre rencontre

► **Breizh CTF**
Rennes



► **Journées des
étudiants**
Webinaire



► **European
Cyber Week**
Rennes



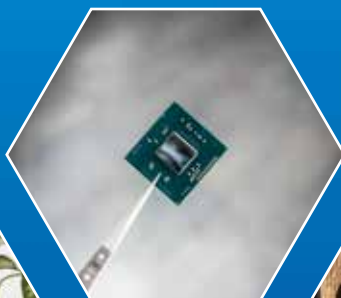
► **Forum écoles**
Bourges, Brest, Lyon,
Paris, Rennes,
Lannion...



 **6**

Comment postuler ?

- › Consultez la liste des postes dans cet ebook, sur le site de l'APEC, sur LinkedIn
- › Adressez votre CV en français à dga-mi-bruz.recrutement.fct@intradef.gouv.fr avec la copie de votre dernier diplôme requis : **master 2/ingénieur CTI/doctorat**
- › Précisez la référence du poste
- › Si votre CV est retenu, vos compétences techniques seront évaluées par un entretien orienté métier
- › Ces postes nécessitent une procédure d'habilitation
- › Le salaire sera déterminé en fonction de votre expérience professionnelle, âge, salaire actuel et diplôme.



Les annonces

- › Pour tous les profils d'ingénieurs (F/H)
- › Pour développer vos compétences
- › Pour acquérir une expérience reconnue
- › Pour contribuer à une mission d'intérêt général et d'actualité.



DGA
DIRECTION GÉNÉRALE
DE L'ARMEMENT

Les postes previsionnels



2023-CASC-01 Administrateur et Analyste sécurité Cyberdéfense	12
2023-EAP-01 Ingénieur en conception de produit de sécurité embarqués	13
2023-EAP-02 Ingénieur en conception d'architecture logicielle de produit de sécurité	14
2023-ESS-01 Ingénieur auditeur organisationnel de la sécurité des systèmes d'information	15
2023-ESS-02 Ingénieur auditeur technique en sécurité des systèmes industriels et	16
2023-ESS-03 Ingénieur auditeur technique de la sécurité des systèmes d'information	17
2023-IAP-01 Ingénieur Architecte produits de sécurité	18
2023-IAPC-01 Ingénieur Cyber - Chef de projet LIO	19
2023-IAPC-02 Ingénieur Cyber - Administrateur Fonctionnel Jira/Confluence	20
2023-IAPC-03 Ingénieur Cyber - Architecte LIO	21
2023-ICOD-01 Ingénieur développeur	22
2023-ICOD-02 Ingénieur développeur mobile Android ou iOS	23
2023-ICOD-03 Ingénieur développeur Linux et embarqué	24
2023-ICSA-01 Architecte cybersécurité systèmes d'armes	25
2023-ICSI-01 Architecte cybersécurité systèmes d'information	26
2023-ICSI-02 Architecte Solution cybersécurité	27
2023-ICSI-03 Ingénieur Sécurisation des systèmes d'information	28
2023-IDIC-01 Data Engineer	29
2023-IDIC-02 Data Analyst	30
2023-IDIC-03 Ingénieur cyber & IA spécialisé en Lutte informatique d'influence	31
2023-IDIC-04 Ingénieur développeur Lutte Informatique d'Influence	32
2023-IDIC-05 Ingénieur Systèmes Big Data	33
2023-IP3C-01 Ingénieur analyste Cyberdéfense spécialisé en lutte informatique offensive	34
2023-IP3C-02 Ingénieur Web sémantique/ Graphe de Connaissances	35
2023-IP3C-03 Ingénieur Cyberdéfense, techniques intrusives en télécommunications & systèmes...	36
2023-IP3C-04 Ingénieur Cyberdéfense spécialisé en systèmes industriels	37
2023-IP3C-05 Ingénieur spécialisé en virtualisation des systèmes informatiques	38



2023-ISPC-01 Ingénieur Cyberdéfense infra compilation	39
2023-ISPC-02 Ingénieur Cyberdéfense Administration Systèmes et Réseaux	40
2023-ISPC-03 Ingénieur Cyberdéfense systèmes d'information	41
2023-ISPC-04 Ingénieur Cyberdéfense systèmes d'information	42
2023-LID-01 Ingénieur en architecture de détection d'intrusion système	43
2023-LID-02 Ingénieur en techniques de détection d'intrusion	44
2023-LID-03 Ingénieur Cyberdéfense SOC	45
2023-LID-04 Architecte Solution Lutte Informatique Défensive	46
2023-SCY-01 Ingénieur Cryptographie – Spécification d'algorithmes	47
2023-SCY-02 Ingénieur Cryptographie – Spécification d'algorithmes	48
2023-SCY-03 Ingénieur Cyberdéfense – Recherche de vulnérabilités cryptographiques ...	49
2023-SCY-04 Ingénieur Conception de logiciel embarqué et sécurité	50
2023-SCY-05 Ingénieur Conception matérielle Cryptographie et Sécurité	51
2023-SDA-01 Directeur de projets Cyber	52
2023-VIM-01 Ingénieur Retro-conception en systèmes embarqués	53
2023-VIMVMAXVMEN-01 Ingénieur Retro-conception en système d'exploitation	54
2023-VIMVMAXVMEN-03 Ingénieur Retro-conception système virtualisé	55
2023-VMAT-01 Ingénieur Retro-conception et analyse de format de données	56
2023-VMAT-02 Ingénieur Cyberdéfense en tests d'intrusion	57
2023-VMAT-03 Ingénieur Retro-conception et analyse de malwares	58
2023-VMAT-04 Ingénieur Cyberdéfense – Recherche de vulnérabilités Web	59
2023-VMAX-01 Ingénieur Retro-conception en produits logiciels Windows	60
2023-VMEN-01 Ingénieur Retro-conception en système Android Linux	61
2023-VMEN-02 Ingénieur Retro-conception en système iOS	62
2023-XCS-01 Ingénieur Evaluation et expertise de la sécurité de composants	63
2023-XEL-01 Ingénieur Expert en sécurité logiciel	64
2023-XEO-01 Ingénieur Cyberdéfense test et validation	65



2023-XIN-01 Ingénieur Investigation Numérique	66
2023-XIP-01 Ingénieur développement logiciel systèmes embarqués	67
2023-XIP-02 Ingénieur électronique spécialisé en systèmes embarqués	68
2023-XIP-03 Ingénieur radio-logicielle	69
2023-XIP-04 Ingénieur électronique radio	70
Index	71



2023-CASC-01

Administrateur et Analyste sécurité Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Supervision SIEM Investigations SOC
Analyses Administration système
Expertise

Description du poste (H/F)

Mission : La personne titulaire du poste sera intégrée dans une équipe dédiée à l'administration et à la supervision de sécurité, à la détection et l'analyse des événements ou informations collectés des moyens opérationnels de Cyberdéfense de DGA MI. Elle devra intégrer des outils de collecte et de détection, assurer la mise en place d'outils de sécurité, participer à l'investigation des événements et superviser le MCS de moyens techniques en cyberdéfense.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) Administrateur et Analyste sécurité Cyberdéfense.

Compétences métiers

- Connaissances des méthodes de collecte de données et d'investigation sur au moins un système d'exploitation (Windows, Linux)
- Connaissance de méthodes et moyens d'analyse/exploitation de journaux d'événements et de traces réseau
- Equipements et outils de supervision de sécurité, MCS

Compétences souhaitées

- Administration systèmes informatiques et réseaux, mécanismes de sécurité
- Architecture de système d'exploitation
- Scripting (python, bash, ...)
- Technique de protection et de détection
- Réseaux IP (LAN, FW, matrice de flux...)

Qualités personnelles :

- Capacité d'analyse et esprit de synthèse
- Autonome tout en sachant travailler en équipe
- Rigoureux et inventif

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-EAP-01

Ingénieur en conception de produit de sécurité embarqués



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Systèmes embarqués Architecture
Conception PoC

Description du poste (H/F)

Mission : Orienter la spécification et la conception technique d'équipements de cybersécurité embarqués. Effectuer une veille technologique sur l'état actuel de la menace technique et sur l'efficacité des mécanismes de sécurité existants. Réaliser des maquetages de solutions et avoir la possibilité d'intégrer une équipe de développement sur une période déterminée.

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une **ingénieur en conception de produit de sécurité embarqués**.

Compétences métiers

- Capacité à réaliser, développer un prototype afin de valider une solution de sécurisation.
- Maîtrise du langage C et connaissance en C++, Python ou VHDL
- Capacité à spécifier, concevoir une architecture sécurisée pour un produit de sécurité à base de processeur, FPGA, SOC, Processeurs ARM, ...)
- Capacité à développer (C ou VHDL) ou intégrer/valider un PoC sur l'aspect fonctionnel et sécurité

Compétences souhaitées

- Connaissance des mécanismes de sécurité permettant de renforcer la sécurité d'un réseau
- Connaissance des mécanismes de boot sécurisés offerts par des plateformes matérielles (intrinsèque aux composants ou TPM)
- Connaissance des protocoles cryptographiques (mécanisme d'authentification, négociation de clés)

Qualités personnelles :

- Synthétique
- Force de proposition
- Forte Autonomie

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique multi-compétences, vous profitez de la richesse des savoir-faire des métiers de DGA-MI et de projets techniques de pointe aux moyens conséquents, le tout en gardant un équilibre entre vie professionnelle et personnelle. Vous serez accompagné lors de votre montée en compétences suite à votre prise de poste.



2023-EAP-02

Ingénieur en conception d'architecture logicielle de produit de sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Logiciel embarqué Architecture
Hyperviseur OS Vulnérabilités PoC Rust
Sandbox

Description du poste (H/F)

Mission : Orienter la spécification et la conception technique d'équipements de cybersécurité (fixes et /ou embarqués). Effectuer une veille technologique sur l'état actuel de la menace technique et sur l'efficacité des mécanismes de sécurité existants. Réaliser des maquetages de solutions et avoir la possibilité d'intégrer une équipe de développement sur une période déterminée.

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une **ingénieur en conception d'architecture logicielle de produit de sécurité**.

Compétences métiers

- Connaissance globale de l'architecture des processeurs embarqués
- Connaissance globale de l'architecture d'OS (plus spécifiquement Linux)
- Conception ou évaluation d'architectures logicielles sécurisées

Compétences souhaitées

- Connaissance globale de l'architecture des processeurs embarqués
- Connaissance globale de l'architecture d'OS (plus spécifiquement Linux)
- Conception ou évaluation d'architectures logicielles sécurisées

Qualités personnelles :

- Synthétique
- Force de proposition
- Forte Autonomie

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique multi-compétences, vous profitez de la richesse des savoir-faire des métiers de DGA-MI et de projets techniques de pointe aux moyens conséquents, le tout en gardant un équilibre entre vie professionnelle et personnelle. Vous serez accompagné lors de votre montée en compétences suite à votre prise de poste.



2023-ESS-01

Ingénieur auditeur organisationnel de la sécurité des systèmes d'information



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Audit Sécurité Vulnérabilité Cyberdéfense
SSI

Description du poste (H/F)

Mission : Auditeur de la sécurité des systèmes d'information : réalisation d'audits de sécurité organisationnels relatifs à la mise en œuvre de systèmes d'information et de systèmes d'armes du Ministère.

Contexte : Au sein de l'équipe d'évaluation et d'audit de sécurité des systèmes d'information (SSI) de la Direction Générale de l'Armement (DGA), vous réaliserez des audits organisationnels de sécurité relatifs à la mise en œuvre de systèmes d'information et de systèmes d'armes du ministère des armées, et vous contribuerez au développement de méthodes d'audit de sécurité.

Vous êtes apte à vous déplacer, environ cinq (5) fois une semaine par an, sur divers sites du ministère des armées.

