



Métiers Cyber

Panorama 2026



DGA MAÎTRISE DE L'INFORMATION

136, La Roche Marguerite 35170 BRUZ

www.defense.gouv.fr/dga/recrutement/recrutement-cyberdefense-dga



Sommaire

- Edito p. 3
- Direction Générale de l'Armement p. 4
- DGA Maîtrise de l'information p. 4
- Un poste à DGA MI p. 5
- Venez nous rencontrer ! p. 5
- Comment postuler ? p. 6
- Fiches de postes p. 7
- Index par mots-clés ...fin



« **DGA Maîtrise de l'information** est un centre apprécié de ses partenaires, qui reconnaissent largement la qualité de son expertise unique et de ses prestations.

*Avec notre positionnement sur des technologies d'avenir, nous sommes très engagés auprès des forces et des industriels au service de la supériorité de nos armées et de la souveraineté du pays : **nous comptons sur vous** pour y contribuer dès les prochains mois. »*



Frédéric Bouyer

Directeur du centre DGA Maîtrise de l'information



DIRECTION
GÉNÉRALE
DE L'ARMEMENT
— —
Maîtrise
de l'information

Force d'expertise, d'essais et d'ingénierie au sein du ministère des Armées, la DGA a pour missions d'**équiper les armées** de façon souveraine, de **préparer le futur** des systèmes de défense, de **promouvoir la coopération européenne** et de **soutenir les exportations**.

Combat terrestre naval, aérien, systèmes électroniques de communication et d'information, dissuasion, espace, cyber-sécurité, robotique, etc.

Avec 18 sites en France, ses 10 200 femmes et hommes **civils** ou **militaires**, dont près de 60% **cadres, ingénieurs** ou **experts**, et son réseau de collaborateurs à l'international, la DGA intervient dans tous les domaines de la défense.



DGA Maîtrise de l'information

Depuis 1968, DGA Maîtrise de l'information (anciennement CELAR) intervient sur l'ensemble des programmes d'armement et sur tout leur cycle.

La mission de DGA MI est d'apporter son **expertise technique** (contribution à la maîtrise du risque technique, capacité d'ingénierie des systèmes et systèmes de systèmes) et sa **capacité en moyens d'essais** au profit de ses clients dans ses domaines de compétences.

Son expertise s'exerce pour **tout type de milieu** (terrestre, naval, aérien, spatial, cyber)

DGA MI est un des 10 centres **d'Ingénierie d'Expertise** de la DGA.

DGA Maîtrise de l'Information c'est :

- > 50 moyens techniques
- ~300 systèmes d'information
- 95 M€ d'investissement/an en moyenne

2000
Personnels
sur le site



Un poste à DGA Maîtrise de l'information ↑ 5

Travailler à DGA Maîtrise de l'information c'est l'opportunité :

- De rejoindre des équipes d'**experts de très haut niveau**,
- D'exercer un métier technique unique, **au service de la nation**,
- De développer vos compétences dans des domaines variés.

DGA Maîtrise de l'information c'est aussi :

- Un **site naturel** arboré de 100 hectares
- Un **restaurant** d'entreprise
- Un accès facilité en **transports en commun**
- Une piste cyclable pour rejoindre le site (création en 2026)
- Des activités **extra-professionnelles** proposées sur le site : pratiques sportives, culturelles, de cohésion, ...



Venez nous rencontrer !

Nos équipes viennent à votre rencontre tout au long de l'année :

- Dans les écoles lors des **journées des étudiants** et des **forums entreprises** (Rennes, Nantes, Lannion, Brest, Lyon, Paris, Bordeaux, Laval...)
- Lors d'événements annuels comme l'**European Cyber Week** organisé à Rennes en novembre de chaque année
- À l'occasion des **compétitions CTF**



- Consultez la liste des postes sur le site de recrutement DGA, sur le site de l'APEC, sur LinkedIn
- Adressez votre CV en français, lettre de motivation et votre dernier diplôme à **dga-mi-bruz.recrutement.fct@intradef.gouv.fr**
- Préciser 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, de la nature du poste et de votre diplôme



**DIRECTION
GÉNÉRALE
DE L'ARMEMENT**
— —
Maîtrise
de l'information

Les descriptions de postes

2026-CYBER-MI-0001 Directeur de projets Cyber	10
2026-CYBER-MI-0002 Ingénieur analyste Cyberdéfense dans les systèmes d'armes	11
2026-CYBER-MI-0003 Ingénieur analyste Cyberdéfense spécialisé en lutte informatique offensive	12
2026-CYBER-MI-0004 Ingénieur analyste Cyberdéfense spécialisé dans les réseaux télécom	13
2026-CYBER-MI-0005 Expert en Ingénierie des Connaissances Data Sciences Cyber	14
2026-CYBER-MI-0006 Ingénieur Validation, Vérification et Intégration d'outils cyber offensifs	15
2026-CYBER-MI-0007 Ingénieur en investigation numérique	16
2026-CYBER-MI-0008 Chef de projet Cyber LIO	17
2026-CYBER-MI-0009 Ingénieur Intégrateur DevOps	18
2026-CYBER-MI-0010 Ingénieur Cyberoffensif Reverse engineering	19
2026-CYBER-MI-0011 Ingénieur développeur iOS ou Android cyber offensif	20
2026-CYBER-MI-0012 Développeur fullstack offensif	21
2026-CYBER-MI-0013 Techlead FullStack offensive	22
2026-CYBER-MI-0014 Ingénieur Retro-conception en produits logiciels Windows	23
2026-CYBER-MI-0015 Ingénieur Retro-conception en système Linux	24
2026-CYBER-MI-0016 Ingénieur Recherche de vulnérabilités Web	25
2026-CYBER-MI-0017 Ingénieur Développement d'outils cyber offensifs	26
2026-CYBER-MI-0018 Ingénieur électronique, radio logicielle et traitement du signal radio	27
2026-CYBER-MI-0019 Développeur systèmes embarqués	28
2026-CYBER-MI-0020 Ingénieur électronique, radio logicielle et traitement du signal radio	29
2026-CYBER-MI-0021 Développeur expérimenté Réseau et Système embarqué	30
2026-CYBER-MI-0022 Ingénieur Cyber techniques intrusives en télécommunications & systèmes industriels	31
2026-CYBER-MI-0023 Ingénieur Cyberdéfense Administration Systèmes et Réseaux	32
2026-CYBER-MI-0024 Administrateur et Analyste sécurité Cyberdéfense	33
2026-CYBER-MI-0025 ASSI Cyberdéfense	34
2026-CYBER-MI-0026 RSSI Technique Cyberdéfense	35
2026-CYBER-MI-0027 Technicien Soutien systèmes d'information	36
2026-CYBER-MI-0028 Ingénieur DevOps	37
2026-CYBER-MI-0029 Ingénieur DevOps Services Cyber	38

2026-CYBER-MI-0030 Ingénieur Cyberdéfense pour les plateformes cyber	39
2026-CYBER-MI-1001 Ingénieur en conception d'architecture logicielle de produit de sécurité	40
2026-CYBER-MI-1002 Ingénieur en conception de produit de sécurité embarqués	41
2026-CYBER-MI-1003 Ingénieur Architecte produits de sécurité	42
2026-CYBER-MI-1004 Ingénieur Conception de logiciel embarqué et sécurité	43
2026-CYBER-MI-1005 Ingénieur en cryptographie algorithmique	44
2026-CYBER-MI-1006 Ingénieur en développement et analyse de logiciels cryptographiques	45
2026-CYBER-MI-1007 Ingénieur Conception matérielle Cryptographie et Sécurité	46
2026-CYBER-MI-1008 Architecte cybersécurité systèmes d'armes	47
2026-CYBER-MI-1009 Ingénieur en architecture de sécurité pour les systèmes d'armes	48
2026-CYBER-MI-1010 Ingénieur auditeur organisationnel de la sécurité des systèmes d'information	49
2026-CYBER-MI-1011 Ingénieur auditeur technique en sécurité des systèmes (...)	50
2026-CYBER-MI-1012 Ingénieur auditeur technique de la sécurité des systèmes d'information	51
2026-CYBER-MI-1013 Architecte cybersécurité systèmes d'information	52
2026-CYBER-MI-1014 Architecte Solution cybersécurité	53
2026-CYBER-MI-1015 Ingénieur Sécurisation des systèmes d'information	54
2026-CYBER-MI-1016 Ingénieur en architecture de détection d'intrusion système	55
2026-CYBER-MI-1017 Ingénieur en techniques de détection d'intrusion	56
2026-CYBER-MI-1018 Ingénieur Cyberdéfense SOC	57
2026-CYBER-MI-1019 Chef de projet Lutte Informatique Défensive	58
2026-CYBER-MI-1020 Ingénieur en rétro-analyse de codes malveillants	59
2026-CYBER-MI-1021 Analyste en menace cyber	60
2026-CYBER-MI-1022 Data Engineer	61
2026-CYBER-MI-1023 Data Analyst	62
2026-CYBER-MI-1024 Ingénieur DevOps Big Data	63
2026-CYBER-MI-1025 Architecte L2I	64
2026-CYBER-MI-1026 Ingénieur Cyberdéfense en tests d'intrusion / TTP	65
2026-CYBER-MI-1027 Ingénieur Expert en sécurité logiciel	66
2026-CYBER-MI-1028 Ingénieur Expert en analyse de composants électroniques	67

2026-CYBER-MI-1029 Ingénieur Evaluation et expertise de la sécurité de composants _____	68
2026-CYBER-MI-1030 Expert en code embarqué de composants de sécurité _____	69
2026-CYBER-MI-1031 Expert en analyse fonctionnelle électronique _____	70
2026-CYBER-MI-1032 Administrateur Systèmes et Réseaux _____	71
2026-CYBER-MI-1033 Expert prototype système embarqué _____	72
Index _____	73

2026-CYBER-MI-0001
Directeur de projets Cyber



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Projets Stratégie

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **plusieurs Directeurs/Directrices de projets**.

Mission : Le titulaire du poste doit assurer l'analyse et la prise en compte des besoins du client, élaborer la réponse au juste niveau, 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.

Votre mission consiste à :

- L'intégration des projets dans la production cyber du centre
- Le reporting et la communication vers les services d'ingénierie et vers les services opérationnels
- 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.

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



2026-CYBER-MI-0002 Ingénieur analyste Cyberdéfense dans les systèmes d'armes



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cyber Modélisation Capitalisation LIO
Systèmes d'armes

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des analystes cyberdéfense dans les systèmes d'armes.

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

Compétences métiers

- Architectures techniques des systèmes numériques
- Communications maritimes, aéronautiques, véhicules terrestres
- 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

Profil recherché

Les attaques informatiques pouvant concerner tout le domaine du numérique, de très nombreux domaines métier/techniques sont concernés. Aussi, des connaissances métiers pointues sur des domaines précis autres que ceux de la cyber (ex : communications, maritime, aéronautique, véhicules terrestres, automates industriels, IOT, systèmes d'armes) seront également grandement appréciées.



