

DGA

Maîtrise de l'information

à BRUZ près de RENNES (35)

Book de postes 2022/2023

Ingénieurs (H/F) Cybersécurité



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



www.defense.gouv.fr/dga

Sommaire

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

Mention : Ce book est une liste des postes prévisionnels pour l'année 2022 pour les différents métiers à DGA Maîtrise de l'information.



MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

La DGA

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



DGA Techniques navales
BREST

DGA Maîtrise de l'information
RENNES

DGA Techniques terrestres
ANGERS

DGA Essais propulseurs
SACLAY

DGA Techniques hydrodynamiques
VAL DE REUIL

DGA Ingénierie des projets
PARIS

DGA Maîtrise NRBC
VERT LE PETIT

DGA Techniques terrestres
BOURGES

DGA Essais de missiles
SAINT MÉDARD

DGA Essais en vol
CAZAUX

DGA Essais de missiles
BISCARROSSE

DGA Techniques aéronautiques
TOULOUSE

DGA Essais en vol
ISTRES

DGA Techniques navales
Toulon

DGA Essais de missiles
Toulon - Ile du Levant

9800

2

Retrouvez notre actualité



@dga



dga



dga



DGA

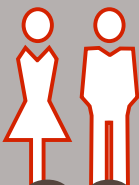
DIRECTION GÉNÉRALE
DE L'ARMEMENT

DGA

Maîtrise de l'information

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




1680

DGA Maîtrise de l'information
Bruz



 3

Un environnement dynamique

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





MINISTÈRE
DES ARMÉES

*Liberté
Égalité
Fraternité*

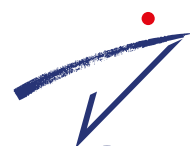
Activités extra- professionnelles



Multiples
activités de
cohésion,
sportives,
culturelles...



5



DGA

DIRECTION GÉNÉRALE
DE L'ARMEMENT

Venez à notre rencontre

► **Breizh CTF**
Rennes



► **Journées des
étudiants**
Webinaire



► **European
Cyber Week**
Rennes



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



Comment postuler ?

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



Les annonces

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





Les postes provisionnels

2022-ICSX-1 Ingénieur Architecte Cybersécurité	12
2022-ICSI-2 Ingénieur Architecte Cyberdéfense	13
2022-ESS-SCI Ingénieur Auditeur technique en sécurité des systèmes Industriels et systèmes d'information	14
2022-ESS-SSI Ingénieur Auditeur technique de la sécurité des systèmes d'information	15
2022-CDP-01 Ingénieur Chef de projet	16
2022-DPS-CDS Ingénieur en architecture de détection d'intrusion système	17
2022-DPS-CPS Ingénieur Cybersécurité	18
2022-DPS-CPSNUM Ingénieur Architecte Solution Cybersécurité	19
2022-DPS-CTD Ingénieur en techniques de détection d'intrusion	20
2022-DPS-SOC Ingénieur Cyberdéfense SOC	21
2022-IAP-01 Ingénieur Architecte produits de sécurité	22
2022-SCY-CA-1 Ingénieur Cryptographie algorithme	23
2022-SCY-CL-1 Ingénieur Recherche de vulnérabilités cryptographiques dans des produits logiciels	24
2022-SCY-CL-2 Ingénieur Conception de logiciel cryptographique	25
2022-SCY-CM-1 Ingénieur Conception Matérielle cryptographie et Sécurité	26
2022-EAP-AL Ingénieur Architecture logicielle de produits de sécurité	27
2022-EAP-AP Ingénieur Architecture de produits de sécurité embarqués	28
2022-APC-IaaS Ingénieur Administration Système et réseaux	29
2022-APC-PaaS Ingénieur Administration et DevOps	30
2022-APC-SaaS Ingénieur Administration Système et réseaux	31
2022-EDS1-1 Ingénieur Développeur Linux C/C++ Cybersécurité	32
2022-EDS1-2 Ingénieur Développeur Android Cybersécurité	33
2022-EDS1-3 Ingénieur Développeur iOS Cybersécurité	34
2022-EDS2-1 Ingénieur développeur C/C++ Cybersécurité	35
2022-EDS2-2 Ingénieur Cybersécurité Cloud Azure	36
2022-EDS3-1 Ingénieur développeur réseau Cybersécurité	37
2022-EDS3-2 Ingénieur développeur fullstack Cybersécurité	38