Compétences métiers

- EBIOS
- Ingénierie de la SSI
- Techniques d'entretien

Compétences souhaitées

- Sécurité informatique
- Connaissance de la menace et des vulnérabilités
- Réglementation
- ISO 27001

Qualités personnelles :

- Autonome sachant travailler en équipe
- Rigoureux, Organisé, Curieux

Les "+" du poste

Le poste proposé vous permettra de travailler dans des environnements hors standard, des contextes d'emploi de systèmes d'information et de systèmes d'armes spécifiques au MinArm. Une diversité propice à l'enrichissement de vos connaissances et compétences, offrant de réelles perspectives d'évolution dans le domaine de la cybersécurité au sein de la DGA.



2023-ESS-02

Ingénieur auditeur technique en sécurité des systèmes industriels et systèmes d'information



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Audit Sécurité Vulnérabilité SSI ICS SCADA
SCI

Description du poste (H/F)

Mission : Auditeur de la sécurité des systèmes d'information : réalisation d'audits techniques de sécurité relatifs à la mise en œuvre de systèmes industriels, de systèmes d'information et de systèmes d'armes du ministère des armées et des analyses de vulnérabilités sur plateformes de tests.

Contexte : Au sein de l'équipe Evaluation de la Sécurité des Systèmes (ESS) de la Direction Générale de l'Armement (DGA), vous réaliserez des audits techniques de sécurité et des analyses de vulnérabilités sur des systèmes industriels, des systèmes d'information et des systèmes d'armes du ministère des armées.

Vous serez également amené(e) à définir/entretenir une plateforme dédiée aux systèmes industriels dans le but de concevoir et réaliser des démonstrations d'attaque/défense, contribuer à l'élaboration de guides de sécurisation/configuration d'équipements industriels ainsi qu'au développement d'outils d'audit technique de sécurité. Il pourra également vous être demandé de sensibiliser/former différents acteurs du ministère des armées sur la sécurisation des systèmes industriels.

Vous êtes apte à vous déplacer environ quatre (4) à six (6) fois une semaine par an sur divers sites du ministère des armées.

Compétences métiers

- Automatismes et informatique industrielle
- Méthodes d'investigation SSI technique
- Ingénierie de la SSI
- Architecture sécurisée de système d'information et de réseau

Compétences souhaitées

- Sécurité informatique
 - Connaissance de la menace et des vulnérabilités
 - Réglementation
 - ISO 27001
- Qualités personnelles :
- Autonome sachant travailler en équipe
 - Rigoureux, Organisé, Curieux

Les "+" du poste

Le poste proposé vous permettra de travailler sur une grande variété de systèmes, ainsi que de multiples technologies matérielles et logicielles déployées dans des environnements hors standard, spécifiques au contexte du MinArm. Une diversité propice à l'enrichissement de vos connaissances et compétences techniques, offrant de réelles perspectives d'évolution dans le domaine de la cybersécurité au sein de la DGA



2023-ESS-03

Ingénieur auditeur technique de la sécurité des systèmes d'information



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Audit Sécurité Vulnérabilité SSI

Description du poste (H/F)

Mission : Auditeur de la sécurité des systèmes d'information : réalisation d'audits de sécurité techniques relatifs à la mise en œuvre de systèmes d'information et de systèmes d'armes du ministère de la défense et des analyses de vulnérabilités sur plateformes de tests.

Contexte : Au sein de l'équipe d'évaluation et d'audit de sécurité des systèmes d'information (SSI) de la Direction Générale de l'Armement (DGA), vous réaliserez des audits techniques de sécurité sur des systèmes d'information et des systèmes d'armes du ministère des armées ainsi que quelques analyses de vulnérabilités sur plateforme de test et contribuerez au développement d'outils d'audit technique de sécurité.

Vous êtes apte à vous déplacer environ quatre (4) à six (6) fois une semaine par an sur divers sites du ministère des armées.

Compétences métiers

- Méthodes d'investigation SSI technique
- Ingénierie de la SSI
- Architecture sécurisée de système d'information et de réseau

Compétences souhaitées

- Sécurité informatique
- Connaissance de la menace et des vulnérabilités
- Réglementation
- ISO 27001

Qualités personnelles :

- Autonome sachant travailler en équipe
- Rigoureux, Organisé, Curieux

Les "+" du poste

Le poste proposé vous permettra de travailler sur une grande variété de systèmes, ainsi que de multiples technologies matérielles et logicielles déployées dans des environnements hors standard, spécifiques au contexte du MinArm. Une diversité propice à l'enrichissement de vos connaissances et compétences techniques, offrant de réelles perspectives d'évolution dans le domaine de la cybersécurité au sein de la DGA



2023-IAP-01

Ingénieur Architecte produits de sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Architecte Cybersécurité Cyberprotection
Cyberdéfense Embarqué Cryptographie
Ingénierie

Description du poste (H/F)

Mission : Dans le cadre du développement des équipements de sécurité qui assurent la protection des systèmes du ministère des Armées, vous coordonnez les travaux des experts. Vous intervenez dans les phases amont d'analyse de sécurité et de spécifications techniques, puis dans le suivi des réalisations industrielles et enfin vous pilotez les évaluations de sécurité et si nécessaire le process d'agrément du produit en lien avec l'ANSSI.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une **Architecte Produits de Sécurité**.

Compétences métiers

- Développement d'équipements et/ou de logiciels pour systèmes embarqués
- Protocoles de communications et télécom, réseau
- Méthode ou langage de modélisation (UML, SysML)
- Notions de Cryptographie
- Sécurité des systèmes d'Information
- Méthodes d'analyse de risque

Compétences souhaitées

- Informatique et/ou électronique
 - Conduite de projet
- Qualités personnelles :
- Esprit de synthèse
 - Travail en équipe
 - Autonomie
 - Aptitudes pour la négociation

Les "+" du poste

Et si vous rejoigniez DGA MI pour travailler sur les futurs produits de cyberprotection ?

En tant qu'architecte vous serez au cœur des programmes d'armement pour assurer leur protection contre les menaces cyber.

A votre arrivée en poste, vous serez accompagné(e) pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et de l'excellence de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus riche de formations internes et externes vous permettant de devenir rapidement autonome sur des projets d'envergure, et dans un environnement de qualité.



2023-IAPC-01 Ingénieur Cyber - Chef de projet LIO



Niveau requis	Contrat	Mots-clés
Ingénieur CTI Master 2	Contractuel civil CDI à Bruz (35)	Cyberdéfense LIO Gestion de projets Agilité Développement logiciel Intégration continue

Description du poste (H/F)

Mission : Le chef de projet Cyber est garant de la solution technique et de sa mise en œuvre sur les différents projets dont il a la charge que ce soit des projets internes ou des projets effectués en sous-traitance.

Il participe aux phases de recueil des besoins des utilisateurs, dans un contexte de schéma directeur ou d'études préalables de projet. Sa compétence technique lui permet d'analyser puis de porter la réponse aux besoins des utilisateurs.

Il pilote les équipes intervenant sur toutes les phases d'un projet (des phases de spécifications et de développement jusqu'à celle d'évaluation).

Il pilote les projets sous-traités (rédaction des CCTP et suivi des marchés de sous-traitance), dans le cadre de marchés de sous-traitance relatifs au domaine (PEA, études, etc.).

Il comprend les choix technologiques et les enjeux associés. Il collabore aussi bien avec des partenaires externes (clients, sous-traitants, éditeurs de logiciels...) que des partenaires internes (autres laboratoires...).

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une chef de projet LIO**.

Compétences métiers	Compétences souhaitées
<ul style="list-style-type: none"> Gestion de Projet Méthodes agiles (Scrum, Kanban, SAFe) Conception Logiciel Intégration continue 	<ul style="list-style-type: none"> Ingénierie de la menace système Réseaux IP, réseaux mobiles, ... DNS, DHCP, Proxy, Firewall, IDS, bases de données, ... Git, JIRA, Confluence, ... <p>Qualités personnelles :</p> <ul style="list-style-type: none"> Rigueur, organisation et curiosité Animation d'équipe Prise de décision Facilité d'adaptation nouveaux contextes techniques et humains



2023-IAPC-02

Ingénieur Cyber - Administrateur Fonctionnel Jira/Confluence



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Atlassian Jira Confluence Sécurité
Supervision

Description du poste (H/F)

Mission : En charge de l'administration des solutions Atlassian (Jira, Confluence et ses différents add-ons) l'administrateur Fonctionnel Jira/Confluence a pour missions :

- Analyser et évaluer les besoins opérationnels des projets et l'organisation des équipes
- Déployer et paramétrer les outils Jira, Confluence ainsi que les différents add-ons (bonne connaissance de gestion des flux de travaux, des formulaires ainsi que du langage JQL – Jira Query Language ; Script Runner - langage Groovy)
- Documenter et accompagner les projets en migration (rédiger et faire évoluer des templates, publier la documentation, les procédures, les pratiques et les outils)
- Suivre l'administration des espaces Confluence
- Participer aux instances de la cellule d'administration
- Interagir avec l'équipe technique d'administration
- Assurer la conduite du changement.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une Administrateur Fonctionnel Jira/Confluence**.

Compétences métiers

Vous justifiez d'une expérience professionnelle de 1 an minimum dans l'administration des solutions Atlassian.

Compétences souhaitées

- Connaissance de la sécurité informatique
- Bonne compétence sur les infrastructures

Qualités personnelles :

- Capacité d'analyse, ingéniosité, inventivité, curiosité, ténacité
- Goût du travail en équipe, intérêt affirmé pour l'innovation

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par une équipe expérimentée connaissant le domaine afin de vous guider au cours des différentes étapes de votre prise de poste.



2023-IAPC-03 Ingénieur Cyber - Architecte LIO



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cyberdéfense LIO Architecture
Modélisation Scénarios

Description du poste (H/F)

Mission : L'architecte Cyber propose un enchaînement de différents outils pour obtenir un effet. Il s'agit d'une approche orientée scénario technique de référence et bout-en-bout. Cela doit se traduire à la fois par la vérification de la bonne intégration des différents outils, du bon fonctionnement du scénario et l'atteinte des effets recherchés, mais également par des recommandations pour les futurs développements (évolutions d'outils existants, nouveaux outils) ou vers la chaîne hiérarchique/métier pour le processus de production (cohérence et prescription sur les choix techniques de la chaîne de CI/CD...).

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une architecte LIO**.

Compétences métiers

- Architecture système de lutte informatique
- Technique en test d'intrusion
- Conception Logiciel
- Standards de modélisation (TOGAF, UML...)
- Veille technique

Compétences souhaitées

- Ingénierie de la menace système
 - Réseaux IP, réseaux mobiles, ...
 - DNS, DHCP, Proxy, Firewall, IDS, bases de données, ...
- Qualités personnelles :
- Rigueur, organisation et curiosité
 - Animation d'équipe
 - Prise de décision
 - Facilité d'adaptation nouveaux contextes techniques et humain

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par une équipe expérimentée connaissant le domaine afin de vous guider au cours des différentes étapes de votre prise de poste.

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cyber sécurité. De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.



2023-ICOD-01
Ingénieur développeur



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Windows Linux iOS
Android Embarqué IoT Kernel LAN 5G
Containerisation Cloud BigData RedTeam

Description du poste (H/F)

Mission : Intégré(e) à une équipe projet, dont l'objectif est de réaliser des logiciels au profit du Ministère des Armées, votre mission consiste à :

- Participer à la définition et au développement des systèmes et outils métiers ;
- Concevoir et développer des logiciels à vocation défensive et offensive.

Contexte : Dans le cadre de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, en forte croissance, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) dans le domaine de l'analyse et du développement de logiciels défensifs et offensifs.

Une expérience dans le domaine de la sécurité informatique sera appréciée. Vous êtes curieux et avez un réel intérêt pour le challenge technique et l'innovation dans un contexte opérationnel fort.