2026-CYBER-MI-0003 Ingénieur analyste Cyberdéfense spécialisé en lutte informatique offensive



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

OSINT Modélisation Capitalisation LIO
Internet Scapping Veille DataMining

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des analystes cyberdéfense en lutte informatique offensive**.

Mission : Le titulaire est en charge des analyses nécessaires à la préparation du développement d'outils au profit de la lutte informatique offensive. Sur le domaine de l'IT (technologies de l'information), il capitalise les informations nécessaires à la compréhension et l'identification de la surface d'attaque du système, puis il contribue à l'élaboration des scénarii d'attaque et à la réalisation de capacités de lutte informatique offensives.

Le titulaire doit aussi posséder une expertise en OSINT et est capable de développer des outils automatisant les recherches, la veille, le scrapping web, ainsi que la mise en valeur des données pour les commanditaires des recherches.

Compétences métiers

- Architectures techniques des systèmes numériques
- Systèmes d'information
- Bases de données
- Architecture web
- Services cloud
- 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

Profil recherché

Les attaques informatiques pouvant concerner tout le domaine du numérique, de très nombreux domaines métier/techniques sont concernés. Aussi, des connaissances métiers pointues sur des domaines précis autres que ceux de la cyber (ex : communications, maritime, aéronautique, véhicules terrestres, automates industriels, IOT, systèmes d'armes) seront également grandement appréciées.



2026-CYBER-MI-0004

Ingénieur analyste Cyberdéfense spécialisé dans les réseaux télécom



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Réseaux Telecom Modélisation
Capitalisation LIO

Description du poste (H/F)

Contexte : Dans le cadre 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), emploie **des ingénieur(e)s analystes cyberdéfense dans les réseaux telecom.**

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

Compétences

- Architecture réseau, réseaux informatiques et télécoms, protocoles de communication réseau
- Architectures techniques des systèmes numériques
- Recherche d'information et analyse de documentation
- Capitalisation et représentation de l'information
- Cybersécurité

Qualités personnelles

- Capacité d'analyse de niveau système
- Capacité de synthèse et de présentation de résultats d'études

Qualités personnelles :

- Autonomie
- Créativité
- Curiosité
- Innovation
- Pédagogie

Profil recherché

Les attaques informatiques pouvant concerner tout le domaine du numérique, de très nombreux domaines métier/techniques sont concernés. Aussi, des connaissances métiers pointues sur des domaines précis autres que ceux de la cyber (ex : communications, maritime, aéronautique, véhicules terrestres, automates industriels, IOT, systèmes d'armes) seront également grandement appréciées.



2026-CYBER-MI-0005 Expert en Ingénierie des Connaissances Data Sciences Cyber



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

KnowledgeGraph Ontology RAG LLM NLP
Développement Python

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des expert(e)s en **Ingénierie des Connaissances - Data Sciences appliquées à la Cyber**.

Mission : Dans un environnement Cyber où les menaces et capacités évoluent rapidement, la capitalisation des connaissances et l'analyse des données sont essentielles pour maintenir une posture proactive et réactive. Le poste implique d'être capable de combiner des technologies de pointe pour imaginer et développer des approches novatrices permettant des avancées significatives dans les domaines de l'ingénierie des connaissances et de la data science servant les intérêts métiers cyber.

Compétences métiers

- Développement : Python (indispensable), Java (fortement souhaitable)
- Modélisations, Ontologies et Graphes de Connaissances : OWL, RDF, SPARQL
- Bases orientées graphes : GraphDB, NebulaGraph, Neo4j
- Systèmes de Gestion de Bases de Données : Elasticsearch, MongoDB
- Traitement du Langage Naturel (NLP) : SpaCy, NLTK, GPT, LLM, RAG

Compétences souhaitées

- Des connaissances sur les technologies du Big Data et/ou des compétences en visualisation des données (outillage ou capacités à développer des IHMs) seront un plus apprécié.
- Qualités personnelles :
- Esprit d'équipe
 - Rigueur
 - Curiosité
 - Autonomie
 - Innovation
 - Créativité

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 êtes intégré dans une équipe dédiée à la recherche et développement de solutions innovantes répondant aux besoins d'extraction, de construction et de gestion de connaissances pour la Cyber. Les activités impliquent développements, modélisations, ontologies, graphes de connaissances, traitement du langage naturel (NLP), déploiement et utilisation de grands modèles de langage (LLM, RAG), etc.



2026-CYBER-MI-0006

Ingénieur Validation, Vérification et Intégration d'outils cyber offensifs



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Test Automatisation Qualification
Validation Vérification Intégration

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des ingénieur(e)s Validation, Vérification et Intégration d'outils cyber offensifs.

Mission : Concevoir et conduire des campagnes de tests des logiciels de lutte informatique offensive pour s'assurer de leur bon fonctionnement et de leur stabilité. Pour chaque projet vous travaillez en équipe pluridisciplinaire en étroite collaboration avec les développeurs du logiciel à qualifier. A ce titre vous êtes amené 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 ;
- Proposer des améliorations des processus métiers.

Vous avez également en charge la qualification de logiciels développés par des industriels, de la préparation du marché jusqu'aux opérations de vérification.

Compétences métiers

- Langage python
- Virtualisation (VMWare, VSphere,...), et conteneurisation (docker, ...)
- Protocoles usuels (IPv4, IPv6, TCP, UDP, HTTP, etc.),
- Linux, Windows

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 lutte informatique offensive. Vous intégrez des équipes projets à échelle humaine (3 à 6 personnes).



2026-CYBER-MI-0007 Ingénieur en investigation numérique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Forensics Investigation numérique DFIR

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des ingénieur(e)s en Investigation Numérique.

Mission : Analyser la furtivité des outils logiciels de lutte informatique offensive 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.

Compétences métiers

- Connaissances DFIR (artefacts forensiques)
- Pratique des outils d'investigation numérique (TSK, Volatility, Sysinternals, Wireshark, Jadx, etc.)
- Développement de preuves de concept
- Matrice ATT&CK et implémentation des techniques associées
- Rétro-ingénierie pour documenter des artefacts forensiques
- Connaissance du comportement des malwares et des techniques d'analyses
- Notions sur les outils de détection d'intrusion (NIDS, EDR, SIEM, ...)

Compétences souhaitées

- Connaissance approfondie du fonctionnement d'un ou plusieurs des OS suivants : Windows, Linux, Android, iOS
 - Sécurité Informatique
 - Fonctionnement des protocoles réseau courants
- Qualités personnelles :
- Curiosité
 - Autonomie, persévérance
 - Force de proposition
 - Très bonne capacité de rédaction et de restitution

Les "+" du poste

En choisissant ce poste vous êtes 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. En outre, vous suivrez une formation métier de 6 semaines la première année.



2026-CYBER-MI-0008 Chef de projet Cyber LIO



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Gestion de projet Agilité Développement
logiciel Intégration continue

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des chefs de projet.

Mission : Le chef de projet Cyber LIO 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. 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 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...).

Compétences métiers

- Gestion de Projet
- Lean
- Méthodes agiles (Scrum, Kanban, XP, SAFe)
- Conception Logiciel
- Intégration continue

Compétences souhaitées

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

Les "+" du poste

Lors de votre arrivée, vous êtes 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.



2026-CYBER-MI-0009 Ingénieur Intégrateur DevOps



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Intégration DevOps Système Docker
Kubernetes Python RedTeam

Description du poste (H/F)

Contexte :

Dans le cadre 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), emploient des **intégrateurs DevOps pour travailler au sein d'un département d'expertise en développement logiciel.**

Missions :

- Participer aux activités d'intégration DevOps des applications métier (Windows, Linux, Mobile, Réseaux, Embarqué)
- Déployer les environnements matériels et virtuels nécessaires au bon déroulement du projet
- Customiser/administrer les plateformes techniques pendant la durée du projet
- Assembler les différentes briques logicielles des équipes de développements afin d'en vérifier la compatibilité et le bon fonctionnement
- Soutenir l'industrialisation des différents processus de l'activité Usine logicielle : production des releases, intégration continue, déploiement continu
- Capitaliser les connaissances liées au métier d'Intégrateur DevOps.

Compétences métiers

- 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

Compétences souhaitées

- Qualités personnelles :
- Esprit d'équipe
 - Communication
 - Capacité à résoudre des problèmes.

Les "+" du poste

En choisissant ce poste, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Vous intégrerez des équipes projets à échelle humaine (3 à 6 personnes) et travaillerez en méthodes Agiles (sprints de 2 à 4 semaines).



2026-CYBER-MI-0010 Ingénieur Cyberoffensif Reverse engineering



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse Exploit Windows Linux Android
iOS IDA Ghidra Fuzzing

Description du poste (H/F)

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), emploient des Ingénieur(e)s Cyberoffensif Reverse engineering.

Mission : Au sein de la sous-direction du domaine Cyberoffensif, dans le cadre du renfort de ses activités de recherche et développement d'outils innovants au profit d'équipes RedTeam, vous analysez des logiciels Windows, Linux, Android, iOS ou des binaires spécifiques aux systèmes embarqués afin d'en comprendre l'architecture et le fonctionnement. Vous recherchez des vulnérabilités dans ces logiciels et menez le développement d'outils cyberoffensifs et de preuves de concept pour en démontrer leur exploitabilité.

Compétences métiers

- Langages C, C++, Rust, Python, JavaScript
- Assembleur ARM, x86/x64
- Rétro-conception de logiciel
- Recherche de vulnérabilités

Compétences souhaitées

- Utilisation avancée d'un de ces OS : Windows, Linux, iOS, Android
 - Développement logiciel
- Qualités personnelles :
- Curieux, innovant, à la recherche de nouveaux défis, autonome
 - Persévérant

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique de très haut niveau technique et profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant et stimulant du cyberoffensif. Vous suivez une formation initiale de 6 mois spécifique aux métiers du reverse-engineering dispensée par les experts de DGA-MI, puis intégrez des équipes projets à échelle humaine (3 à 6 personnes).



2026-CYBER-MI-0011 Ingénieur développeur iOS ou Android cyber offensif



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

iOS Android ObjectiveC Swift Java Kotlin
Rust Développement RedTeam

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des ingénieur(e)s en développement iOS ou Android cyberoffensif.

Mission : La mission consiste à concevoir et implémenter des logiciels à vocation offensive. Pour cela vous étudiez le fonctionnement interne des systèmes Android, iOS ou MacOS, vous suivez toutes leurs évolutions et maîtrisez ainsi les subtilités du développement cyber mobile.