2022-XIN-AIN Ingénieur Expert en Investigation Numérique	39
2022-XIN-IN Ingénieur Expert Investigation Numérique & Détection d'Intrusion	40
2022-XEO Ingénieur Cyberdéfense Tests et Automatisation	41
2022-XCS Ingénieur Cyberdéfense -Vulnérabilités Composants	42
2022-XIP-ES1 Ingénieur développement logiciel systèmes embarqués Cyberdéfense	43
2022-XIP-ES2 Ingénieur électronique embarquée Cyberdéfense	44
2022-XIP-XPI Ingénieur radio-logicielle Cyberdéfense	45
2022-XIP-XT Ingénieur électronique radio	46
2022-XEL-1 Ingénieur Expert en Sécurité logiciel	47
2022-XEL-2 Ingénieur Infra compilation	48
2022-SECU-1 Ingénieur Analyste supervision de sécurité Cyberdéfense	49
2022-SECU-2 Ingénieur Expert Cybersécurité ASSI/RSSI Cyberdéfense	50
2022-ICM-01 Ingénieur analyste en Cyberdéfense	51
2022-ICM-02 Ingénieur Web sémantique / Graphe de connaissances	52
2022-ICM-07 Ingénieur Analyste en Cyberdéfense Cloud	53
2022-ICM-09 Ingénieur cyber / Lutte informatique d'Influence	54
2022-ICM-10 Ingénieur cyber d'essais /lutte informatique d'influence	55
2022-ICM-11 Ingénieur cyber OSINT / lutte informatique d'influence	56
2022-ICM-12 Data Engineer	57
2022-ICM-13 Big Data Administrator	58
2022-ICM-14 Data Analyst	59
2022-VIM-VSE-1 Ingénieur Cyberdéfense-Reverse-engineering en système d'exploitation Windows	60
2022-VIM-VSE-2 Ingénieur Cyberdéfense-Reverse-engineering en système d'exploitation Linux/Android	61
2022-VIM-VSE-3 Ingénieur Cyberdéfense-Reverse-engineering en système d'exploitation iOS	62
2022-VIM-VSE-4 Ingénieur Cyberdéfense-Reverse-engineering en produits logiciels	63
2022-VIM-VSE-5 Ingénieur Cyberdéfense-Reverse-engineering en systèmes embarqués	64





MINISTÈRE DES ARMÉES

*Liberté
Égalité
Fraternité*



2022-VSP-REVS Ingénieur Retro-Conception et Recherche de vulnérabilités	65
2022-VSP-TH Ingénieur Cyberdéfense en tests d'intrusion	66
Index	68





2022-ICSX-1

Ingénieur Architecte Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

IT EBIOS ISO 27001 SCADA Agilité
AMOA Cybersécurité Cyberdéfense

Description du poste (H/F)

Mission : Prise en compte de la cybersécurité dans les projets de défense, définition d'architectures de sécurité, définition de moyens de cyberdéfense, analyses de risques, élaboration de spécifications techniques, suivi de réalisations industrielles ou étatiques, conduite à l'homologation de sécurité, rédaction de documents de référence.

Contexte : Dans le cadre du renfort de ses activités de définition et suivi des programmes dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une architecte Cybersécurité en charge de la sécurisation des systèmes et/ou de la définition des architectures de supervision de la sécurité.

Compétences indispensables

- Lutte Informatique Défensive
- Réglementation liée à la sécurité
- Méthodologie liée à la sécurité
- Chiffrement, Authentification forte
- Proxy, PKI, SIEM
- Firewalls, IDS, IPS, SOC
- Antivirus, HSM
- Active Directory.

Compétences souhaitées

- Informatique, électronique
- Télécommunications.

Qualités personnelles :

- Fort relationnel, Autonomie
- Aptitudes pour la négociation
- Travail en équipe.

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm. Vous profiterez d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur un ou plusieurs projets d'envergure, et ce, dans un environnement idéal pour votre équilibre de vie pro / perso.