Compétences souhaitées

- Maîtrise d'un langage de programmation (Rust, python, C, C++, Go, kotlin...) ;
- Maîtrise du développement de programmes userland et/ou kernel sous Windows, Linux, embarqué/IoT, Android ou iOS ;
- Développement Web (backend ou fullstack), aide à la décision, big data, Cloud, SaaS ;
- Développement réseau : LAN, 5G, WAN, blockchain ;

Les "+" du poste

À votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-ICOD-02

Ingénieur développeur mobile Android ou iOS



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur iOS Android ObjectiveC
Swift Kotlin JAVA C Python MacOS
RedTeam

Description du poste (H/F)

Mission : Intégré(e) à une équipe projet, dont l'objectif est de réaliser des logiciels au profit du Ministère des Armées, votre mission consiste à :

- Participer à la définition et au développement des systèmes et outils métiers ;
- Concevoir et développer des logiciels à vocation défensive et offensive
- Etudier le fonctionnement interne des systèmes Android, iOS ou MacOS;

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) dans le domaine de l'analyse et du développement d'applications de sécurité Android ou iOS.

Compétences métiers

- Maîtriser le langage C, ObjectiveC, Swift, Kotlin ou Java
- Connaître le langage Python
- Être intéressé par le développement iOS ou Android (expérience souhaitée sur le développement d'applications mobiles, mais pas indispensable)

Compétences souhaitées

- Familier avec les outils de développement (debugger, chaîne de compilation, IDE)
- Familier avec les outils d'intégration continue et la méthodologie agile.

Qualités personnelles :

- Capacité à s'intégrer à une équipe
- Être curieux et avoir un esprit de synthèse

Les "+" du poste

En choisissant ce poste, vous intégrerez une équipe bienveillante et dynamique, et profiterez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. À votre arrivée, vous bénéficierez ainsi d'une formation initiale de 3 mois. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.



2023-ICOD-03 Ingénieur développeur Linux et embarqué



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Linux Embarqué IoT Kernel
RedTeam

Description du poste (H/F)

Mission : Intégré(e) à une équipe projet, dont l'objectif est de réaliser des logiciels au profit du Ministère des Armées, votre mission consiste à :

- Participer à la définition et au développement des systèmes et outils métiers ;
- Concevoir et développer des logiciels à vocation défensive et offensive

Contexte : Dans le cadre de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, en forte croissance, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) dans le domaine de l'analyse et du développement de logiciels défensifs et offensifs en environnement Linux et embarqué.

Compétences métiers

- Maîtriser le langage C ;
- Connaître les langages C++, Python, script shell ;
- Maîtriser le développement en environnement Linux (userland et éventuellement kernel) ;
- Une appétence pour le domaine de l'IoT, des plateformes Raspberry Pi, des microcontrôleurs, de chips ESP32, PyCom etc. sera appréciée.

Compétences souhaitées

- Savoir utiliser des outils de développement (IDE, compilateurs, cross-compilateurs)
- Être familier avec Git, le processus d'intégration continue, la gestion de projet type Jira
- Avoir des notions d'Agilité

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-ICSA-01

Architecte cybersécurité systèmes d'armes



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Architecte EBIOS ISO27001
Cyber-détection

Description du poste (H/F)

Mission : Vous piloterez la démarche de sécurisation des systèmes d'armes vis à vis de la menace cyber. Vous interviendrez sur différents projets, tels que des grands programmes d'armement (satellites, avions de combats, sous-marins, missiles...), afin de livrer des systèmes cyber sécurisés à nos forces militaires. Plus précisément :

- Conduire des analyses de risques et participer à l'élaboration de spécifications techniques ;
- Apporter un soutien technique et réglementaire aux équipes programmes sur les questions de cybersécurité en pilotant le suivi des activités de développement réalisées par les industriels;
- Orienter les choix de politique cryptographique dans le but de protéger les informations du système,
- Animer et coordonner des équipes d'experts lors des phases d'évaluations, d'analyse de vulnérabilités et d'audits sur les systèmes, pour en vérifier la conformité et proposer les plans d'actions.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une **Architecte cybersécurité systèmes d'armes**.

Compétences métiers

- Réglementation liée à la sécurité (Guides de recommandations ANSSI, LPM, RGS, RGPD)
- Méthodologie liée à la sécurité (ISO27001, EBIOS RM)
- Cyber-détection
- Architecture réseau
- Ingénierie système
- Informatique embarquée

Compétences nécessaires

- Capacités rédactionnelles
- Facultés d'analyse et de synthèse
- Attrait pour le relationnel et la négociation
- Facilité à rendre compte.
- Autonomie
- Initiative

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe d'architectes expérimentés et passionnés, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.



2023-ICSI-01 Architecte cybersécurité systèmes d'information



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Système d'information Architecte Chef de
Projet Sécurité informatique Product Owner
Agile EBIOS ISO27001

Description du poste (H/F)

Mission : Vous piloterez la démarche de sécurisation des systèmes d'information vis à vis de la menace cyber. Vous interviendrez sur les grands projets numériques, informatiques ou réseaux de l'ensemble du Ministère des Armées, afin de livrer des systèmes cyber sécurisés à nos clients. Plus précisément :

- Conduire des analyses de risques et participer à l'élaboration de spécifications techniques ;
- Apporter un soutien technique et réglementaire aux équipes programmes sur les questions de cybersécurité en pilotant le suivi des activités de développement réalisées par les industriels;
- Orienter les choix de politique cryptographique dans le but de protéger les informations du système,
- Animer et coordonner des équipes d'experts lors des phases d'évaluations, d'analyse de vulnérabilités et d'audits sur les systèmes, pour en vérifier la conformité et proposer les plans d'actions.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une Architecte cybersécurité systèmes d'information.

Compétences métiers

- Réglementation liée à la sécurité (Guides de recommandations ANSSI, LPM, RGS, RGPD)
- Méthodologie liée à la sécurité (ISO27001, EBIOS RM)
- Méthode Agile
- Lutte Informatique Défensive
- Architecture réseau
- Systèmes d'information
- Gestion de projet
- Ingénierie système

Compétences nécessaires

- Capacité rédactionnelles
- Facultés d'analyse et de synthèse
- Attrait pour le relationnel et la négociation
- Facilité à rendre compte
- Autonomie
- Initiative

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe d'architectes expérimentés et passionnés, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso



2023-ICSI-02 Architecte Solution cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité Cloud privé DevSecOps Agile
Architecture

Description du poste (H/F)

Mission : Analyser le besoin et les exigences de sécurité, concevoir des architectures sécurisées de systèmes d'information, contribuer à des choix techniques, piloter la réalisation et le déploiement de projets en mode AGILE.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur cybersécurité.

Compétences métiers

- Sécurité des architectures de type cloud privé
- Sécurité dans une approche DevSecOps
- Architectures Zero Trust
- Sécurité des architectures micro-services

Compétences souhaitées

- Conduite de projet en mode agile
- Services applicatifs (web services, messagerie, annuaire, etc.)
- Identité numérique

Qualités personnelles :

- Travail en équipe
- Esprit de synthèse
- Autonomie

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.



2023-ICSI-03

Ingénieur Sécurisation des systèmes d'information



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité Cloud privé DevSecOps Agile
Architecture

Description du poste (H/F)

Mission : Mener des expertises techniques pour évaluer la sécurisation des systèmes d'information, et accompagner la sécurisation des systèmes d'information au sein des projets de la DGA.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur cybersécurité.

Compétences métiers

- Vulnérabilités liées aux systèmes d'exploitation et aux logiciels ainsi que des contremesures applicables
- Mécanismes de sécurité des systèmes d'exploitation
- Déploiement et configuration de solutions de protection (authentification forte, endpoint protection, pare-feu, solution de chiffrement, ...)
- Sécurité des réseaux IP et réseaux sans fil

Compétences souhaitées

- Architectures techniques des intranets et de leurs composants (fédération d'identité, gestion de parc, messagerie, services applicatifs, ...)
- Cryptographie appliquée
- Mécanismes de virtualisation et conteneurisation (OS et réseau)
- Rédaction de recommandations techniques et suivi d'études
- Systèmes d'exploitation Linux et Windows

Qualités personnelles :

- Capacité à s'intégrer à une équipe et à y travailler, tout en étant autonome
- Curiosité, esprit de synthèse, créativité
- Savoir restituer une analyse technique à des interlocuteurs variés (profils techniques ou profils décideurs)
- Savoir s'adapter à des contextes très différents

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.



2023-IDIC-01 Data Engineer



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

BigData Spark Hadoop Elasticsearch JAVA
SCALA Iceberg

Description du poste (H/F)

Mission : La personne titulaire du poste sera intégrée dans une équipe dédiée à la conception de plateformes Big Data afin d'exploiter des données d'intérêt pour la Cyberdéfense. Elle devra concevoir de nouvelles architectures et implémenter des pipelines de données distribués afin de répondre aux problématiques posées.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un Data Engineer.

Compétences métiers

- Bon relationnel.
- Maîtrise des technologies suivantes :
 - Stockage distribué (HDFS, ...)
 - Recherche plein texte (Elasticsearch, ...)
 - Traitements distribués (Spark, Yarn, ...)
 - Gestionnaires de workflows (Cadence, ...)
 - Outils d'exploration / visualisation (Kibana, Zeppelin, ...)
- Capacité à appréhender de nombreuses sources de données hétérogènes et à concevoir et implémenter des workflows d'ingestion, nettoyage, structuration, enrichissement et exploitation de ces mêmes données.
- Bonnes pratiques de développement logiciel.

Compétences souhaitées

- Connaissance du domaine Cyber.
- Outils de sécurisation et de gouvernance de la donnée (Atlas, Ranger, ...).
- Bases Graph.
- Bases OLAP

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-IDIC-02 Data Analyst



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Analyses Fingerprint OSINT BigData

Description du poste (H/F)

Mission : La personne titulaire du poste sera intégrée dans une équipe dédiée à la conception de plateformes Big Data permettant d'exploiter les données d'intérêt pour la Cyberdéfense dans les 4 domaines de la lutte informatique. Dans un processus d'amélioration continue, elle sera chargée de contribuer au choix des datasets utiles aux métiers, au recueil, à l'intégration et à l'exploitation de ces données dans un data warehouse.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un (ou une) ingénieur chargé de l'analyse des données d'intérêt Cyber.

Le poste consiste à :

- Identifier et analyser les sources de données pertinentes pour la Cyberdéfense.
- Spécifier les pipelines de données conjointement avec l'équipe d'ingénierie Big Data.
- Contribuer au développement d'outils d'analyse et d'étiquetage des données avec les équipes Data & IA dans une démarche CI/CD.
- Capitaliser et valoriser les connaissances acquises dans le strict respect des exigences du ministère de la défense et des différents domaines de la lutte informatique (LID, LIO et L2I).

Compétences métiers

- Maîtrise d'outils d'analyse et visualisation de données type Kibana, Zeppelin, ...
- Scripting et développement (Bash, Python, Java, Scala).
- Connaissances réseau et système.

Compétences souhaitées

- Connaissance des techniques de hacking (fingerprinting, détection et exploitation de vulnérabilités).
- Esprit de synthèse et bon relationnel.