Compétences métiers

- Maîtriser un langage parmi le C, Java ou Kotlin,
- Connaître le langage Python
- La connaissance des Langages ObjectiveC, Swift ou Rust serait un plus

Compétences souhaitées

- Intérêt pour écosystèmes Android ou iOS
 - Familier des outils de développement mobiles (debugger, chaîne de compilation, IDE)
 - Familier des 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

Vous avez l'occasion de travailler sur des projets innovants et variés tant en termes de difficulté que de durée, ou de technologies mises en œuvre. Vous adoptez des pratiques de développement rigoureuses (revues de code, intégration continue, pair programming...) au sein d'un environnement agile, dans un esprit collaboratif.

Accompagnés de nombreux experts cyber aux compétences reconnues, vous pouvez compter sur des moyens techniques conséquents et une large offre de formations pour que chaque mission soit un succès.



2026-CYBER-MI-0012 Développeur fullstack offensif



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Datas Fullstack Angular Python Offensif

Description du poste (H/F)

Contexte : Dans le cadre du renfort de ses activités de recherche et développement d'outils innovants au profit d'équipes RedTeam, la division Cyberoffensive de la Direction Générale de l'Armement, site de Bruz (près de Rennes), emploie **des ingénieur(e)s dans le domaine du développement d'applications web** au profit de la cyber sécurité offensive.

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

- Intervenir sur différentes phases du projet : analyse, modélisation, démonstrateurs, spécifications, développement, tests, mise en production.
- Travailler au quotidien dans un contexte agile avec nos architectes et nos développeurs seniors, afin de réaliser des projets dans le respect de nos normes de développement et de qualité associées.
- Maintenir et être force de proposition sur l'amélioration continue des plateformes et des chaînes CI/CD des différents projets.

Compétences métiers

- Maîtrise d'un framework JS, une connaissance d'Angular est un plus
- Maîtrise d'un langage de programmation backend, une connaissance de Python est un plus
- Expérience et bonne connaissance des API REST, une sensibilisation à GraphQL est un plus

Compétences générales

- Pratique confirmée des outils GIT/GITLAB, JIRA
- Maîtrise des technologies de containerisation
- Familier avec les principes d'intégration continue CI/CD
- Méthodologies Agile
- Maîtrise de l'environnement Linux
- Connaissances en modélisation et base de données

Profil recherché

Vous êtes autonome et disposez d'une première expérience significative de quelques années en développement web. Vous êtes curieux et avez un réel intérêt pour le challenge technique et l'innovation dans un contexte opérationnel fort.



2026-CYBER-MI-0013 Techlead FullStack offensive



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Datas Fullstack Angular Python Techlead
Offensif

Description du poste (H/F)

Contexte : Dans le cadre du renfort de ses activités de recherche et développement d'outils innovants au profit d'équipes RedTeam, la division Cyberoffensive de la Direction Générale de l'Armement, site de Bruz (près de Rennes), emploie **des ingénieur(e)s dans le domaine du développement d'applications web** au profit de la cyber sécurité offensive.

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

- Intervenir sur différentes phases du projet : analyse, modélisation, démonstrateurs, spécifications, développement, tests, mise en production.
- Travailler au quotidien dans un contexte agile avec nos architectes et nos développeurs, afin de réaliser des projets dans le respect de nos normes de développement et de qualité associées.
- Concevoir, développer et déployer des solutions robustes tant côté front-end que back-end tout en veillant à la qualité du code
- Apporter votre expertise technique pour orienter le développement de nos produits
- Maintenir et être force de proposition sur l'amélioration continue des plateformes et des chaînes CI/CD des différents projets.
- Rester à l'affût des avancées technologies pour garantir que notre solution reste cohérente et actuelle.
- Faire progresser l'équipe

Compétences métiers

- Maîtrise d'Angular
- Maîtrise fine d'un langage de programmation backend, une connaissance de Python est un plus
- Maîtrise en modélisation et base de données
- Maîtrise des API REST, une sensibilisation à GraphQL est un plus

Compétences générales

- Pratique confirmée des outils GIT/GITLAB, JIRA
- Maîtrise des technologies de containerisation
- Familier avec les principes d'intégration continue CI/CD
- Méthodologies Agile
- Maîtrise de l'environnement Linux



2026-CYBER-MI-0014 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
IDA Ghidra Fuzzing

Description du poste (H/F)

Contexte : Au sein de la sous-direction du domaine Cyberoffensif, dans le cadre du renfort de ses activités de recherche et développement d'outils innovants au profit d'équipes RedTeam, vous analysez des logiciels fonctionnant sous Windows afin d'en comprendre l'architecture et le fonctionnement. Vous recherchez des vulnérabilités dans ces logiciels et menez le développement d'outils cyberoffensifs et de preuves de concept pour en démontrer leur exploitabilité.

Mission : Rechercher des vulnérabilités sur des logiciels fonctionnant sous Windows. Comprendre et documenter le système, analyser sa surface d'attaque, développer des preuves de concept. Au-delà, inventer des scénarios d'attaque, automatiser, s'outiller, prévoir l'avenir.

Compétences métiers

- Processeurs Intel x86/x64 (assembleur)
- Rétro-conception de logiciel
- Méthodes et outils de rétro-conception de binaires
- Langages C/C++, C#, Python, Rust, Dotnet, ...
- Recherche de vulnérabilités

Compétences souhaitées

- Bonne connaissance du système Windows
 - Développement système bas-niveau
- Qualités personnelles :
- Ténacité, persévérance, curiosité, esprit d'équipe, rigueur

Profil recherché

En choisissant ce poste, vous intégrez une équipe dynamique de très haut niveau technique et profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant et stimulant du cyberoffensif. Vous suivez une formation initiale de 6 mois spécifique aux métiers du reverse-engineering dispensée par les experts de DGA-MI, puis intégrez des équipes projets à échelle humaine (3 à 6 personnes).



2026-CYBER-MI-0015 Ingénieur Retro-conception en système Linux



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse Vulnérabilité IDA Ghidra Exploit
Fuzzing Linux

Description du poste (H/F)

Contexte : Au sein de la sous-direction du domaine Cyberoffensif et dans le cadre du renfort de ses activités de recherche et développement d'outils innovants au profit d'équipes RedTeam, la Direction Générale de l'Armement, site de Bruz (près de Rennes), emploie **des ingénieur(e)s en reverse engineering Linux.**

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.

Compétences métiers

- Processeurs Intel x86/x64 (assembleur)
- Rétro-conception de logiciel
- Méthodes et outils de rétro-conception de binaires
- Langages C/C++, Python, Rust, ...
- Recherche de vulnérabilités

Compétences souhaitées

- Bonne connaissance du système Windows
 - Développement système bas-niveau
- Qualités personnelles :
- Ténacité, persévérance, curiosité, esprit d'équipe, rigueur

Profil recherché

Vous êtes rétro-concepteur, ou pas, développeur, ou pas. Vous avez une formation d'informatique fondamentale, ou d'informatique industrielle, ou pas. Vous n'avez pas nécessairement une formation en cybersécurité. Vous êtes curieux, vous aimez les énigmes et les puzzles. Vous souhaitez rejoindre une équipe dynamique et relevez les défis avec nous, venez ! Lors de votre arrivée vous êtes formé à la rétro-conception et à la recherche de vulnérabilités. Ivraf ba irhg gr ibve.



2026-CYBER-MI-0016 Ingénieur 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)

Contexte : Au sein de la sous-direction du domaine Cyberoffensif et dans le cadre du renfort de ses activités de recherche et développement d'outils innovants au profit d'équipes RedTeam, la Direction Générale de l'Armement, site de Bruz (près de Rennes), emploie **des ingénieur(e)s en recherche de vulnérabilités Web.**

Mission : Vous recherchez les vulnérabilités sur des applications Web, analysez la surface d'attaque, concevez des scénarios, développez des POC et mettez-en œuvre des process d'automatisation.

Compétences métiers

- 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

Vous rejoignez une équipe soudée, heureuse de transmettre et avide d'apprendre. Vous bénéficiez également d'une formation interne spécifique ainsi que des formations privées très spécialisées. Du temps de veille est aussi disponible afin de favoriser les démarches autodidactes.

Vous profitez du savoir-faire et des moyens exceptionnels de DGA MI dans un cadre de travail unique.



2026-CYBER-MI-0017 Ingénieur Développement d'outils cyber offensifs



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Windows Linux Kernel
Réseau Containerisation Cloud
RedTeam IA

Description du poste (H/F)

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), **emploient des ingénieur(e)s de développement d'outils cyber offensifs.**

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.

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 (C, C++, python, Rust, Go...)
- Maîtrise du développement de programmes userland et/ou kernel sous Windows / Linux
- 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

Profil recherché

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 intégrez des équipes projets à échelle humaine (3 à 6 personnes), travaillez en méthodes Agiles (sprints de 2 à 4 semaines) et suivez une formation initiale de 3 mois sur nos métiers de la cyberdéfense. Vous êtes curieux et avez un réel intérêt pour le challenge technique et l'innovation dans un contexte opérationnel fort.



2026-CYBER-MI-0018

Ingénieur électronique, radio logicielle et traitement du signal radio



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Offensif Embarqué IoT

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s électronique, radio logicielle et traitement du signal radio.**

Mission : Intégré dans une équipe dynamique dont la principale mission est d'analyser les phénomènes radiofréquences (TEMPEST) ou/et la sécurité des interfaces radiofréquence, vous serez amené à étudier et à développer des outils et des protocoles d'échange de données. Vous les mettrez en œuvre sur des plateformes radio-logicielles lors d'expérimentations et participerez à des projets de recherche et d'ingénierie visant à identifier les nouvelles menaces basées sur les signaux électromagnétiques.

Compétences souhaitées

- C, C++, Matlab, Python, VHDL
- Traitement du signal, du développement sur radio-logicielle, des systèmes de communication radio
- TEMPEST
- Utilisation d'outils de mesures comme les analyseurs de spectre ou les oscilloscopes

Les "+" du poste

Au sein du principal centre d'expertise de la direction technique de la DGA, vous contribuez à la réalisation de l'outil de défense et à la préparation des programmes futurs. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine de la cybersécurité. Vous intégrez des équipes projets dynamiques à échelle humaine (3 à 6 personnes), travaillez en méthodes Agiles et suivez une formation initiale de 3 mois sur nos métiers de la cyberdéfense.



2026-CYBER-MI-0019 Développeur systèmes embarqués



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Offensif Embarqué IoT

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s en développement de logiciels cyber offensifs dans des environnements embarqués.**

Mission : Intégré(e) à une équipe projet dont l'objectif est de réaliser des logiciels offensifs 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 offensive.

Compétences métiers

- Maîtriser le langage C
- Connaître les langages C++, Python, script shell
- Avoir des connaissances sur les systèmes IoT et les plateformes Raspberry Pi, microcontrôleurs, chips ESP32, PyCom, OS temps réel, etc.
- Une connaissance des systèmes de communication 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

Au sein du principal centre d'expertise de la direction technique de la DGA, vous contribuez à la réalisation de l'outil de défense et à la préparation des programmes futurs. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine de la cybersécurité. Vous intégrez des équipes projets dynamiques à échelle humaine (3 à 6 personnes), travaillez en méthodes Agiles et suivez une formation initiale de 3 mois sur nos métiers de la cyberdéfense.



2026-CYBER-MI-0020

Ingénieur électronique, radio logicielle et traitement du signal radio



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

SDR Radiofréquence Traitement du
signal Vulnérabilités Sécurité
Radiologicielle Softwareradio TEMPEST

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des ingénieur(e)s électronique, radio logicielle et traitement du signal radio.

Mission : Intégré dans une équipe dynamique dont la principale mission est d'analyser les phénomènes radiofréquences (TEMPEST) ou/et la sécurité des interfaces radiofréquence, notamment sur les couches basses protocolaires des systèmes de communication, vous êtes amené à étudier et à développer des outils et des protocoles d'échange de données et à les mettre en oeuvre sur des plateformes radio-logicielles lors d'expérimentations. Vous participez également à des projets de recherche et d'ingénierie visant à identifier les nouvelles menaces basées sur les signaux électromagnétiques.

Compétences métiers

- Electronique analogique et numérique
- Systèmes de communication radio
- Développements radio-logicielle
- Connaissance de l'électromagnétisme
- Equipements de mesure (antennes, analyseur de spectre, oscilloscope)
- Analyse de protocoles
- Développement embarqué
- Rétro-ingénierie de firmware

Compétences souhaitées

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

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 intégrez des équipes projets à échelle humaine (3 à 10 personnes), êtes amenés à intervenir sur des systèmes et des plateformes complexes.



2026-CYBER-MI-0021

Développeur expérimenté Réseau et Système embarqué



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeurs Protocoles réseaux
Télécommunication Rust C/C++ Python
Go

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des **ingénieur(e)s expérimentés dans le domaine du développement de logiciels pour les Télécommunications et les systèmes embarqués**. Les projets se déroulent dans un environnement technologique riche et diversifié. La veille et la formation sont des socles importants dans la réussite de nos projets.

Mission : L'expert est intégré à une équipe experte dans la réalisation de logiciels Cyber Offensifs dédiés aux systèmes d'information et de communications numériques au profit des opérations du Ministère des Armées. La mission consiste à :

- Participer à la définition et au développement des systèmes et outils métiers ;
- Concevoir et développer des produits et/ou composants logiciels cyber offensifs.

Compétences souhaitées

Titulaire d'un diplôme de niveau BAC+5 (ingénieur, master 2, etc.), avec une expérience minimale de 5 ans dans le développement de solutions de Télécommunications, l'expert technique intervient dans le développement de produits logiciels cyber sur des thématiques Réseaux répondant à de forts enjeux opérationnels.

Une expérience dans le domaine de la sécurité informatique est un plus indéniable. Il faut être curieux, motivé par le développement et l'expertise réseau et avoir un réel intérêt pour l'innovation. L'expert technique dispose de compétences sur l'un ou plusieurs des sujets suivants :

- Génie Logiciel et architecture, C/C++, Rust, Go ...
- Protocoles réseaux IP, de routage et de sécurité
- Equipements et Architecture de communication
- OS et systèmes embarqués

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique de très haut niveau technique et profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant et stimulant du cyberoffensif.



2026-CYBER-MI-0022

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)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s Télécommunications & Systèmes Industriels**.

Mission : Vous contribuez 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 devez synthétiser et exposer les résultats obtenus aussi bien à l'oral qu'à l'écrit.

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

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

En choisissant ce poste, vous intégrez une équipe dynamique de très haut niveau technique et profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant et stimulant du cyberoffensif.



2026-CYBER-MI-0023

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 laC
HPC SDN VDI

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s Administration Systèmes et Réseaux**.

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.

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.



2026-CYBER-MI-0024 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)

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), emploie **des ingénieur(e)s Administrateur et Analyste sécurité Cyberdéfense**.

Mission : La personne titulaire du poste est 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 doit 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.

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

En choisissant ce poste, vous intégrez une équipe dynamique et à taille humaine, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité au profit d'activités stratégiques. Lors de votre arrivée vous êtes accompagné par un collaborateur afin d'appréhender en toute sérénité votre nouveau poste dans un contexte multi-projets.



2026-CYBER-MI-0025 ASSI Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Droits d'accès Sensibilisation sécurité
Protection du secret Outils de sécurité

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ASSI Cyberdéfense**.

Mission : Contribuer à la maîtrise de la sécurité des moyens opérationnels de Cyberdéfense de DGA MI dans un environnement de management des risques. Participer à la mise en œuvre de la politique de sécurité cyberdéfense aussi bien d'un point de vue gestion des informations et supports classifiés, protection physique et droits d'accès, sensibilisation des utilisateurs aux bonnes pratiques de sécurité.

Compétences métiers

- Réglementation sécurité : Protection du secret, du patrimoine scientifique et technique, homologation des SI
- Organisation SSI et normes associées
- Outils de sécurité, MCS
- Gestion de droits d'accès

Compétences souhaitées

- Gestion de moyens informatiques
 - Environnement des systèmes d'information
 - Gestion de ticketing
- Qualités personnelles :
- Organisation et méthode
 - Autonome tout en sachant travailler en équipe
 - Réactif
 - Très bon relationnel

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et à taille humaine, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité au profit d'activités stratégiques. Lors de votre arrivée vous êtes accompagné par un collaborateur afin d'appréhender en toute sérénité votre nouveau poste dans un contexte multi-projets.



2026-CYBER-MI-0026 RSSI Technique Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Analyse de risques Architecture système et réseau
Virtualisation Synthèse RSSI Audit technique Supervision

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des RSSI Technique Cyberdéfense**.

Mission : Assurer la maîtrise technique de la sécurité des moyens opérationnels de Cyberdéfense de DGA MI dans un environnement de management des risques. Piloter la sécurité technique des moyens Cyberdéfense en lien avec les équipes en charge de l'évolution et du maintien en condition des moyens de production (urbaniste, administration, supervision de sécurité). Assurer le rôle de RSSI de système et participer à l'homologation des SI en instruisant la partie technique des dossiers.

Compétences métiers

- Conception d'architectures complexes et hétérogènes
- Technologie de supervision système et réseaux
- Ingénierie de la sécurité des systèmes d'information
- Processus d'homologation et normes associées

Compétences souhaitées

- Analyse documentaire, synthèse et présentation de résultat
 - Gestion de projet technique
 - Connaissance de la méthode agile
- Qualités personnelles :
- Organisation et méthode
 - Autonome tout en sachant travailler en équipe
 - Rigoureux
 - Très bon relationnel

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et à taille humaine, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité au profit d'activités stratégiques. Lors de votre arrivée vous êtes accompagné par un collaborateur afin d'appréhender en toute sérénité votre nouveau poste dans un contexte multi-projets.



2026-CYBER-MI-0027 Technicien Soutien systèmes d'information



Niveau requis

BTS IUT

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

GLPI Ticketing MCO Matériel Réseaux
Windows Linux

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des techniciens pour maintien en condition opérationnel**.

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 la réception, la priorisation et l'orientation des tickets utilisateurs. Vous apportez un soutien de premier niveau aux utilisateurs, autant sur du matériel, du réseau, du système ou de l'applicatif, et relayez les demandes vers les experts. Vous participez également à la gestion d'un important parc matériel hétérogène.

Compétences métiers

- Support aux utilisateurs et hot-line (population d'informaticiens)
- Utilisation et paramétrage d'outil de ticketing (ex : GLPI, MANTIS, Jira, ...)
(La maîtrise de Jira Management est un plus)
- Administration systèmes informatiques et réseaux
- Brassage d'équipements réseaux et informatiques
- Masterisation de postes informatiques
- Configuration de matériels Android ou IOS

Compétences souhaitées

- Utilisation des environnements Linux (Debian/Ubuntu) et Windows (Active Directory)
- Utilisation des équipements IP, switches (HP, Cisco), pare-feux (Stormshield, pfSense)
- Gestion d'un parc informatique et périphériques divers
- Réponse utilisateurs

Qualités personnelles :

- Rigueur, résistance au stress et organisation
- Soucis du client et bon relationnel
- 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.



2026-CYBER-MI-0028 Ingénieur DevOps



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

DevOps CI/CD Ansible Docker k8s
Kubernetes Administration système
Support

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s DevOps**.

L'expert technique est en charge de de la conception, de la réalisation et du maintien en conditions opérationnelles et de sécurité du cloud privé pour l'hébergement des projets de Lutte Informatique Offensive. Vous êtes en interaction avec d'autres services de la Division des Systèmes d'Informations Cyber, notamment pour le support utilisateurs de 2e niveau, les infrastructures physiques et les administrateurs de sécurité.

Mission : Imaginer et concevoir des solutions techniques répondant aux besoins des experts en Lutte Informatique Offensive. Réaliser et déployer des socles et des outils métier sur des environnements sécurisés.

Assurer la supervision, l'évolution et le maintien en condition opérationnelle des systèmes d'information récents et innovants dans un environnement mixte Windows et Linux.

Compétences techniques

- | | |
|---|---|
| <ul style="list-style-type: none"> Orchestration (Ansible) Utilisation des techniques de virtualisation (VMware vSphere) Utilisation des techniques de conteneurisation (Docker, K8S) Maîtrise d'un langage de scripting (Bash, Python, Powershell, ...) Connaissance des cycles de développement et d'intégration continue, CI/CD | <ul style="list-style-type: none"> Connaissance en supervision système et de sécurité Connaissance en architecture et conception des systèmes d'information Support aux projets et utilisateurs (population d'informaticiens) (GLPI, JSM ...) Connaissance de développement d'applications au profit des utilisateurs finaux (Angular, Node, Go, ...) |
|---|---|

Les "+" du poste

Vous êtes force de proposition et contribuez à l'amélioration continue du laboratoire ou des outils internes. Vous intervenez au développement et au déploiement de solutions métier, en se basant sur un socle technique polyvalent à base de virtualisation VMware, conteneurisation Docker et K8S et d'orchestration Ansible.



2026-CYBER-MI-0029 Ingénieur DevOps Services Cyber



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

DevSecOps Build CI/CD Automatisation
InfraAsCode

Description du poste (H/F)

Contexte : Dans le cadre 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), emploie **des Ingénieur(e)s DevOps Services Cyber**.

Mission : Intégrée à une équipe dont l'objectif est d'assurer la compilation, le test et le déploiement sécurisé de logiciels du Ministère des Armées, les missions consistent à :

- Développer, maintenir une chaîne de compilation, de test et de déploiement ;
- Assurer la sécurité de la chaîne de compilation ;
- Automatiser le déploiement du cyber range et assurer son bon fonctionnement ;
- Participer à l'évolution et à l'intégration de nouveaux services au sein du cyber range ;
- Développer des outils transverses ;
- Être force de proposition pour faire évoluer les technologies mises en oeuvre (automatisation, virtualisation, conteneurisation, ...)