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-IDIC-03

Ingénieur cyber & IA spécialisé en Lutte informatique d'influence



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

L2I IA Développeur TAL Multimédia

Description du poste (H/F)

Mission : Le titulaire sera chargé du pilotage des développements d'applications pouvant mettre en œuvre des techniques d'intelligence artificielle au profit la lutte informatique d'influence. Il aura en charge :

- Les relations avec les opérationnels, le recueil du besoin et l'animation de la feuille de route;
- Le suivi de la réalisation de traitements correspondants aux besoins exprimés par les opérationnels sur des thématiques multimédias, de traitement et d'analyse de données, de traitement du langage, que ces développements soient réalisés en interne ou en sous-traitance ;
- La prescription, le suivi et l'évaluation des travaux confiés aux industriels ;
- Les relations avec les experts métiers (Cyber et IA) de DGA-MI.
- L'animation d'une veille technique, le maintien et le développement des relations avec les partenaires universitaires

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) Cyber Lutte informatique d'influence (L2I) et intelligence artificielle. Ces travaux concernent les domaines de la détection de l'influence adverse, la contre-influence et le traitement des données issues de médias sociaux, conformément à doctrine L2I du ministère des armées

Compétences métiers

- Maîtrise des différentes techniques d'intelligence artificielle et en particulier d'apprentissage automatique et apprentissage profond (Machine Learning et Deep learning)
- Pratique des principaux frameworks (Tensorflow/Keras, PyTorch, Scikit-learn).

Compétences souhaitées

- Maîtrise des environnements de développement ;
- Maîtrise des outils de déploiement (Docker)
- Méthodes d'intégration continue (devops) ;
- Conception d'IHM/FH.FH.

Qualités personnelles :

- Curiosité ;
- Travail en équipe ;
- Adaptabilité aux nouvelles technologies



2023-IDIC-04

Ingénieur développeur Lutte Informatique d'Influence



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

L2I Développeur FullStack

Description du poste (H/F)

Mission : La personne sera chargée de venir renforcer les équipes dédiées à la lutte informatique d'influence (L2I)

Contexte : La doctrine L2I (lutte informatique d'influence) a été présentée par la ministre des Armées en octobre 2021. Les capacités de veille, détection et caractérisation de cette menace vont être amenées à croître fortement dans les années à venir. Dans ce cadre, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) Cyber.

DGA-MI cherche des ingénieurs développeurs Full-Stack, afin d'accompagner le développement des capacités de traitement multimédias développées par les équipes d'intelligence artificielle et la prise en compte des besoins exprimés par les entités opérationnelles.

Compétences métiers

- API REST ;
- Technologies front-end/back-end ;
- Outils de conteneurisation (Docker) ;
- Outils de suivi de version et de bugs (Git, Jira).

Compétences souhaitées

- Proposer et faire évoluer l'architecture du système en fonction des besoins et évolutions technologiques ;
- Produire et documenter le code répondant aux besoins exprimés ;
- Réaliser des IHM simples et intuitives répondant aux besoins des opérationnels ;
- Spécifier, suivre et contrôler les composants potentiellement confiés à une MOE industrielle

Qualités personnelles :

- Curiosité ;
- Travail en équipe ;
- Adaptabilité aux nouvelles technologies

Les "+" du poste

Vous évoluerez dans un environnement novateur, nécessitant à la fois de fortes capacités de travail en équipe, mais aussi une autonomie et un esprit d'initiative.



2023-IDIC-05 Ingénieur Systèmes Big Data



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Ansible Docker BigData Hadoop
Spark Elasticsearch Grafana

Description du poste (H/F)

Mission : Vous participez à la définition, à l'implémentation, au déploiement et au maintien en condition opérationnelle de plateformes Big Data hébergeant des données d'intérêt pour la Cyberdéfense. Vous intervenez sur un spectre large, depuis les infrastructures, en passant par les systèmes, jusqu'à la pile logicielle interne, en boucle courte avec les équipes " Data " (Engineering/Analysts/Science).

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un Administrateur Big Data.

Compétences métiers

- L'administration des systèmes Linux (Debian ou dérivés)
- Une chaîne d'automatisation, de gestion de version et de déploiement (idéalement Ansible et Gitlab CI/CD)
- Une solution de conteneurisation (Docker swarm ou Kubernetes)

Compétences souhaitées

- Hardware et infrastructures d'hébergement de serveurs
- Composants d'infrastructures Big Data (Hadoop, Spark, Elasticsearch, ...)
- Sécurisation de systèmes
- Gestion d'un service en production
- Connaissance du domaine Cyber

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-IP3C-01

Ingénieur analyste Cyberdéfense spécialisé en lutte informatique offensive



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

OSINT LIO Modélisation Capitalisation L2I

Description du poste (H/F)

Mission : Le titulaire sera en charge des analyses nécessaires à la préparation du développement d'outils au profit de la lutte informatique offensive. Sur les domaines dont il a la charge, il capitalisera les informations nécessaires à la compréhension et l'identification de la surface d'attaque du système, puis il contribuera à l'élaboration des scénarii d'attaque et à la réalisation de capacités de lutte informatique offensives.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) pluridisciplinaire dans le domaine de la lutte informatique offensive. Ces travaux s'inscrivent dans le cadre de la doctrine de lutte informatique offensive (LIO) du ministère des armées.

Compétences métiers

- Connaissances des méthodes de collecte de données et d'investi Architectures techniques des systèmes numériques ;
- Recherche d'information et analyse de documentation ;
- Capitalisation et représentation de l'information ;
- Cybersécurité

Compétences souhaitées

- Capacité d'analyse de niveau système
 - Capacité de synthèse et de présentation de résultats d'études
- Qualités personnelles :
- Autonomie
 - Créativité
 - Curiosité
 - Innovation
 - Pédagogie

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-IP3C-02

Ingénieur Web sémantique/ Graphe de Connaissances



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

KnowledgeGraph LinkedData

Description du poste (H/F)

Mission : La personne titulaire du poste sera intégrée dans une équipe dédiée à la mise en place d'une infrastructure d'extraction et de gestion de connaissances pour la cybersécurité. Pour cela, elle devra utiliser l'ensemble des outils du web sémantique et maîtriser le développement logiciel.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cybersécurité, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) Web sémantique/ Graphe de Connaissances.

Le poste consiste à mettre en place des outillages d'ingénierie de la connaissance cyber visant à structurer et automatiser les phases de collecte des données puis d'extraction, de modélisation et d'enrichissement de la connaissance d'intérêt cyber à des fins de capitalisation..

Compétences métiers

- La maîtrise des normes RDF, RDFS, OWL 2, SPARQL;
- La connaissance des normes SHACL, R2RML, outil et norme de raisonnement;
- Des connaissances en base graphes de type triple stores.

Compétences souhaitées

- Le développement informatique : python, java ;
- Des connaissances en développement IHM JavaScript
- Des bases de Cyber Défense

Qualités personnelles :

- Créativité
- Autonome
- Innovation

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-IP3C-03

Ingénieur Cyberdéfense, techniques intrusives en télécommunications & systèmes industriels



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Vulnérabilités Exploitation Hacking Pentest
Telecom SCADA ICS Smartcities

Description du poste (H/F)

Mission : Vous contribuerez au renforcement de la sécurité des infrastructures du Ministère des Armées en simulant leur exposition à des attaques cybernétiques. Les travaux menés consistent à rechercher des éléments techniques ou vulnérabilités, d'enchaîner et scénariser ces actions afin de mettre en exergue certains effets redoutés. Vous devrez synthétiser et exposer les résultats obtenus aussi bien à l'oral qu'à l'écrit.

Vous intégrerez une équipe projet pluridisciplinaire composée d'experts du domaine (administration et exploitation métier, reverse-engineering, investigation numérique, développement).

Contexte : Le pôle Cyberdéfense de la DGA recrute un(e) ingénieur(e) cyberdéfense pour rejoindre le laboratoire Hacking et Expertise Système. Vous aurez la charge de réaliser des expertises technologiques sur des domaines spécifiques, comme des infrastructures de télécommunications ou industrielles.

Compétences métiers

- Architecture système et réseaux
- Cybersécurité
- Architecture et sécurité des systèmes de télécommunications
- Architecture et sécurité des systèmes industriels
- Audit et test d'intrusion (pentest)
- Analyse et gestion de risques

Compétences souhaitées

Qualités personnelles :

- Créativité
- Autonome
- Innovation

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-IP3C-04

Ingénieur Cyberdéfense spécialisé en systèmes industriels



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

SCADA ICS GTB Automates Embarqué
Systèmes industriels

Description du poste (H/F)

Mission : En qualité d'ingénieur polyvalent à forte compétence dans le domaine des systèmes industriels, vous serez en charge de comprendre les différentes technologies d'un système étudié, de vous maintenir à l'état de l'art tout en étant force de proposition sur le sujet. L'objectif est de mettre en place une ou plusieurs plateformes opérationnelles représentatives du système industriel étudié. Ces prototypes permettront à des équipes projet d'évaluer, de mesurer puis d'appréhender concrètement l'impact de scénarios de menaces cyber pouvant peser sur ces systèmes.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) cyberdéfense spécialisé dans les systèmes industriels.

Compétences métiers

- Automates Programmables Industriels, RTU (Remote Terminal Unit), et langages de programmation associés (Instruction List, Structured Text, Sequential Function Chart, Function Block Diagram, Ladder)
- Réseaux et Bus de terrain industriels : liaisons Ethernet (ModbusTCP, EthernetIP, Profinet, ...), Profibus, Série (RS-232 / 422 / 485), Protocoles JTAG, ...)
- Logiciels de Supervision d'installations automatisées
- Serveurs de communication (OPC, DDE, SuiteLink, ...)
- Compétence en câblage électrique de tableaux basse-tension ; connaissance/compétence en électrotechnique, domotique, mécanique, ...
- Participation à la mise en œuvre de gros systèmes (SCADA, GTB, GTC, GMAO, ...)
- Développement informatique : C, scripts Python, Perl, ...
- Compétences générales en sécurité informatique

Compétences souhaitées

- Systèmes d'exploitation (Windows, Linux, MAC OS, Android, ...)
- Réseaux de communication (IP, GSM, RSx, SCADA ...)
- Routage et sécurité réseau
- Virtualisation (VMWare, Virtualbox, QEMU...)
- Sauvegardes (NAS, SAN ...)

Qualités personnelles :

- Organisation
- Autonomie



2023-IP3C-05

Ingénieur spécialisé en virtualisation des systèmes informatiques



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Virtualisation Systèmes informatiques
Réseau Administration VMWare

Description du poste (H/F)

Mission : En qualité d'ingénieur polyvalent à forte compétence dans le domaine de la virtualisation des systèmes informatiques, vous serez en charge d'homogénéiser, dans la limite du possible, les systèmes d'information de l'ensemble du parc de plateformes CYBER. Vous chercherez naturellement à vous maintenir à l'état de l'art du domaine tout en étant force de proposition sur ces sujets.

L'objectif est de fournir à des plateformes techniques de différentes natures, un écosystème commun, offrant des services génériques (réseaux, restauration, sauvegarde ...), complétés de besoins spécifiques.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) cyberdéfense spécialisé en virtualisation des systèmes informatiques.

Compétences métiers

- Réseaux IP
- Virtualisation systèmes, notamment les solutions VMware
- Virtualisation éléments réseaux
- Administration systèmes informatiques

Compétences souhaitées

- Systèmes d'exploitation (Windows, Linux, MAC OS, Android, ...)
- Routage et sécurité réseau
- Sauvegardes (NAS, SAN ...)
- Sécurité informatique
- Développement informatique : C
- Scripting (bash, python ...)

Qualités personnelles :

- Autonome
- Organisation

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues plus expérimentés et par un référent métier pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur des projets d'envergure, et ce, dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.



2023-ISPC-01

Ingénieur Cyberdéfense infra compilation



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

DevSecOps Compilation Build CI/CD

Description du poste (H/F)

Mission : Intégré.e à une équipe dont l'objectif est d'assurer la compilation, le test et le déploiement sécurisé de logiciels du Ministère des Armées, votre mission consistera à :

- Assurer la sécurité de la chaîne de compilation ;
- Développer, maintenir une chaîne de compilation, de test et de déploiement ;
- Participer au développement d'outils métiers et à leur intégration dans la chaîne de développement ;
- Contribuer à la spécification et la diffusion des bonnes pratiques en matière de chaînes de compilation, au sein du Ministère et de ses partenaires.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur.e infra de compilation**.