Compétences métiers

- Administration systèmes (Linux et Windows)
- Administration réseaux
- Automatisation de déploiement (ansible)
- Infrastructure as Code (terraform, packer)
- Connaissances en développement (Bash, Powershell, Python)

Compétences souhaitées

- Maîtrise des environnements Linux (Debian/Ubuntu)
- Utilisation d'outils de gestion de version (git)
- Utilisation des techniques de conteneurisation

Qualités personnelles :

- Curiosité
- Autonomie
- Capacité à s'intégrer dans une équipe
- Facilité d'adaptation à de nouveaux contextes techniques et humains

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.



2026-CYBER-MI-0030 Ingénieur Cyberdéfense pour les plateformes cyber



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Plateformes Conception Réseaux Radio
Mobile Satellite Systèmes GTB IOT

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des Ingénieur(e)s Cyberdéfense pour les plateformes cyber.**

Mission : L'expert technique est en charge de concevoir, réaliser/faire réaliser et assurer le maintien en conditions opérationnelles de plateformes dont l'objectif est en amont de supporter le développement de capacités cyber offensives puis de démontrer aux opérationnels du domaine l'efficacité de ces dernières et en aval de soutenir ces mêmes opérationnels dans la réalisation de leurs missions.

Compétences métiers

- Réseaux et télécommunications (fixe, mobile, radio, satellite)
- Navires, Drones, Satellites
- Systèmes d'armes
- Systèmes industriels
- GTB, domotique, IOT, vidéosurveillance

Compétences souhaitées

- Systèmes d'exploitation (Windows, Linux) et Virtualisation (VMWare, Openstack, etc.)
- Réseaux de communication (Routage IP, Ethernet, Wifi, Bluetooth)
- Compétences générales en sécurité informatique
- Sauvegardes (NAS, SAN, etc)
- Câblage électrique BT, électrotechnique, mécanique

Qualités personnelles :

- Autonomie
- Organisation
- Créativité

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique d'ingénieurs spécialistes dans différents domaines et métiers. Tout en vous acculturant à la cyber-sécurité offensive, vous apprenez, appliquez et optimisez les méthodes et processus de DGA MI pour la conception et la gestion de plateformes techniques cyber.

Parallèlement, vous faites partie d'une ou plusieurs équipes projets à échelle humaine (5 à 10 personnes), dans lesquelles vous intervenez en tant que référent plateforme métier, partagez vos connaissances et êtes force de proposition.



2026-CYBER-MI-1001

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
Conception

Description du poste (H/F)

Contexte :

Dans le cadre 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), emploient des **ingénieur(e)s en conception d'architecture logicielle de produit de sécurité**.

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 maquettages de solutions et avoir la possibilité d'intégrer une équipe de développement sur une période déterminée.

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

- Vulnérabilités des logiciels
 - Développement logiciel embarqué ou sur poste de travail
 - Mécanismes de sécurité implémentés dans les systèmes d'exploitation et dans les processeurs
- 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 êtes accompagné lors de votre montée en compétences suite à votre prise de poste.



2026-CYBER-MI-1002 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)

Contexte :

Dans le cadre 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), emploient des **ingénieur(e)s en conception de produit de sécurité embarqués**.

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 maquettings de solutions et avoir la possibilité d'intégrer une équipe de développement sur une période déterminée.

Compétences métiers

- 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 boot sécurisés offerts par des plateformes matérielles (intrinsèque aux composants ou TPM)
 - Connaissance de base des protocoles cryptographiques
- 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 êtes accompagné lors de votre montée en compétences suite à votre prise de poste.



2026-CYBER-MI-1003 Ingénieur Architecte produits de sécurité



Niveau requis	Contrat	Mots-clés
Ingénieur CTI Master 2	Contractuel civil CDI à Bruz (35)	Architecte Cyberprotection Embarqué Cryptographie Ingénierie Conduite de projet

Description du poste (H/F)

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), emploient des **Architectes Produits de Sécurité**.

Mission : Dans le cadre du développement des équipements de sécurité qui assurent la protection des systèmes du ministère des Armées, les experts techniques coordonnent les travaux des experts. Ils interviennent dans les phases amont de collecte du besoin opérationnel, d'analyse de sécurité et de spécifications techniques, puis dans le suivi des réalisations industrielles et enfin ils pilotent les évaluations de sécurité et la qualification des équipements. La phase de qualification peut être précédée d'un process, dont ils assurent le pilotage, conduisant à présenter à l'ANSSI les éléments permettant d'instruire l'obtention d'un agrément.

Compétences métiers	Compétences souhaitées
<ul style="list-style-type: none"> Développement d'équipements et/ou de logiciels pour systèmes embarqués Protocoles de communications et télécom, réseau Notions de Cryptographie Sécurité des systèmes d'Information Méthodes d'analyse de risque 	<ul style="list-style-type: none"> Informatique et/ou électronique Conduite de projet Qualités personnelles : <ul style="list-style-type: none"> Esprit de synthèse Travail en équipe Autonomie Aptitudes pour la négociation

Les "+" du poste

En tant qu'architecte (eq. Chef de projet) vous êtes au cœur des programmes d'armement pour assurer leur protection contre les menaces cyber. A l'arrivée en poste, vous êtes 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..



2026-CYBER-MI-1004 Ingénieur Conception de logiciel embarqué et sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cryptographie C Développement
Systèmes embarqués Sécurité logiciel

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des experts en développement de logiciels de sécurité et cryptographie.**

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

Les missions consistent à :

- 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

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 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.



2026-CYBER-MI-1005 Ingénieur en cryptographie algorithmique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cryptographie Mathématiques
Conception

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des Ingénieur(e)s en cryptographie algorithmique**.

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

Compétences souhaitées

L'expert technique a des compétences sur l'un ou plusieurs des sujets suivants : domaines de la cryptographie, des mathématiques, des statistiques et/ou de la logique.

Il a une expérience professionnelle préalable, éventuellement en dehors du domaine de la cryptographie.

Par ailleurs, il bénéficie d'une expérience minimale en programmation et maîtrise l'anglais technique (littérature scientifique). Il fait également preuve d'autonomie, de curiosité, d'adaptation et de rigueur.

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe dynamique et forte d'une expérience unique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Vous intégrez des équipes projets à échelle humaine (2 à 3 personnes), et fournissez une expertise sur des programmes d'armements de plus grande ampleur, impliquant des acteurs étatiques et industriels.



2026-CYBER-MI-1006 Ingénieur en développement et analyse de logiciels cryptographiques



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

C Cryptographie Analyse de code
Développement Debugger IDA Ghidra
Reverse Exploit

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s en développement et analyse de logiciels cryptographiques.**

Mission : Analyse et Implémentation d'algorithmes cryptographiques. Recherche et exploitation de vulnérabilités cryptographiques.

Les missions consistent à :

- Développer des algorithmes et protocoles cryptographiques de façon sûre et optimisée.
- Analyser des algorithmes développés par des tiers.
- Rechercher et analyser à partir d'un code source ou d'un binaire les failles cryptographiques dans les implémentations d'algorithmes ou protocoles cryptographiques.
- Développer des preuves de concept pour l'exploitation des vulnérabilités.
- Avoir une activité de veille technologique dans le domaine de la recherche et exploitation de failles cryptographiques dans les produits logiciels..

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



2026-CYBER-MI-1007 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)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s Conception matérielle Cryptographie et Sécurité.**

Mission : l'expert technique participe au suivi de la conception matérielle des composants de sécurité de défense et entretient un état de l'art et une expertise sur le domaine des composants, des fonctions de sécurité et de l'implémentation de la cryptographie.

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.



2026-CYBER-MI-1008 Architecte cybersécurité systèmes d'armes



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Architecte EBIOS ISO27001

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des **Architectes cybersécurité systèmes d'armes**.

Mission : Ils assurent, en toute autonomie, le pilotage de la démarche de sécurisation des systèmes d'armes tout au long de son développement (de la spécification à l'audit final) vis à vis de la menace cyber. Ils interviennent sur différents projets, à différents stades, chez des industriels de la Défense et/ou PME, des laboratoires académiques ou non au profit d'Etudes Amont ou de grands programmes d'armement (satellites, avions de combats, hélicoptères, missiles...) afin de préparer l'avenir et délivrer des systèmes cyber sécurisés à nos forces militaires.

Compétences métiers

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

Qualités personnelles

- Esprit de synthèse
- Autonomie
- Proactivité
- Travail en équipe
- Aptitudes pour la négociation

Les "+" du poste

En tant qu'architecte, vous êtes au cœur des programmes d'armement pour assurer la protection des systèmes d'armes contre les menaces cyber. A votre arrivée en poste, vous êtes 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.

Intégrer la DGA, c'est aussi la possibilité d'évoluer, de changer de fonction ou d'activité, sur différents sites, et de bénéficier d'une qualité et d'un équilibre de vie personnelle-vie professionnelle.



2026-CYBER-MI-1009 Ingénieur en architecture de sécurité pour les systèmes d'armes



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Architecte Electronique Informatique
embarquée

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des Ingénieur(e)s en architecture de sécurité pour les systèmes d'armes**.

Mission : En s'appuyant sur leur expertise et celles des experts du centre, ils pilotent la conception électronique, informatique et cryptographique de la solution de sécurité des systèmes d'armes.

Ils participent, en coopération avec des architectes, à la démarche de sécurisation des systèmes d'armes tout au long de son développement (de la spécification à l'audit final) vis à vis de la menace cyber. Ils orientent la spécification et la conception technique cyber de systèmes d'armes.

Ils interviennent sur différents projets à différents stades chez des industriels de la Défense et/ou PME, des laboratoires académiques ou non au profit d'Etudes Amont ou de programmes tels que des grands programmes d'armement (satellites, avions de combats, sous-marins, missiles...) afin de préparer l'avenir et de livrer des systèmes cyber sécurisés à nos forces militaires.

Ils effectuent une veille technologique sur l'état actuel de la menace technique et sur l'efficacité des mécanismes de sécurité existants

Compétences métiers

- Electronique embarquée
- Informatique embarquée
- Cryptographie
- Réglementation liée à la sécurité
- Méthodologie liée à la sécurité
- Lutte Informatique Défensive
- Architecture réseau
- Ingénierie système

Compétences nécessaires

Qualités personnelles :

- Esprit de synthèse
- Autonomie
- Proactivité
- Travail en équipe
- Aptitudes pour la négociation

Les "+" du poste

En tant qu'architecte vous êtes au cœur des programmes d'armement pour assurer la protection des systèmes d'armes contre les menaces cyber. A votre arrivée en poste, vous êtes accompagné(e) pour monter en compétence en toute sérénité.



2026-CYBER-MI-1010

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 EBIOS Sécurité Cyberdéfense SSI
SMSI ISO27K

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des auditeurs (auditrices) organisationnel(le)s de la sécurité des systèmes d'information et des systèmes d'armes.**

Mission : 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), ils réalisent des audits organisationnels de sécurité sur des systèmes d'information et des systèmes d'armes du ministère des Armées.

Ils contribuent également au développement de méthodes d'audit de sécurité.

Compétences métiers

- Ingénierie de la SSI
- Techniques d'entretien
- Normes ISO 2700x
- SMSI
- EBIOS

Compétences souhaitées

- Principales technologies des systèmes d'information et de la SSI
 - Culture cyber (menaces, vulnérabilités, risques, ...)
- Qualités personnelles :
- Autonome sachant travailler en équipe
 - Rigoureux, Organisé, Curieux

Profil recherché

La connaissance d'un des domaines suivant est appréciée : réglementation autour de la sécurité des systèmes d'information (SSI), SMSI, méthodes d'analyse de risque (EBIOS, ...).

Une expérience en audit de sécurité, la pratique ou la connaissance de la fonction de responsable de sécurité de(s) système(s) d'information (RSSI) sont également un plus, autant que la connaissance de la démarche qualité, ou de méthodes d'organisation du travail.

D'un naturel curieux, les auditeurs ont de bonnes facultés d'adaptation, un très bon relationnel et le goût du travail en équipe.

Ils sont aptes à se déplacer, environ cinq (5) fois une semaine par an, sur divers sites du ministère des Armées, ainsi que pour quelques déplacements ponctuels sur une (1) journée.



2026-CYBER-MI-1011

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)

Contexte : Dans le cadre 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), emploient **des auditeurs (auditrices) techniques en sécurité des systèmes industriels et des systèmes d'information.**

Mission : Au sein de l'équipe Évaluation de la Sécurité des Systèmes (ESS) de la Direction Générale de l'Armement (DGA), ils réalisent 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.

Ils sont également amenés 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 peut également leur être demandé de sensibiliser/former différents acteurs du ministère des Armées sur la sécurisation des systèmes industriels.

Compétences métiers

- Automatismes et informatique industrielle
- Architecture sécurisée des systèmes d'information et des réseaux
- Méthodes d'investigation technique SCI/SSI

Compétences souhaitées

- Principales technologies des systèmes d'information, des systèmes de contrôle industriels et de la SSI
- Culture cyber (menaces, vulnérabilités, risques, ...)

Qualités personnelles :

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

Profil recherché

Des connaissances dans les domaines suivants sont un plus pour candidater : produits et solutions de sécurité dédiés aux systèmes industriels, systèmes de sondes et systèmes de détection d'intrusion, systèmes de gestion de bases de données, systèmes d'exploitation temps réel, lutte informatique défensive (LID), SOC, gestion technique des bâtiments (GTB), réseaux électriques TBT/BT/HT/THT.

D'un naturel curieux, les auditeurs ont de bonnes facultés d'adaptation, un très bon relationnel et le goût du travail en équipe.

Ils sont aptes à se déplacer environ quatre (4) à six (6) fois une semaine par an sur divers sites du ministère des armées.



2026-CYBER-MI-1012

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)

Contexte : Dans le cadre 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), emploient des auditeurs (auditrices) techniques de la sécurité des systèmes d'information et des systèmes d'armes.

Mission : 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), ils réalisent 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.

Ils contribuent également au développement d'outils d'audit technique de sécurité.

Compétences métiers

- Architecture sécurisée de système d'information et de réseau
- Méthodes d'investigation SSI technique
- Normes ISO 2700x

Compétences souhaitées

- Principales technologies des systèmes d'information et de la SSI
 - Culture cyber (menaces, vulnérabilités, risques, ...)
- Qualités personnelles :
- Autonome sachant travailler en équipe
 - Rigoureux, Organisé, Curieux

Profil recherché

Des connaissances dans les domaines suivants sont un plus pour candidater : sondes et systèmes de détection d'intrusion (IDS/IPS), systèmes de gestion de bases de données, systèmes d'exploitation temps réel, systèmes de contrôle industriels (ICS, SCADA), lutte informatique défensive (SOC).

Les auditeurs possèdent de bonnes connaissances théoriques et pratiques des principales technologies de l'information et ils portent de l'intérêt à la sécurité des systèmes d'information (SSI), la cybersécurité, la cyberdéfense.

D'un naturel curieux, les auditeurs ont de bonnes facultés d'adaptation, un très bon relationnel et le goût du travail en équipe.

Ils sont aptes à se déplacer environ cinq (5) fois une semaine par an, sur divers sites du ministère des Armées, plus quelques déplacements ponctuels sur une (1) journée.



2026-CYBER-MI-1013 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)

Contexte : Dans le cadre 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), emploient **des Architectes cybersécurité systèmes d'information**.

Mission : Ils pilotent la démarche de sécurisation des systèmes d'information vis à vis de la menace cyber. Ils interviennent 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.

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



2026-CYBER-MI-1014 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)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s cybersécurité**.

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.

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.



2026-CYBER-MI-1015 Ingénieur Sécurisation des systèmes d'information



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Architecte Système d'exploitation Système d'information

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s cybersécurité**.

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.

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.



2026-CYBER-MI-1016 Ingénieur en architecture de détection d'intrusion système



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

LID CTI SOC CERT IDS NDR EDR SIEM
Architecte

Description du poste (H/F)

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), emploient **des ingénieur(e)s en architecture de détection d'intrusion système**.

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.

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.



2026-CYBER-MI-1017 Ingénieur en techniques de détection d'intrusion



Niveau requis	Contrat	Mots-clés
Ingénieur CTI Master 2	Contractuel civil CDI à Bruz (35)	Détection intrusion EDR NDR SIEM Python C Linux Sandbox Honeypot Suricata Snort Zeek

Description du poste (H/F)

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), emploient **des ingénieur(e)s en techniques de détection d'intrusion**.

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

Compétences métiers

- Développement pour la réalisation de preuve de concept en environnement Linux
- Connaissance de l'architecture bas niveau et des mécanismes internes de Linux
- Connaissance du comportement des malwares et de techniques d'exploitation
- Mise en oeuvre d'une ou plusieurs solutions de détection d'intrusion et de supervision de la sécurité en environnement Linux (sondes de détection d'intrusion, honeypot, sandbox, collecteurs d'évènements, SIEM)
- 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.



2026-CYBER-MI-1018 Ingénieur Cyberdéfense SOC



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

SOC Détection SIEM IoC Administration
système Splunk Elasticsearch

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des ingénieur(e)s Cyberdéfense SOC.

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.

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.



2026-CYBER-MI-1019 Chef de projet Lutte Informatique Défensive



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

LID CERT SOC Chef de projet

Description du poste (H/F)

Contexte : Dans le cadre de la forte montée en puissance des besoins du ministère en termes de supervision cyber de systèmes complexes, les équipes de Lutte Informatique Défensive (LID) de la Direction Générale de l'Armement, site de Bruz (près de Rennes), emploient **plusieurs ingénieurs(es) Cyberdéfense Chef de projet LID.**

Mission : La mission principale consiste à assurer le pilotage technique de projets d'implémentation de capacités de Lutte Informatique Défensive au profit du CERT et des SOC's du MinArm. Intégré au sein d'une équipe pluridisciplinaire de programme d'armement, le chef de projet est positionné comme architecte référent sur un périmètre fonctionnel et comme point de contact privilégié d'un ou plusieurs organismes opérationnels LID. D'un naturel autonome et pédagogue, il est au contact direct des utilisateurs afin de collecter et comprendre leurs besoins et de les décliner en spécifications techniques en vue de leur réalisation par les industriels du domaine. Garant de la cohérence et de la bonne exécution des travaux demandés, il met à profit sa connaissance des aspects techniques et métier du domaine Cyberdéfense pour comprendre et challenger à la fois le besoin opérationnel et la réponse industrielle, si besoin en s'appuyant et coordonnant les contributions des experts LID DGA sur certaines thématiques pointues. En coordination avec l'industriel en charge, il pilote les actions étatiques durant les travaux de conception, de réalisation et de déploiement des nouvelles capacités, et assure à l'issue les activités de test et validation permettant d'accepter la capacité en service opérationnel.

Compétences métiers

- Architecture d'ensemble des systèmes de Cyberdéfense (PDIS)
- Techniques et stratégies de détection (NIDS, EDR, SIEM)
- Systèmes de gestion d'incidents et de crise (SIRP/SOAR)
- Plateformes de gestion de l'information sur la menace (TIP)
- Fonctions d'investigation numérique (sandbox, FPC)
- Sécurisation des systèmes informatiques
- Connaissances infrastructures et réseaux

Compétences souhaitées

- Chefferie de projet
 - Conduite de réunion
 - Domaine Cyber
- Qualités personnelles :
- Capacité à s'intégrer à une équipe et à y travailler, tout en étant autonome,
 - Curiosité, esprit de synthèse, créativité
 - Capacité à se former en permanence et à s'adapter aux évolutions techniques
 - Pédagogie, persévérance



2026-CYBER-MI-1020 Ingénieur en rétro-analyse de codes malveillants



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Ghidra

Description du poste (H/F)

Contexte :

Dans le cadre 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), emploient des ingénieur(e)s en rétro-analyse de codes malveillants.

Missions :

- Analyse approfondie de binaires malveillants
- Production de signatures de détection
- Développement d'outils d'aide à l'analyse
- Capitalisation, sous forme de rapports techniques

Compétences métiers

- Rétro ingénierie de binaires complexes
 - Maîtrise des outils (IDA/GHIDRA, etc.)
- Connaissances générales :
- Architectures des processeurs
 - Fonctionnement interne des systèmes d'exploitation
 - Langages de programmation courants (C,C++, etc.) et processus de compilation
 - Cryptographie et méthodes d'obfuscation
 - Recherche de vulnérabilités
 - Protocoles réseaux

Compétences souhaitées

Qualités personnelles :

- Capacité à travailler en équipe
- Curiosité scientifique et technique
- Aisance rédactionnelle

Profil recherché

En choisissant ce poste vous intégrez une équipe pluridisciplinaire, dans un contexte interministériel fort. Les travaux s'inscrivent dans un cadre opérationnel concret, que ce soit sur des temps courts ou lors d'analyses plus approfondies. Vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Vous intégrez une équipe à échelle humaine (~8 personnes) et suivez une formation initiale (jusqu'à 6 mois) sur nos métiers de la cyberdéfense.



2026-CYBER-MI-1021 Analyste en menace cyber



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Incidents Menace

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient des analystes en menace cyber.