Compétences métiers

- Administration systèmes informatiques et réseaux
- Automatisation de déploiement (Ansible)
- Intégration continue (Jenkins, Gitlab/CI)
- Connaissance des scripts Python, PowerShell
- Support aux projets et utilisateurs (population d'informaticiens)

Compétences souhaitées

- Maîtrise des environnements Linux (Debian/Ubuntu) et Windows (Active Directory)
- Utilisation des techniques de virtualisation (VMware vSphere, Horizon)
- Utilisation des techniques de conteneurisation (Docker, K8S)

Qualités personnelles :

- Rigueur, organisation et curiosité
- Autonomie
- Capacité à s'intégrer dans une équipe
- Facilité d'adaptation

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et expérimentée afin de vous guider lors de votre prise de poste. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.



2023-ISPC-02

Ingénieur Cyberdéfense Administration Systèmes et Réseaux



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

VMWare Network Storage Backup IaC
HPC SDN VDI

Description du poste (H/F)

Mission : Concevoir, déployer et administrer les systèmes d'information au profit des activités de cyberdéfense.

L'administrateur système et réseau assure la supervision, la gestion, la sécurisation, l'évolution et le maintien en conditions opérationnelles de l'infrastructure des Systèmes d'Information au profit des activités de cyberdéfense, dans le strict respect des exigences du ministère des Armées et des activités liées au domaine.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur Administration Systèmes et Réseaux**.

Compétences métiers

- Conception d'architectures complexes et hétérogènes
- Technologies système d'exploitation (Windows, Linux)
- Technologies serveurs (Lenovo, Dell, HPE)
- Technologies de virtualisation (vmware vSphere, NSX-T)
- Technologies de stockage SAN, NAS (Dell EMC, NetApp), VSAN
- Technologie de supervision système et réseaux
- Réseaux IP, routeurs, switches (HP, Cisco), pare-feux (Arkoon, Stormshield, Forcepoint, pfSense)
- Techniques de sauvegarde (Veeam backup)
- Scripts Python, Perl, Shell

Compétences souhaitées

- Très bonne connaissance de la sécurité informatique
 - Bonne compétence sur les infrastructures
- Qualités personnelles :
- Capacité d'analyse, ingéniosité, inventivité, curiosité, ténacité
 - Goût du travail en équipe, intérêt affirmé pour l'innovation et inventif

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et expérimentée afin de vous guider lors de votre prise de poste. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.



2023-ISPC-03

Ingenieur Cyberdéfense systèmes d'information



Niveau requis

Ingenieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Docker Virtualisation DevOps

Description du poste (H/F)

Mission : Assurer le déploiement, la supervision, la sécurisation, l'évolution et le maintien en condition opérationnelle des Systèmes d'Information au profit des activités cyber dans un environnement mixte Windows et Linux récent et innovant.

Vous participez entre autres à l'administration et au maintien en condition de l'environnement métier hébergé au sein d'un cloud privé ainsi qu'au support des experts cyber. Vous interviendrez également au développement et déploiement de solutions métier, en se basant sur un socle technique polyvalent à base de virtualisation VMware, conteneurisation Docker (K8S à l'étude) et d'orchestration Ansible.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur DevOps**.

Compétences métiers

- Administration systèmes informatiques et réseaux
- Gestionnaire de configuration (Ansible)
- Orchestration (Tower)
- Connaissance en supervision de sécurité et système
- Connaissance des scripts Python
- Support aux projets et utilisateurs (population d'informaticiens)
- Connaissance des cycles de développement et de l'intégration continue
- Développement d'applications web au profit des utilisateurs finaux (angular, node, ...)

Compétences souhaitées

- Maîtrise des environnements Linux (Debian/Ubuntu) et Windows
- Utilisation des techniques de virtualisation (VMware vSphere)
- Utilisation des techniques de conteneurisation (Docker, K8S)
- Utilisation de pare-feux (pfSense)

Qualités personnelles :

- Rigueur, organisation et curiosité
- Capacité à s'intégrer dans une équipe
- Facilité d'adaptation

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et expérimentée afin de vous guider lors de votre prise de poste. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.



2023-ISPC-04

Ingenieur Cyberdéfense systèmes d'information



Niveau requis

Ingenieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Docker Ansible WinSrv AD VDI

Description du poste (H/F)

Mission : Assurer le déploiement, la supervision, la sécurisation, l'évolution et le maintien en condition opérationnelle des Systèmes d'Information au profit des activités cyber dans un environnement mixte Windows et Linux récent et innovant.

Vous participez entre autres à l'administration des services communs avec annuaire AD, communication mail et visio ainsi qu'à la gestion du parc (MECM) et au support des experts cyber. Vous intervenez également au déploiement de solutions métier, en se basant sur un socle technique polyvalent à base de virtualisation VMware, conteneurisation Docker (K8S à l'étude) et d'orchestration Ansible.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur systèmes d'information**.

Compétences métiers

- Administration systèmes informatiques et réseaux
- Gestionnaire de configuration (Ansible)
- Gestion d'un parc informatique Windows et Linux (GPO, MECM)
- Connaissance en supervision de sécurité et système
- Connaissance des scripts Python, PowerShell
- Support aux projets et utilisateurs (population d'informaticiens)

Compétences souhaitées

- Maîtrise des environnements Linux (Debian/Ubuntu) et Windows (Active Directory)
- Utilisation des techniques de virtualisation (VMware vSphere, Horizon)
- Utilisation des techniques de conteneurisation (Docker, K8S)
- Utilisation des équipements IP, switches (HP, Cisco), pare-feux (Stormshield, pfSense)

Qualités personnelles :

- Rigueur, organisation et curiosité
- Capacité à s'intégrer dans une équipe
- Facilité d'adaptation

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et expérimentée afin de vous guider lors de votre prise de poste. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.



2023-LID-01

Ingénieur en architecture de détection d'intrusion système



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

LID TTP SOC IDS NIDS HIDS SIEM
Architecte

Description du poste (H/F)

Mission : Expertiser des architectures de détection d'intrusion système et des stratégies de Lutte Informatique Défensive, instanciées au sein de projets de la DGA, en phase de conception d'intégration et/ou de déploiement.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur en architecture de détection d'intrusion système**.

Compétences métiers

- Sécurité des systèmes d'information (menaces, vulnérabilités, mécanisme de sécurité)
- Solutions de détection d'intrusion et supervision de la sécurité : sondes de détection d'intrusion (Réseau, Hôte), SIEM, outils de visualisation et aide à la décision, composants d'un SOC, ...
- Intégration système de solutions LID
- Stratégies de détection

Compétences souhaitées

- Techniques d'intrusion, techniques de détection
- Architectures de systèmes d'information
- Elaboration de spécifications techniques

Qualités personnelles :

- Capacité à s'intégrer à une équipe et à y travailler, tout en étant autonome
- Curiosité, esprit de synthèse, créativité
- Savoir s'adapter à des contextes très différents

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso. Par ailleurs, nous vous proposons une formation pluriannuelle sur le domaine de la Lutte Informatique Défensive.



2023-LID-02

Ingénieur en techniques de détection d'intrusion



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Détection intrusion NIDS HIDS SIEM
Python C Windows Linux Sandbox
Honeypot Suricata Snort

Description du poste (H/F)

Mission : Concevoir, expérimenter, analyser et maquetter des techniques et des produits de détection d'intrusion.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur en techniques de détection d'intrusion**.

Compétences métiers

- Expérience de mise en œuvre d'une ou plusieurs solutions de détection d'intrusion et de supervision de la sécurité (sondes de détection d'intrusion, honeypot, sandbox, collecteurs d'événements, SIEM)
- Expérience en développement pour la réalisation de preuve de concept
- Connaissance du comportement des malwares et de techniques d'exploitation
- Connaissance de l'architecture bas niveau et des mécanismes internes de Windows ou de Linux
- Rédaction de spécifications techniques, de dossier de synthèse ou de référentiel technique
- Suivi contractuel de prestations confiées à des industriels de la défense

Compétences souhaitées

- Systèmes d'exploitation (Windows, Linux, Android, ...)
- Sécurité informatique
- Réseau/Télécommunication (VoIP, Active Directory, SDN, Cloud, ...)
- Techniques de virtualisation
- Développement informatique : C, C++, Go, Rust
- Scripting (bash, python, powershell, ...)

Qualités personnelles :

- Autonomie
- Créativité
- Innovation
- Rigueur

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso. Par ailleurs, nous vous proposons une formation pluriannuelle sur le domaine de la Lutte Informatique Défensive.



2023-LID-03 Ingénieur Cyberdéfense SOC



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

SOC Détection SIEM IoC Administration
système

Description du poste (H/F)

Mission : Contribuer à la construction d'une capacité de supervision de la sécurité (SOC), intégrer des outils de détection et de collecte de données, contribuer à l'administration du SOC, mettre en supervision de sécurité des systèmes d'information de la Direction Générale de l'Armement, expérimenter de nouvelles techniques de détection.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur Cyberdéfense SOC.

Compétences métiers

- Maîtrise de méthodes de collecte de données et d'investigation sur au moins un système d'exploitation (Windows, Linux)
- Connaissance de méthodes d'analyse de journaux d'événements et de traces réseau
- Connaissance de modes opératoires d'attaquants
- Connaissance des techniques d'exploitation de vulnérabilités
- Connaissance des protocoles courants pour le fonctionnement des services réseaux et applicatifs et d'au moins un système d'exploitation (Windows, Linux)
- Des connaissances en investigation numérique sont un plus (notamment d'outils de prélèvements)

Compétences souhaitées

- Architecture de systèmes d'information
- Administration de systèmes d'exploitation (Linux, Windows)
- Réseaux (LAN, IP, ...)
- Technique de protection et de détection (Sondes NIDS/HIDS, Pare-feu, Antivirus, ...)
- Scripting (python, bash, powershell, ...)

Qualités personnelles :

- Capacité à s'intégrer à une équipe et à y travailler, tout en étant autonome
- Curiosité, esprit de synthèse, créativité
- Persévérance

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso. Par ailleurs, nous vous proposons une formation pluriannuelle sur le domaine de la Lutte Informatique Défensive.



2023-LID-04

Architecte Solution Lutte Informatique Défensive



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

LID TTP SOC IDS NIDS HIDS SIEM
Architecte

Description du poste (H/F)

Mission : En relation avec les experts, les opérationnels du ministère des armées et les industriels du domaine LID, piloter l'ensemble des activités d'un projet de mise en place de capacités LID : analyser le besoin métier des opérationnels, concevoir les architectures, élaborer les exigences contractuelles, piloter les activités de choix techniques, suivre la réalisation et le déploiement des capacités.

Contexte : Dans le cadre du renfort de ses activités de conduite de projets techniques dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur architecte solution LID.

Compétences métiers

- Architecture de système de LID.
- Gestion de projet au sein d'une équipe pluridisciplinaire.
- Intégration système et produit de solutions LID.
- Solutions de détection d'intrusion et supervision de la sécurité : sondes de détection d'intrusion (Réseau, Hôte), SIEM, outils de visualisation et aide à la décision, composants d'un SOC, ...

Compétences souhaitées

- Travail en équipe
- Esprit de synthèse
- Autonomie
- Animation de réunion
- Proactivité

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.



2023-SCY-01

Ingénieur Cryptographie – Spécification d’algorithmes



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cryptographie Protocoles

Description du poste (H/F)

Mission : Concevoir et spécifier des protocoles cryptographiques, fournir une expertise au profit des programmes d’armement, et vous maintenir à l’état de l’art sur le domaine de la cryptographie.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l’Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur en cryptographie.**

Compétences métiers

Vous justifiez de compétences dans le domaine des protocoles et des preuves de sécurité.

Compétences souhaitées

- Expérience minimale en programmation
- Architecture de système d’exploitation
- Maîtrise l’anglais technique (littérature scientifique)

Qualités personnelles :

- Autonomie
- Curiosité
- Adaptation
- Rigueur

Les “+” du poste

Dans le cadre de vos fonctions, vous serez amené à interagir avec le monde universitaire. Pour cette raison, une connaissance de cet environnement constituera un avantage pour ce poste. Vous intégrez une équipe jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.



2023-SCY-02

Ingénieur Cryptographie – Spécification d’algorithmes



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cryptographie Chiffrement symétrique
Statistiques

Description du poste (H/F)

Mission : Concevoir et spécifier des algorithmes de cryptographie symétrique, fournir une expertise au profit des programmes d’armement, et vous maintenir à l’état de l’art sur le domaine de la cryptographie. Fournir une expertise en statistiques et génération d’aléa.

Contexte : Dans le cadre du développement de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l’Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur en cryptographie**.

Compétences métiers

- Cryptographie symétrique
- Connaissance solides en mathématiques

Compétences souhaitées

- Intérêt pour les statistiques
- Expérience minimale en programmation
- Architecture de système d’exploitation
- Maîtrise l’anglais technique (littérature scientifique)

Qualités personnelles :

- Autonomie
- Curiosité
- Adaptation
- Rigueur

Les “+” du poste

Dans le cadre de vos fonctions, vous serez amené à interagir avec le monde universitaire. Pour cette raison, une connaissance de cet environnement constituera un avantage pour ce poste. Vous intégrez une équipe jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.



2023-SCY-03

Ingénieur Cyberdéfense – Recherche de vulnérabilités cryptographiques dans des produits logiciels



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

C Cryptographie Analyse de code
Développeur Debugger IDA Ghidra
Reverse Exploit

Description du poste (H/F)

Mission : Recherche et exploitation de vulnérabilités cryptographiques dans des produits logiciels.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une experte en **recherche de vulnérabilités cryptographiques**.

Compétences métiers

- Algorithmes et protocoles cryptographiques
- Cryptographie symétrique, asymétrique, fonctions de hachage
- Vulnérabilités classiques liées à l'implémentation de la cryptographie
- Langages C/C++
- Langage assembleur (au moins un)
- Analyse de code
- Débogage
- Analyse de binaire et rétro-conception

Compétences souhaitées

- Langage Python
 - Langage script
 - Sécurité logicielle
 - Qualité logicielle
 - Réseau
- Qualités personnelles :
- Autonomie
 - Curiosité
 - Force de proposition
 - Organisation

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité tout en bénéficiant d'un cadre de vie privilégié.



2023-SCY-04

Ingénieur Conception de logiciel embarqué et sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

C Cryptographie Développeur Systèmes
embarqués Sécurité logicielle

Description du poste (H/F)

Mission : Conception et développement de logiciels embarqués sur des composants de sécurité. Plus précisément :

- Spécifier et développer des modules logiciels cryptographiques.
- Accompagner les équipes de conception logicielle pendant les phases d'architecture.
- Accompagner les équipes de développement logiciel pour rechercher et analyser les failles dans les implémentations.
- Garantir la sécurité des implémentations.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une experte en développement de logiciels de sécurité et cryptographie**.

Compétences métiers

- Langage C et assembleur
- Connaissances en cryptographie et en services de sécurité
- Sécurité des implémentations cryptographiques

Compétences souhaitées

- Sécurité des composants (attaques en faute, canaux auxiliaires)
- Conception logicielle
- Sécurité logicielle
- Qualité logicielle

Qualités personnelles :

- Autonomie
- Rigueur
- Organisation
- Communication
- Savoir s'affirmer dans un cadre d'équipes pluridisciplinaires

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité tout en bénéficiant d'un cadre de vie privilégié.



2023-SCY-05

Ingénieur Conception matérielle Cryptographie et Sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

FPGA ASIC Cryptographie Systèmes
embarqués Sécurité des composants

Description du poste (H/F)

Mission : Le titulaire participera au suivi de la conception matérielle des composants de sécurité de défense et entretiendra un état de l'art et une expertise sur le domaine des composants, des fonctions de sécurité et de l'implémentation de la cryptographie.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur Conception matérielle Cryptographie et Sécurité.**

Compétences métiers

- Langage HDL (VHDL, Verilog, ...)
- Connaissances en cryptographie et en services de sécurité
- Sécurité des composants (types d'attaque, mécanismes de protection)

Compétences souhaitées

- Architecture des composants
- Conception logiciel embarqué (langage C)

Qualités personnelles :

- Autonomie
- Curiosité
- Communication
- Savoir s'affirmer dans un cadre d'équipes pluridisciplinaires

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité tout en bénéficiant d'un cadre de vie privilégié. Vos compétences seront mises à profit au sein d'une équipe d'experts pluridisciplinaires en charge de la réalisation des produits de sécurité du ministère des armées.





2023-SDA-01

Directeur de projets Cyber



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cyberdéfense Projets Stratégie

Description du poste (H/F)

Mission : Le titulaire du poste doit assurer l'analyse et la prise en compte des besoins du client, élaborer la réponse, conduire les projets dans leurs dimensions technique, économique, calendaire et dans le respect des engagements pris vis à vis du client, piloter le retour d'expérience pour contribuer efficacement à l'élaboration des prévisions de prestations futures.

Il s'agit d'assurer :

- l'intégration des projets dans la production cyber du centre
- les travaux prospectifs visant à définir la feuille de route du domaine
- le pilotage et l'animation d'équipes pluridisciplinaires en participant directement aux travaux
- la vérification de la conformité des prestations avec les exigences du client
- le développement et la reconnaissance de ses collaborateurs.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une Directeur/Directrice de projets.**

Compétences métiers

- Pilotage de projets
- Management d'équipes
- Collecte, analyse du besoin et négociation
- Elaboration de la stratégie Cyber du domaine

Compétences souhaitées

- Capacité d'analyse, ingéniosité, inventivité, curiosité, ténacité
- Goût du travail en équipe, intérêt affirmé pour l'innovation

Qualités personnelles :

- Rigueur, organisation, autonomie et curiosité
- Capacité à s'intégrer dans une équipe
- Facilité d'adaptation nouveaux contextes techniques et humains

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Vous travaillerez avec des équipes projets à échelle humaine (3 à 6 personnes), travaillerez en méthodes Agiles (sprints de 2 à 4 semaines) et suivrez une formation initiale sur nos métiers de la cyberdéfense.



2023-VIM-01

Ingénieur Retro-conception en systèmes embarqués



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra Exploit Fuzzing ASM

Description du poste (H/F)

Mission : Analyse de binaires spécifiques aux systèmes embarqués afin d'en comprendre l'architecture et le fonctionnement, recherche de vulnérabilités dans ces binaires et mise au point de preuves de concept pour en démontrer leur exploitabilité.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur en retro-conception en systèmes embarqués.

Compétences métiers

- Connaissance en assembleur (ARM, MIPS...)
- Développement C, python
- Désassembleurs, debuggers
- Radio logicielle

Compétences souhaitées

- Techniques de recherche de vulnérabilités
- Systèmes embarqués, temps réel
- Méthodes de protection logicielles
- Architecture d'OS embarqués, cross-compilation

Qualités personnelles :

- Curieux, innovant, à la recherche de nouveaux défis, autonome
- Tenace, persévérant

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste. Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.



2023-VIMVMAXVMEN-01

Ingenieur Retro-conception en système d'exploitation



Niveau requis

Ingenieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra Exploit Fuzzing
Windows Linux Android

Description du poste (H/F)

Mission : Analyse de logiciels binaires afin d'en comprendre l'architecture et le fonctionnement, recherche de vulnérabilités dans ces logiciels et mise au point de preuves de concept pour en démontrer leur exploitabilité.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur débutant ou avec expérience en retro-conception de binaires.

Compétences métiers

- Recherche de vulnérabilités
- Connaissance en assembleur ARM ou x86/x64
- Développement d'outils d'aide à la retro ingénierie
- Veille techno. régulière

Compétences souhaitées

- Maîtrise au minimum d'un OS standard (Windows, Linux, iOS, Android)
- Développement C/C++, Python
- Développement bas niveau
- Désassembleurs et débogueurs

Qualités personnelles :

- Curieux, innovant, à la recherche de nouveaux défis, autonome
- Persévérant

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.



2023-VIMVMAXVMEN-03

Ingénieur Retro-conception système virtualisé



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra Exploit Fuzzing Cloud
Virtualisation

Description du poste (H/F)

Mission : Analyse de logiciels binaires afin d'en comprendre l'architecture et le fonctionnement, recherche de vulnérabilités dans ces logiciels et mise au point de preuves de concept pour en démontrer leur exploitabilité.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur débutant ou avec expérience en retro-conception de binaires.

Compétences métiers

- Recherche de vulnérabilités
- Connaissance en assembleur ARM ou x86/x64
- Développement d'outils d'aide à la retro ingénierie
- Veille techno. régulière

Compétences souhaitées

- Maîtrise au minimum d'une solution de virtualisation
- Développement C/C++, Python
- Désassembleurs et débogueurs

Qualités personnelles :

- Curieux, innovant, à la recherche de nouveaux défis, autonome
- Persévérant

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.



2023-VMAT-01

Ingénieur Retro-conception et analyse de format de données



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse Windows Linux Fichier Protocoles

Description du poste (H/F)

Mission : Analyse et rétro-conception de format de données propriétaires, tels que formats de fichiers, protocoles réseau, ... et développement de preuves de concept.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur en retro-conception et analyse de format de données.

Compétences métiers

- Bonnes connaissances des systèmes d'exploitation ;
- Manipulation de données binaires ;
- Développement Python/Ruby et au moins un langage compilé ;
- Notions de reverse-engineering ;

Compétences souhaitées

- Bonne connaissance d'au moins un moteur de bases de données ;
- Automatisation de génération et de parsing de données ;
- Maîtrise d'un langage de script système (powershell, shell, etc.) ;
- Connaissances de protocoles réseau et dissection.

Qualités personnelles :

- Curieux, innovant, à la recherche de nouveaux défis, autonome
- Persévérant

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste. Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

De plus, nous vous offrons un cadre de vie privilégié avec notamment notre site en pleine nature...



2023-VMAT-02

Ingénieur Cyberdéfense en tests d'intrusion



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Tests d'intrusion Vulnérabilités Pentest
Sécurité offensive TTP

Description du poste (H/F)

Mission : Réalisation de test d'intrusion sur systèmes réels. Recherche et exploitation de vulnérabilités systèmes, réseaux, web. R&D relative aux tests d'intrusion.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur en tests d'intrusion.

Compétences métiers

- Bonnes connaissances des méthodes et outils de tests d'intrusion (cartographie, analyse, exploitation, rebond, ...);
- Connaissances de base en techniques de recherche et d'exploitation de vulnérabilités ;
- Adaptation de codes d'exploitation permettant de démontrer l'exploitabilité de vulnérabilités ;
- Connaissance en développement (Python et/ou C et/ou Java)

Compétences souhaitées

- Bonnes connaissances en OS et leur administration (Windows, Linux, Android...);
- Bonnes connaissances applicatives (Active Directory, LDAP, Serveurs Web, Serveurs de messagerie, DNS, SGBD, applications de sécurité (HIDS, NIDS, Antivirus, produit de supervision...), etc.);
- Bonnes connaissances en technologies réseaux et protocoles associés ;
- Développement Python, C/C++, Java, C#

Qualités personnelles :

- Inventif, curieux, passionné, esprit d'équipe, persévérant

Les "+" du poste

Nous privilégions le travail en équipe, le partage de connaissances et disposons de formations spécialisées (SANS, Offensive Security, ...) ainsi que des formations internes spécifiques aux métiers du reverse-engineering. Du temps de veille est aussi disponible afin de favoriser les démarches autodidactes.