Missions :

- Collaborer avec des entités ministérielles et interministérielles, aux niveaux technique et stratégique, dans le contexte de la menace cyber visant les intérêts de l'Etat
- Analyser les impacts d'un incident de sécurité. Capitaliser et valoriser les connaissances acquises. Produire des synthèses de niveaux techniques et stratégiques en fonction des interlocuteurs
- Analyser des fuites de données et en évaluer l'impact
- Faire une veille quotidienne dans le domaine de la menace cyber

Compétences métiers

- Compréhension des TTP et MOA
- Rédaction de synthèses stratégiques et techniques
- Manipulation de grands volumes de données à des fins d'analyse
- Identification d'enjeux stratégiques, pour la DGA, dans le contexte des incidents cyber
- Recherches OSINT sur internet et utilisation de bases de connaissance de données techniques publiques

Compétences souhaitées

- Structure des activités cyber de l'Etat
 - Typologie de la menace cyber en France
 - Méthodologies de modélisation de la menace cyber
- Qualités personnelles :
- Capacité à travailler au niveau interministériel
 - Curiosité et rigueur
 - Aisance rédactionnelle et orale
 - Capacité à travailler sur des échéances courtes

Profil recherché

En choisissant ce poste vous intégrez une équipe pluridisciplinaire, dans un contexte interministériel fort. Les travaux s'inscrivent dans un cadre opérationnel concret, que ce soit sur des temps courts ou lors d'analyses plus approfondies. Vous profiterez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Vous intégrerez une équipe à échelle humaine (~8 personnes).



2026-CYBER-MI-1022 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)

Contexte : Dans le cadre 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), emploient **des Data ingénieur(e)s**.

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

Compétences maîtrisées

- Stockage distribué (HDFS, ...)
- Recherche plein texte (Elasticsearch, ...)
- Traitements distribués (Spark, Yarn, ...)
- Gestionnaires de workflows (Cadence ou équivalent)
- Outils d'exploration / visualisation (Kibana, Zeppelin, ...)

Compétences souhaitées

- Une 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.
- De bonnes pratiques de développement logiciel.

Profil recherché

Vous disposez de compétences en Big Data et vous n'en pouvez plus de travailler sur des données marketing ?

Le monde de la Cybersécurité s'ouvre à vous ! Venez mettre à profit votre savoir-faire au sein d'une équipe d'experts du ministère des armées dans un environnement et un cadre de vie privilégiés au cœur de la région Bretagne. Vous intégrerez une équipe dynamique et profiterez du savoir-faire et des moyens de DGA MI sur des projets innovants au croisement de la cybersécurité, du traitement de données massives et de l'intelligence artificielle.



2026-CYBER-MI-1023 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)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s chargé(e)s de l'analyse des données d'intérêt Cyber**.

Mission : La personne titulaire du poste est intégrée dans une équipe dédiée à la conception de plateformes Big Data permettant d'exploiter des données d'intérêt pour la Cyberdéfense, aussi bien au profit de la lutte informatique défensive, offensive, que d'influence.

Le poste consiste à :

- Identifier et analyser les sources de données pertinentes pour la Cyberdéfense.
- Définir les datasets métiers à produire
- En lien avec les ingénieurs data, spécifier les pipelines de données à développer et plus globalement, contribuer au développement d'outils d'analyse et d'étiquetage des données au profit des opérationnels
- Exploiter ces données au sein d'une infrastructure de traitement de données massives.

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

Vous disposez de compétences en analyse de données et vous n'en pouvez plus de travailler sur des données marketing ? Le monde de la Cybersécurité s'ouvre à vous ! Venez mettre à profit votre savoir-faire au sein d'une équipe d'experts du ministère des armées dans un environnement et un cadre de vie privilégiés au cœur de la région Bretagne. Vous intégrerez une équipe dynamique et profiterez du savoir-faire et des moyens de DGA MI sur des projets innovants au croisement de la cybersécurité, du traitement de données massives et de l'intelligence artificielle.



2026-CYBER-MI-1024 Ingénieur DevOps Big Data



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux k8s Ansible Docker BigData
Hadoop Spark Elasticsearch Grafana

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des Ingénieur(e)s DevOps / Big Data**.

Mission : ils participent 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 et au profit des différents domaines de luttes informatiques : défensive, offensive et d'influence. Ils interviennent sur un spectre large, depuis les infrastructures, en passant par les systèmes, jusqu'à la pile logicielle interne, en boucle courte avec les data engineers qui développent et intègrent notre pile applicative, ainsi que les data analysts qui l'exploitent...

Compétences métiers

- L'administration des systèmes Linux (Debian ou dérivés)
- Une chaîne d'automatisation, de gestion de version et de déploiement (Ansible, Gitlab CI/CD)
- Une solution de conteneurisation (Docker swarm ou Kubernetes)
- Le hardware et les infrastructures d'hébergement de serveurs
- Les composants d'infrastructure Big Data (Hadoop, Spark, MinIO, Elasticsearch, ...)
- La sécurisation de systèmes
- La gestion d'un service en production
- Les spécificités du domaine Cyber

Les "+" du poste

Vous êtes curieux et doté d'un bon relationnel, vous appréciez interagir avec les autres métiers du projet. Venez mettre à profit votre savoir-faire au sein d'une équipe d'experts du ministère des armées dans un environnement et un cadre de vie privilégiés au cœur de la région Bretagne. Vous intégrerez une équipe dynamique et profiterez du savoir-faire et des moyens de DGA MI sur des projets innovants au croisement de la cybersécurité, du traitement de données massives et de l'intelligence artificielle.



2026-CYBER-MI-1025 Architecte L2I



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

L2I Architecte Chef de projet

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des architectes spécialisées en lutte informatique d'influence (L2I)**.

Mission : L'architecte L2I assure la spécification et le suivi de développement de produits et de solutions dédiées à la L2I, coordonne techniquement les différents développements du périmètre à sa charge et contribue à la qualification des systèmes de son périmètre.

Il participe aux phases de recueil des besoins exprimés par les entités opérationnelles dans un contexte de schéma directeur ou d'études préalables de projet. Il est le référent sur la partie du périmètre fonctionnel L2I qui lui est confié et assure le développement au juste besoin et au moindre coût des capacités nécessaires

Compétences métier

- Gestion de projet ;
- Méthodes Agiles ;
- La connaissance du secteur public ou du domaine de l'influence informationnelle serait un plus.

Compétences souhaitées

- Architecture des systèmes IT ;
- Ingénierie système ;
- Pilotage de marché de sous-traitance ;
- Spécifications de systèmes IT ;
- Tests/Recette de systèmes IT ;

Qualités personnelles :

- Organisation
- Autonomie/Initiative

Profil recherché

En choisissant ce poste, vous donnez du sens à votre activité professionnelle, vous serez au contact des entités opérationnelles et profiterez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Vous intégrerez une équipe dynamique travaillant sur des projets variés, à échelle humaine (10 personnes) et que vous pourrez suivre dans la durée.



2026-CYBER-MI-1026 Ingénieur Cyberdéfense en tests d'intrusion / TTP



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Tests d'intrusion Pentest RedTeam TTP
C2

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s en tests d'intrusion ou développement offensif**.

Mission : Dans des environnements techniques challengeant, ils allient discrétion, persistance et innovation pour réaliser des tests d'intrusion. Des missions longues durée, depuis nos locaux ou en déplacement, leur permettent de participer à toutes les étapes d'un pentest: phishing, primo-intrusion, contournement de solution de sécurité, EOP, C2.

Compétences métiers

- Bonnes connaissances des techniques et outils de tests d'intrusion (reconnaissance, exploitation, postexploitation, ...)
- Connaissances en techniques et outils de recherche et d'exploitation de vulnérabilités
- Capacité à adapter des codes et des outils d'exploitation
- Connaissance en développement (Python, C#, C, Java)
- Contournement de solutions de sécurité et discrétion opérationnelle

Compétences souhaitées

- Bonnes connaissances en OS et leur administration (Windows, Linux, ...)
- Bonnes connaissances applicatives (Active Directory/LDAP, Serveurs Web, Serveurs de messagerie, DNS, SGBD, EDR, Antivirus, HIDS/NIDS, applications de supervision, ...)
- Bonnes connaissances réseaux et protocoles associés

Qualités personnelles :

- Curieux, Innovant et Persévérant
- Pondéré, Organisé et Conscientieux
- Esprit d'équipe et autonomie

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 au métier et au reverse engineering.

En choisissant ce poste, vous intégrez une équipe établie et dynamique. Vous profitez du savoir-faire et des moyens de DGA MI en cybersécurité.



2026-CYBER-MI-1027 Ingénieur Expert en sécurité logiciel



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Sécurité logiciel Analyse statique Analyse
dynamique C/C++ Python Rust JAVA

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des expert(e)s en sécurité logiciel**.

Mission :

- Garantir l'absence de vulnérabilités dans les logiciels de sécurité du ministère des Armées.
- Analyser les constituants logiciels des produits de sécurité. Vérifier la robustesse du produit face aux attaques.
- Participer à l'évolution des méthodes et techniques d'évaluation, que ce soit en terme d'écriture de code, que de la maîtrise de la supply chain logicielle. Définir, mettre en place et développer de nouveaux outils ou méthodes d'évaluation par une veille technique permanente dans les domaines de l'analyse et de la sécurité des systèmes d'information.
- Intervenir auprès des industriels de défense, ainsi que des équipes internes de développement.

Compétences métiers

- C++, Java, Python, Assembleur x86 et ARM, Rust
- Fonctionnement d'un compilateur
- Windows, Linux, iOS ou/et Android
- Protocoles réseaux
- Utilisation d'outils d'analyse dynamique
- Cryptographie
- Sécurité informatique

Compétences souhaitées

Compétences indispensables :

- Expertise en développement logiciel
- Expertise en langage C
- Analyse statique de code : outillage, méthodologie de revue de code

Qualités personnelles :

- Curiosité, autonomie, persévérance, esprit d'équipe

Les "+" du poste

Vous travaillez sur différentes technologies et plateformes, auprès de spécialistes qui vous guident pour une montée en compétence et un maintien à niveau dans des domaines techniques de pointe.



2026-CYBER-MI-1028 Ingénieur Expert en analyse de composants électroniques



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Electronique Composants Matériaux
Analyses technologiques

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des expert(e)s en analyse de composants électroniques**.

Mission : L'Expert technique intervient sur l'analyse de composants électroniques essentiellement numériques sur différentes technologies silicium.

L'activité se déroule majoritairement en laboratoire sur divers moyens de caractérisation, de préparation d'échantillons et d'inspections. Ils sont amenés à travailler en étroite collaboration avec les experts en charge de l'évaluation des composants et de la conception. Le travail conduit à nouer des contacts avec tous les acteurs publics ou privés du domaine.

Compétences métiers

- Analyse de composants (micro-section, révélation chimique, microscopie optique et électronique...)
- Maîtrise des technologies d'assemblages
- Microélectronique

Compétences souhaitées

- Rigueur
- Autonomie
- Persévérance
- Initiative

Les "+" du poste

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



2026-CYBER-MI-1029 Ingénieur Evaluation et expertise de la sécurité de composants



Niveau requis	Contrat	Mots-clés
Ingénieur CTI Master 2	Contractuel civil CDI à Bruz (35)	Python Cryptographie Embarqué Informatique IA Electronique

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des ingénieur(e)s en évaluation et expertise cryptographique de la sécurité de composants.**

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

Les experts techniques interviennent sur l'analyse des vulnérabilités des fonctions cryptographiques et des contremesures mises en place dans des composants afin de vérifier la robustesse de celles-ci vis-à-vis d'attaques.