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

De plus, nous vous offrons un cadre de vie privilégié avec notamment notre site en pleine nature...



2023-VMAT-03

Ingénieur Retro-conception et analyse de malwares



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra Exploit Protocoles
Malware Analysis

Description du poste (H/F)

Mission : Rétro-conception et analyse de code malveillants. Analyse d'attaques émergentes et de leurs infrastructures. Capitaliser des connaissances sur les modes opératoires d'attaque et leurs techniques et outils.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur débutant ou avec expérience en retro-conception et analyse de malwares.

Compétences métiers

- Analyse de malwares
- Connaissance d'au moins un assembleur
- Développement C/C++
- Désassembleurs et debuggers
- Développement Python

Compétences souhaitées

- Connaissance de l'architecture d'OS standards (Windows, Linux, Android)
- Connaissances de protocoles
- Méthodes de protection logicielles (stack cookies, ASLR, SMEP, DEP...) et contournement
- Recherche de vulnérabilités exploitables

Qualités personnelles :

- Curieux, innovant, à la recherche de nouveaux défis, autonome
- Persévérant

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste. Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

De plus, nous vous offrons un cadre de vie privilégié avec notamment notre site en pleine nature...



2023-VMAT-04

Ingénieur Cyberdéfense – Recherche de vulnérabilités Web



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Vulnérabilités Web Développeurs PHP
Ruby JAVA Python Docker OWASP

Description du poste (H/F)

Mission : Rechercher des vulnérabilités Web (boîte blanche), développer des POC, scénarios, automatiser, s'outiller, ...

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), **recrutent un ou une ingénieur en recherche de vulnérabilités Web.**

Compétences métiers

- Analyse connaître les principales classes de vulnérabilités telles que LFI/RFI, SQLi, XSS, XXE...
- Avoir de " bonnes bases " de développement Web (PHP et/ou Java...)
- Audit de code, bases de pentest
- En bonus : administration et durcissement d'architectures Web

Compétences souhaitées

- Scripting (python, bash, ...)
 - Sécurité informatique
 - Docker
- Qualités personnelles :
- Ténacité, Curiosité, Esprit d'équipe, Rigueur

Les "+" du poste

Nous privilégions le travail en équipe, le partage de connaissances et disposons de formations internes pour monter en compétences ainsi que des formations " privées " très spécialisées. Du temps de veille est aussi disponible si l'on veut évoluer de manière autodidacte...

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

De plus, nous vous offrons un cadre de vie privilégié avec notamment notre site en pleine nature...



2023-VMAX-01

Ingénieur Retro-conception en produits logiciels Windows



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse Vulnérabilités Exploit Windows

Description du poste (H/F)

Mission : Expert en rétro-conception et recherche de vulnérabilités sur des logiciels fonctionnant sous Windows. Compréhension et documentation du système, analyse de la surface d'attaque, développement de preuves de concept.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur en recherche de vulnérabilités sur des logiciels fonctionnant sous Windows.

Compétences métiers

- Bonne connaissance du système Windows
- Maîtrise des méthodes et outils de rétro-conception de binaires
- Expérience en recherche de vulnérabilités

Compétences souhaitées

- Processeurs Intel x86/x64 (assembleur)
 - Développement C/C++, Python
- Qualités personnelles :
- Ténacité, Curiosité, Esprit d'équipe, Rigueur

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste. Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.

En choisissant ce poste, vous intégrerez une équipe soudée, heureuse de transmettre et aide d'apprendre, vous profiterez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

Vous apprécierez aussi un cadre de vie privilégié avec notamment notre site en pleine nature...



2023-VMEN-01

Ingenieur Retro-conception en système Android Linux



Niveau requis

Ingenieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra Exploit Fuzzing
Android Linux

Description du poste (H/F)

Mission : Analyse de logiciels binaires afin d'en comprendre l'architecture et le fonctionnement, recherche de vulnérabilités dans ces logiciels et mise au point de preuves de concept pour en démontrer leur exploitabilité.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur débutant ou avec expérience en retro-conception de binaires.

Compétences métiers

- Recherche de vulnérabilités
- Connaissance en assembleur ARM ou x86/x64
- Développement d'outils d'aide à la retro ingénierie
- Veille techno. régulière

Compétences souhaitées

- Maîtrise au minimum d'un OS standard (Windows, Linux, iOS, Android)
- Développement C/C++, Python
- Développement bas niveau
- Désassembleurs et débogueurs

Qualités personnelles :

- Curieux, innovant, à la recherche de nouveaux défis, autonome
- Persévérant

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.



2023-VMEN-02

Ingénieur Retro-conception en système iOS



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra Exploit Fuzzing iOS

Description du poste (H/F)

Mission : Analyse de logiciels binaires afin d'en comprendre l'architecture et le fonctionnement, recherche de vulnérabilités dans ces logiciels et mise au point de preuves de concept pour en démontrer leur exploitabilité.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur débutant ou avec expérience en retro-conception de binaires.

Compétences métiers

- Recherche de vulnérabilités
- Connaissance en assembleur ARM
- Développement d'outils d'aide à la retro ingénierie
- Veille techno. régulière

Compétences souhaitées

- Développement C/C++, Python
 - Développement bas niveau iOS
 - Désassembleurs et débogueurs
- Qualités personnelles :
- Curieux, innovant, à la recherche de nouveaux défis, autonome
 - Persévérant

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.

Vous bénéficierez d'une formation interne spécifique aux métiers reverse-engineering dispensée par les experts de DGA-MI.



2023-XCS-01

Ingénieur Evaluation et expertise de la sécurité de composants



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Electronique FPGA Embarqué ASIC Python
Cryptographie

Description du poste (H/F)

Mission : Expertiser la sécurité de composants et sous modules électroniques utilisés par le ministère des Armées au sein de ses programmes.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur-e en évaluation et expertise de la sécurité de composants.

Expert technique, vous interviendrez sur l'ensemble des fonctions du composant (du niveau transistor au logiciel embarqué en passant par les fonctions électroniques) afin d'évaluer la sécurité des composants vis-à-vis d'attaques matérielles et logicielles. Vous êtes amené à travailler en étroite collaboration avec les équipes en charge de la conception et de l'implémentation des composants cryptographiques gouvernementaux. Votre travail vous amènera à nouer des contacts avec tous les acteurs publics ou privés du domaine. Vous travaillerez en relation avec des électroniciens, informaticiens, cryptographes et des experts en physique des composants.

Compétences métiers

- Expertise en sécurité et/ou conception de composants électroniques (FPGA, ASIC, microcontrôleur)
- Electronique numérique
- Informatique embarquée (firmware)
- Langages C et Python

Compétences souhaitées

- Cryptographie
 - Bonus : compétences en intelligence artificielle
- Qualités personnelles :
- rigueur, de l'autonomie, de la persévérance et de l'initiative de votre part

Les "+" du poste

Vous intégrerez une équipe dynamique composée d'une vingtaine d'experts de haut niveau et profiterez du savoir-faire et des moyens uniques de DGA MI dans le domaine innovant de la cybersécurité.



2023-XEL-01

Ingénieur Expert en sécurité logiciel



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeurs Analyse statique Analyse
dynamique C C++ Python Rust JAVA

Description du poste (H/F)

Mission : Garantir l'absence de vulnérabilités dans les logiciels de sécurité du ministère des Armées.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une expert.e en sécurité logiciel**.

Au sein d'une équipe pluridisciplinaire spécialisée, vous aurez la charge d'analyser les constituants de produits de sécurité. Vous vérifierez la robustesse du produit face aux attaques que vous aurez imaginées afin de démontrer l'exploitabilité des vulnérabilités identifiées. Vous travaillerez sur différentes technologies et plateformes, auprès de spécialistes qui vous guideront pour une montée en compétence et un maintien à niveau dans des domaines techniques de pointe.

Compétences métiers

- Expertise en développement logiciel
- Expertise en langage C
- Analyse statique de code
- Analyse dynamique de code

Compétences souhaitées

- Compétences techniques :
- Connaissances sur les langages C++, Java, Python, Assembleur x86 et ARM, Rust
- Connaissances sur les systèmes Windows, Linux, iOS ou/et Android
- Cryptographie
- Sécurité informatique

Qualités personnelles :

- Curiosité
- Autonomie
- Persévérance
- Esprit d'équipe

Les "+" du poste

Vous intégrerez une équipe dynamique composée d'une vingtaine d'experts de haut niveau et profiterez du savoir-faire et des moyens uniques de DGA MI dans le domaine innovant de la cybersécurité.



2023-XEO-01

Ingénieur Cyberdéfense test et validation



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cyberdéfense Test Automatisation
Qualification Validation Intégration

Description du poste (H/F)

Mission : Concevoir et conduire des campagnes de tests de logiciels de cyberdéfense pour s'assurer de leur bon fonctionnement et de leur stabilité. Pour chaque projet vous travaillerez en équipe pluridisciplinaire en étroite collaboration avec les développeurs du logiciel à qualifier. A ce titre vous devrez notamment à :

- Définir la stratégie de validation ;
- Concevoir et exécuter les tests fonctionnels, de non-régression, d'endurance, etc... ;
- Mettre en place l'intégration et l'automatisation des tests, participer à la mise en œuvre des plateformes de qualification ;
- Suivre les anomalies ;
- Rédiger les rapports de test ;
- Communiquer vers l'ensemble des acteurs concernés.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **des ingénieur.e.s test et validation**.

Compétences métiers

Vous avez une forte appétence pour le métier du test, vous disposez d'une bonne capacité d'apprentissage du métier et des processus du test logiciel ou vous justifiez déjà d'une expérience dans le domaine du test logiciel, vous disposez de bonnes connaissances en Python et de connaissances dans le déploiement d'environnements virtualisés.

Compétences souhaitées

Qualités personnelles :

- Rigueur, organisation et curiosité
- Capacité à s'intégrer dans une équipe
- Facilité d'adaptation nouveaux contextes techniques et humains

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et vous bénéficiez du savoir-faire et des moyens de DGA MI dans le domaine innovant et passionnant de la cybersécurité. Vous intégrerez des équipes projets à échelle humaine (3 à 6 personnes) et travaillerez en méthode Agile (sprints de 2 à 4 semaines).



2023-XIN-01 Ingénieur Investigation Numérique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Forensic R&D Investigation numérique DFIR

Description du poste (H/F)

Mission : Analyser la furtivité des outils de cybersécurité produits à DGA-MI, en caractérisant l'empreinte de ces outils (mémoire, disque, réseau, etc.) sur des environnements multiples, mener des analyses d'investigation numérique sur des environnements variés et analyser les limites des outils de détection d'intrusion.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ou une ingénieur** en investigation numérique.

Compétences métiers

- Connaissances DFIR, notamment les artefacts forensiques
- Pratique des outils d'investigation numérique (The Sleuth Kit, Volatility, Sysinternals, Wireshark, Jadx ...)
- Développement de preuves de concept (Python, C/C++, ...)
- Matrice ATT&CK et implémentation des techniques associées
- Connaissance du comportement des malwares et des techniques d'analyses
- Notions sur les outils de détection d'intrusion (EDR, SIEM, ...)

Compétences souhaitées

- Connaissance approfondie du fonctionnement des OS standards (Windows, Linux, Android)
- Sécurité Informatique
- Fonctionnement des protocoles réseau courants

Qualités personnelles :

- Curiosité
- Autonomie, persévérance
- Force de proposition
- Bonne capacité de rédaction/restitution

Les "+" du poste

En choisissant ce poste, vous suivrez une formation initiale de 1 mois sur notre métier, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité, vous intégrez une équipe dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité.