Ils sont amenés à travailler en étroite collaboration avec les équipes en charge de la conception et de l'implémentation des algorithmes cryptographiques gouvernementaux. Le travail les amène à nouer des contacts avec tous les acteurs publics ou privés du domaine.

Compétences métiers	Compétences souhaitées
<ul style="list-style-type: none"> • Electronique : conception ou test de composants ou de cartes • Cryptographie : implémentation et/ou attaques • Langages C et Python • Informatique embarquée (firmware) 	<ul style="list-style-type: none"> • Rigueur • Autonomie • Persévérance • Initiative

Les "+" du poste

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



2026-CYBER-MI-1030

Expert en code embarqué de composants de sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Firmware Assembleur C Python

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des expert(e)s en code embarqué de composants de sécurité.**

Mission :

Les experts techniques interviennent sur l'analyse, l'écriture et la modification de logiciels bas niveau (firmware) sur des composants de type microcontrôleurs, ASIC ou Systems On Chip (SoC). Ils sont amenés à concevoir des solutions optimisées et innovantes pour le matériel cible, les implémenter et les tester.

Compétences métiers

- Architecture de composants numériques
- Logiciel embarqué dans un micro-contrôleur et/ou un composant spécifique
- Langages : C, Python, assembleur (IDA, GHIDRA, etc.)
- Outils de debug temps réel : sondes JTAG

Compétences souhaitées

- Rigueur
- Autonomie
- Persévérance
- Initiative

Les "+" du poste

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



2026-CYBER-MI-1031 Expert en analyse fonctionnelle électronique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Micro-électronique Electronique FPGA
Python IA

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des expert(e)s en analyse fonctionnelle électronique**.

Mission : Les experts techniques réalisent l'analyse de blocs électroniques au niveau RTL (VHDL/Verilog) ou de schémas de portes logiques. Ils sont amenés à en reconstituer les fonctions ainsi qu'en expertiser la sécurité en s'assurant l'absence de vulnérabilité. Ils ont en charge de développer de nouveaux outils permettant d'automatiser les travaux.

Ils sont amenés à travailler en étroite collaboration avec les experts en charge de l'évaluation des composants et de la conception. Le travail les conduit à nouer des contacts avec tous les acteurs publics ou privés du domaine.

Compétences métiers

- Micro-électronique
- Electronique
- Conception de composants de la modélisation jusqu'au test
- Python

Compétences souhaitées

- Rigueur
- Autonomie
- Persévérance
- Initiative

Les "+" du poste

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



2026-CYBER-MI-1032 Administrateur Systèmes et Réseaux



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Administration système Réseaux Windows
Linux Python C

Description du poste (H/F)

Contexte : Dans le cadre de ses activités 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), emploient **des ingénieur(e)s en administration informatique**.

Mission : Assurer l'administration systèmes et réseaux de parcs informatiques composés de 5 à 50 machines.

L'expert technique est responsable du bon fonctionnement des systèmes d'information au sein du département auquel il est rattaché. Ceux-ci sont composés de PC (de 5 à 50) ainsi que d'équipements de mesure et d'expertise. Il est en charge de la gestion au quotidien de ces SI ainsi que de leur évolution dans un contexte sécurité très fort. Il est en contact étroit avec les experts du département afin de développer les services et outils répondant à leurs besoins. Enfin il assure aussi l'interface avec les différents services informatiques du site ainsi qu'avec des industriels.

Compétences métiers

- Administration système Windows et/ou Linux,
- Langages C et Python,
- Administration réseaux (maintenance, fiabilité, évolutions),
- Déploiement des équipements et configuration de l'infrastructure (NAS, firewall, serveur, switch),
- Création et Mise en place de VM.

Compétences souhaitées

- Bonus : connaissances en sécurité des réseaux (réglementation et pratique)
- Qualités personnelles :
- Rigueur, bon relationnel, autonomie, persévérance et initiative

Les "+" du poste

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



2026-CYBER-MI-1033 Expert prototype système embarqué



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Intrusion Capteur Détecteur Prototype
Design

Description du poste (H/F)

Contexte : Dans le cadre 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), emploient **des expert(e)s en analyse de prototype système embarqué.**

Mission : Les experts techniques réalisent l'analyse des protections physiques de produits mettant en œuvre des techniques de détection d'ouverture et d'intrusion (observation, démontage et inspection à l'aide d'outils dédiés) afin d'en déterminer les vulnérabilités. Pour cela, ils doivent définir un plan de test et l'exécuter sur l'équipement.

Ils doivent également faire évoluer les méthodes et techniques d'évaluation, en participant à la définition, au développement et à la mise en place de nouveaux outils ou méthodes d'évaluation par une veille technique dans les domaines de la vérification et de la sécurité physique.

Ils sont aussi amenés à contribuer à la conception de la protection physique sur de nouveaux équipements.

Compétences métiers

- Connaissances en mécanique (lecture de plan/vue 3D, techniques d'assemblage mécanique, etc.)
- Maîtrise de logiciel de CAO (Autocad,...)
- Maîtrise de petit outillage électroportatif
- Analyse de schémas électriques et du routage de cartes électroniques

Compétences souhaitées

- Rigueur
- Autonomie
- Persévérance
- Initiative

Les "+" du poste

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



Index

Administration système	33, 37, 57, 71
Agile.....	17, 52, 53
Analyse de code	45
Analyse de risques.....	35
Analyse dynamique.....	66
Analyse statique	66
Analyses.....	33, 62
Analyses technologiques	67
Android	19, 20
Angular	21, 22
Ansible.....	37, 63
Architecte	42, 47, 48, 52, 54, 55, 64
Architecture.....	35, 40, 41, 53
ASIC.....	46
Assembleur	69
Audit	35, 49, 50, 51
Automatisation	15, 38
Backup	32
BigData	61, 62, 63
Build.....	38
C.....	69
C/C++	30, 43, 45, 56, 66, 71
C2.....	65
Capitalisation.....	11, 12, 13
Capteur	72
CERT	55, 58
Chef de projet.....	52, 58, 64
CI	37, 38
Cloud	26, 53
Composants	67
Conception	39, 40, 41, 44
Conduite de projet	42
Containerisation	26
Cryptographie.....	42, 43, 44, 45, 46, 68
CTI.....	55
Cyber	11
Cyberprotection.....	42
DataMining	12
Datas.....	21, 22

Debugger	45
Design	72
Détecteur	72
Détection intrusion	56, 57
Développement	14, 17, 20, 43, 45
Développeur	25, 26, 27, 28, 30
DevOps	18, 37
DevSecOps	38, 53
DFIR	16
Docker	18, 25, 37, 63
Droits d'accès	34
EBIOS	47, 49, 52
EDR	55, 56
Elasticsearch	57, 61, 63
Electronique	48, 67, 68, 70
Embarqué	27, 28, 42, 68
Expertise	33
Exploit	19, 23, 24, 45
Exploitation	31
Fingerprint	62
Firmware	69
Forensics	16
FPGA	46, 70
Fullstack	21, 22
Fuzzing	19, 23, 24
Gestion de projet	17
Ghidra	19, 23, 24, 45, 59
GLPI	36
Go	30
Grafana	63
GTB	39
Hacking	31
Hadoop	61, 63
Honeypot	56
HPC	32
Hyperviseur	40
IA	26, 68, 70
IaC	32
Iceberg	61
ICS	31, 50

IDA	19, 23, 24, 45, 59
IDS	55
Incidents	60
Informatique	68
Informatique embarquée.....	48
InfraAsCode.....	38
Ingénierie	42
Intégration	15, 17, 18
Internet	12
Intrusion	72
Investigation numérique.....	16
Investigations.....	33
IoC	57
iOS	19, 20
IOT	27, 28, 39
ISO 27001.....	47, 49, 52
JAVA.....	20, 25, 61, 66
k8s.....	37, 63
Kernel	26
KnowledgeGraph	14
Kotlin	20
Kubernetes	18, 37
L2I	64
LID	55, 58
Linux.....	19, 24, 26, 36, 40, 56, 63, 71
LIO	11, 12, 13
LLM	14
Logiciel embarqué.....	40
Matériaux.....	67
Matériel.....	36
Mathématiques	44
MCO	36
Menace.....	60
Micro-électronique	70
Mobile	39
Modélisation.....	11, 12, 13
NDR.....	55, 56
Network.....	32
NLP	14
ObjectiveC.....	20



Offensif	21, 22, 27, 28
Ontology	14
OS	40
OSINT	12, 62
Outils de sécurité	34
OWASP	25
Pentest.....	31, 65
PHP.....	25
Plateformes	39
PoC.....	40, 41
Product Owner	52
Projets	10
Protection du secret	34
Protocoles	30
Prototype.....	72
Python	14, 18, 25, 30, 56, 66, 68, 69, 70, 71
Qualification.....	15
Radio.....	39
Radiofréquences.....	29
Radiologique.....	29
RAG.....	14
RedTeam	18, 20, 21, 22, 26, 65
Réseaux	13, 26, 36, 39, 71
Reverse	19, 23, 24, 45, 59
RSSI	35
Ruby	25
Rust.....	20, 30, 66
Sandbox.....	56
Satellite	39
SCADA.....	31, 50
SCALA	61
SCI	50
Scrapping.....	12
SDN.....	32
SDR	29
Sécurité.....	29
Sécurité des composants	46
Sécurité logiciel.....	43, 66
Sensibilisation sécurité	34
SIEM.....	33, 55, 56, 57



Smartcities.....	31
SMSI.....	49
Snort.....	56
SOC.....	33, 55, 57, 58
Softwareradio.....	29
Spark.....	61, 63
Splunk.....	57
Storage.....	32
Stratégie.....	10
Supervision.....	33, 35
Support.....	37
Suricata.....	56
Swift.....	20
Synthèse.....	35
Système d'exploitation.....	54
Système d'information.....	52, 54
Systèmes.....	18, 39
Systèmes d'armes.....	11
Systèmes embarqués.....	41, 43, 46
Techlead.....	22
Telecom.....	13, 31
Télécommunication.....	30
TEMPEST.....	29
Test.....	15
Tests d'intrusion.....	65
Ticketing.....	36
Traitement du signal.....	29
TTP.....	65
Validation.....	15
VDI.....	32
Veille.....	12
Vérification.....	15
Virtualisation.....	14, 35
VMWare.....	32
Vulnérabilités.....	23, 24, 25, 29, 31, 40, 50, 51
Web.....	25
Windows.....	19, 23, 26, 36, 71
Zeek.....	56