2023-XIP-01

Ingenieur developpement logiciel systemes embarques



Niveau requis

Ingenieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Sécurité Cybersécurité Embarqué
Vulnérabilités Logiciel

Description du poste (H/F)

Mission : Analyser l'architecture et le fonctionnement de systèmes embarqués. Rechercher des vulnérabilités en définissant et exécutant un plan de test. Développer des outils pour rechercher des vulnérabilités (émulation, fuzzing, tests spécifiques).

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions de cybersécurité de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ingénieur développement logiciel systèmes embarqués**.

Intégré à une équipe dynamique dont la mission principale est d'évaluer le niveau de sécurité d'équipements de systèmes d'information du Ministère des Armées, vous aurez en charge l'analyse et le test de systèmes embarqués afin d'en rechercher les vulnérabilités.

Vous devrez aussi faire preuve d'innovation en faisant évoluer les méthodes les outils et méthodes d'évaluation.

Compétences métiers

- Maîtrise de langages de programmation (C, C++, asm, Python...) et de leurs environnements (OS, hyperviseur, cross-compilation...) sur systèmes embarqués.
- Connaissance des CPLD/FPGA, et du langage VHDL.
- Maîtrise des protocoles courants pour le fonctionnement des services réseaux (ARP, IPv4/IPv6, TCP/UDP, SNMP, ...) et des protocoles de sécurité (IPSEC, ...).
- Maîtrise d'outils de type émulateur, débogueur et analyseur de protocoles.
- Mise en œuvre de méthodologies de revue de code

Compétences souhaitées

- Mise en œuvre de méthodologies de tests dans l'objectif de rechercher des vulnérabilités.
- Mise en œuvre d'outils de fuzzing logiciel et de protocole.
- Lecture de schémas électroniques, analyse du routage

Qualités personnelles :

- Capacité d'analyse,
- Initiative, Goût du travail en équipe
- Curiosité, Intérêt pour l'innovation



2023-XIP-02

Ingénieur électronique spécialisé en systèmes embarqués



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Sécurité Cybersécurité Embarqué GNSS
GPS Gallileo Radio-navigation

Description du poste (H/F)

Mission : Analyser l'architecture et le fonctionnement de systèmes embarqués. Vérifier la conformité à des guides d'implémentation. Examiner le processus de développement et de production industriel. Collaborer à l'élaboration de guides de référence.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions de cybersécurité de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ingénieur électronique spécialisé en systèmes embarqués**.

Intégré à une équipe dynamique, dont la mission principale est d'évaluer le niveau de sécurité d'équipements et de systèmes du Ministère des Armées, vous menez des expertises au profit de systèmes d'armes de pointe (missiles, frégates, avions, ...), dans un contexte industriel, opérationnel et international, sur l'aspect de la sécurité des radio-navigations par satellite.

Compétences métiers

- Lecture de schémas électroniques et connaissance des composants standards.
- Maniement de langages de programmation (C, C++, asm, Python...) et de leurs environnements (OS, compilation, IDE, ...) sur systèmes embarqués.
- Connaissance des CPLD/FPGA, et maniement du langage VHDL.
- Connaissance des protocoles d'échange électronique (RS232, ARINC, 1553, UART, I2C, ...).
- Maniement d'outils de type debugueur, analyseur de protocoles et analyseur de code

Compétences souhaitées

- Systèmes de radionavigation par satellites.
- Systèmes d'armes.
- Outils de gestion de développement et de configuration logiciel (GIT, MyPLM, DOORS, ...).
- Sécurité des systèmes d'information.
- Cryptographie.

Qualités personnelles :

- Polyvalence, curiosité
- Rigueur
- Réactivité
- Esprit de collaboration

Permis de conduire de véhicules de catégorie B indispensable.



2023-XIP-03 Ingénieur radio-logicielle



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Sécurité Cybersécurité Radiofréquence
Radiologicielle Vulnérabilités SDR
Traitement du signal

Description du poste (H/F)

Mission : Etudier des protocoles radiofréquences d'échange de données. Analyser les couches bas niveau (ISO 1/2). Développer des prototypes sur la base de plateformes radio-logicielles. Rechercher des vulnérabilités sur des protocoles de communication aux interfaces radiofréquences.

Contexte : Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions de cybersécurité de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent **un ingénieur radio-logicielle**.

Intégré dans une équipe dynamique et innovante dont la principale mission est d'évaluer la sécurité des interfaces radio, vous mènerez des analyses sur les couches basses protocolaires de systèmes de communication.

Vous serez ainsi amené à étudier des protocoles d'échange de données et à développer des plateformes à base de radio-logicielles

Compétences métiers

- Maîtrise de systèmes de communication radio (traitement du signal, modulation, ...)
- Développement radio-logicielle
- Analyse de protocoles (à partir d'outils comme Wireshark, Scapy)
- Développement embarqué
- Rétro-ingénierie de firmware

Compétences souhaitées

- Méthodologie d'analyse
- Sécurité des systèmes d'information
- Langages informatiques usuels (C, Matlab, Python, VHDL...)
- Utilisation d'équipements de mesure (antennes, analyseur de spectre, oscilloscope, ...)

Qualités personnelles :

- Capacité d'analyse, ingéniosité, inventivité, curiosité, ténacité
- Goût du travail en équipe, intérêt affirmé pour l'innovation



2023-XIP-04 Ingénieur électronique radio



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Sécurité Cybersécurité Radiofréquence
Radiologicielle Vulnérabilités SDR
Traitement du signal TEMPEST SPC

Description du poste (H/F)

Mission : Analyser des phénomènes électromagnétiques liés à l'utilisation de systèmes de traitement de l'information. Piloter des essais de matériels et de plateformes. Rechercher des vulnérabilités électromagnétiques.

Contexte Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions Cyber de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un **ingénieur électronique radio**.

Intégré dans une équipe dynamique dont la principale mission est de mener une activité d'évaluation, de recherche et de développement en Cyberdéfense pour le compte du Ministère des Armées dans le domaine des phénomènes électromagnétiques, vous serez amené à :

- Piloter des campagnes de tests TEMPEST sur des matériels et plateformes en laboratoire ou sur le territoire national et à l'étranger,
- Réaliser des outils à base de récepteurs radiofréquence ou radio-logiciel,
- Participer à des projets de recherche et d'ingénierie dans le domaine de la radio.

Compétences métiers

- Maîtrise de l'électronique analogique et numérique
- Maîtrise de systèmes de communication radio (traitement du signal, modulation, ...)
- Développements radio-logicielle
- Connaissance de l'électromagnétisme
- Utilisation d'équipements de mesure (antennes, analyseur de spectre, oscilloscope, ...)

Compétences souhaitées

- Langages informatiques usuels (C, C++, Matlab, Python, VHDL, ...)
- Méthodologie de test
- Sécurité des systèmes d'information
- Anglais

Qualités personnelles :

- Ingéniosité, curiosité, intérêt affirmé pour l'innovation
- Goût de l'expérimentation et du travail en équipe
- Capacité d'analyse et de synthèse
- Rigueur, discrétion

Permis de conduire de véhicules de catégorie B indispensable.





Index

5G.....	22
AD.....	42
Administration système	12, 38, 45, 46
Agile.....	19, 26, 27, 28
Analyse de code	49
Analyse dynamique.....	64
Analyse statique	64
Analyses.....	12, 30
Android	22, 23, 54, 61
Ansible.....	33, 42
Architecte	18, 25, 26, 43
Architecture.....	13, 14, 21, 27, 28
ASIC.....	51, 63
ASM.....	53
Atlassian	20
Audit	15, 16, 17
Automates	37
Automatisation	65
Backup	40
BigData	22, 29, 30, 33
Build.....	39
C.....	23, 44, 49, 50, 64
C++	64
Capitalisation.....	34
Chef de Projet	26, 52
Chiffrement symétrique	48
CI	39
Cloud.....	22, 27, 28, 55
Compilation.....	39





Conception	13
Confluence.....	20
Containerisation.....	22
Cryptographie.....	18, 47, 48, 49, 50, 51, 63
Debugger	49
Détection.....	45
Détection intrusion	44
Développeur.....	19, 22, 23, 24, 31, 32, 49, 50, 59, 64
DevSecOps	27, 28, 39, 41
DFIR	66
Docker	33, 41, 42, 59
EBIOS	25, 26
Elasticsearch.....	29, 33
Electronique	63
Embarqué	18, 22, 24, 37, 63, 67, 68
Expertise.....	12
Exploit.....	49, 53, 54, 55, 58, 60, 61, 62
Exploitation.....	36
Fichier.....	56
Fingerprint.....	30
Forensic.....	66
FPGA	51, 63
FullStack	32
Fuzzing.....	53, 54, 55, 61, 62
Gallileo.....	68
Gestion de projets.....	19
Ghidra	49, 53, 54, 55, 58, 61, 62
GNSS.....	68
GPS.....	68
Grafana.....	33
GTB.....	37
Hacking.....	36
Hadoop.....	29, 33





HIDS	43, 44, 46
Honeypot	44
HPC	40
Hyperviseur	14
IA	31
IaC	40
Iceberg	29
ICS	16, 36, 37
IDA	49, 53, 54, 55, 58, 61, 62
IDS	43, 46
Ingénierie	18
Intégration	65
Investigation numérique	66
Investigations	12
IoC	45
iOS	22, 23, 62
IoT	22, 24
ISO27001	25, 26
JAVA	23, 29, 59, 64
Jira	20
Kernel	22, 24
KnowledgeGraph	35
Kotlin	23
L2I	31, 32, 34
LAN	22
LID	43, 46
LinkedData	35
Linux	14, 22, 24, 33, 41, 42, 44, 54, 56, 61
LIO	19, 21, 34
Logiciel	67
Logiciel embarqué	14
MacOS	23
Malware Analysis	58





Modélisation.....	19, 21, 34
Multimédia.....	31
Network.....	40
NIDS.....	43, 44, 46
ObjectiveC.....	23
OS.....	14
OSINT.....	30, 34
OWASP.....	59
Pentest.....	36, 57
PHP.....	59
PoC.....	13, 14
Product Owner.....	26
Protocoles.....	47, 56, 58
Python.....	23, 44, 59, 63, 64
Qualification.....	65
Radiofréquence.....	69, 70
Radiologicielle.....	69, 70
Radio-navigation.....	68
RedTeam.....	22, 23, 24
Réseau.....	38
Reverse.....	49, 53, 54, 55, 56, 58, 60, 61, 62
Ruby.....	59
Rust.....	14, 64
Sandbox.....	14
Sandbox.....	44
SCADA.....	16, 36, 37
SCALA.....	29
Scénarios.....	21
SCI.....	16
SDN.....	40
SDR.....	69, 70
Sécurité des composants.....	51
Sécurité logicielle.....	50





Sécurité offensive	57
SIEM.....	12, 43, 44, 45, 46
Smartcities.....	36
Snort	44
SOC.....	12, 43, 45, 46
Spark.....	29, 33
SPC.....	70
Statistiques.....	48
Storage	40
Stratégie	52
Supervision	12
Supervision	20
Suricata	44
Swift	23
Système d'information	26
Systèmes embarqués	13, 50, 51
Systèmes industriels.....	37
Systèmes informatiques.....	38
TAL	31
Telecom	36
TEMPEST.....	70
Test.....	65
Tests d'intrusion.....	57
Traitement du signal	69, 70
TTP	43, 46, 57
Validation	65
VDI	40, 42
Virtualisation.....	38, 41, 55
VMWare.....	38, 40
Vulnérabilités.....	14, 15, 16, 17, 36, 57, 59, 60, 67, 69, 70
Web	59
Windows.....	22, 44, 54, 56, 60
WinSrv	42