2022-ICSI-2 Ingénieur Architecte Cyberdéfense

Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

SOC APT IT Détection intrusion Réponse à
incidents Sécurité informatique

Description du poste (H/F)

Mission : Mise en place de capacités de supervision de sécurité au profit des SOC's et du CERT du ministère des armées : recueil du besoin utilisateur, définition des architectures cibles, élaboration de spécifications techniques, suivi de réalisations industrielles ou étatiques, accompagnement des forces dans la mise en œuvre des capacités.

Contexte : Dans le cadre de la montée en puissance significative des organismes en charge de la défense des SI du MinArm (SOC's d'armées, CERT MinArm), les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une architecte Cyberdéfense intervenant sur les projets d'implémentation de capacités techniques de supervision de sécurité au profit de ces organismes.

Compétences indispensables

- Cyberdéfense (processus métier de détection et de réponse à incidents),
- Déploiement multi-sites d'équipements en environnement Data center,
- Démarche d'ingénierie système et définition d'architectures de SI,
- Méthodologie liée à la sécurité,
- IDS/IPS, Agents HIDS/HIPS, EDR,
- Collecteurs et indexeurs de logs,
- SIEM, SIRP/SOAR.

Compétences souhaitées

- Informatique, électronique, Télécom.

Qualités personnelles :

- Fort relationnel, Autonomie
- Aptitudes pour la négociation
- Travail en équipe.

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm. Vous profiterez d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur un ou plusieurs projets d'envergure, et ce, dans un environnement idéal pour votre équilibre de vie pro / perso.





2022-ESS-SCI

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 Cyberdéfense
Cybersécurité SSI ICS SCADA SCI

Description du poste (H/F)

Mission : Réalisation d'audits techniques de sécurité relatifs à la mise en œuvre de systèmes industriels, de systèmes d'information et de systèmes d'armes du ministère des armées et des analyses de vulnérabilités sur plateformes de tests en contribuant au développement d'outils d'audit technique de sécurité.

Définir/entretenir une plateforme dédiée aux systèmes industriels pour 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. Sensibiliser/former différents acteurs du ministère des armées sur la sécurisation des systèmes industriels.

Compétences indispensables

- Automatismes et informatique industrielle (automates : Schneider et Siemens, logiciels de supervision : winCC, PCvue, ...)
- Méthodes d'investigation SSI technique
- Ingénierie de la SSI
- Architecture sécurisée de système d'information et de réseau

Compétences souhaitées

- 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

Qualités personnelles :

- Fort relationnel, Autonomie
- Aptitudes pour la négociation
- Travail en équipe.

Les "+" du poste

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





2022-ESS-SSI

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 Cyberdéfense
Cybersécurité **Erreur ! Signet non défini.**SSI

Description du poste (H/F)

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), vous réaliserez des audits techniques de sécurité sur des systèmes d'information et des systèmes d'armes du ministère des armées ainsi que quelques analyses de vulnérabilités sur plateforme de test et contribuerez au développement d'outils d'audit technique de sécurité.

Compétences indispensables

- Méthodes d'investigation SSI technique
- Ingénierie de la SSI
- Architecture sécurisée de système d'information et de réseau
- Configuration ou administration de systèmes d'exploitation Microsoft Windows et Linux, réseaux IP
- Produits et solutions de sécurité, systèmes de supervision de la sécurité

Compétences souhaitées

- Sondes et systèmes de détection d'intrusion
- Systèmes de gestion de bases de données
- Systèmes d'exploitation temps réel
- Systèmes de contrôle industriels (ICS, SCADA)
- Lutte informatique défensive (LID), SOC.

Qualités personnelles :

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

Les "+" du poste

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





2022-CDP-01

Ingénieur Chef de projet



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Projet Serveurs vSphere Cyberdéfense
Erreur ! Signet non défini.

Description du poste (H/F)

Mission : Ingénieur Chef de Projet d'un moyen socle offrant des services communs permettant de réaliser des travaux de R&D, d'expertise et de capitaliser les techniques, sources, outils, tests et exercices autour de la Cybersécurité (protection, lutte informatique). Le développement du moyen sera incrémental en partant de la mutualisation d'infrastructures informatiques existantes et en augmentant l'offre de services au fil des versions.

Tous ces travaux sont réalisés au profit des activités de cyberdéfense, dans le strict respect des exigences du ministère des Armées et des activités liées au domaine.

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une – Ingénieur Chef de projet.

Compétences indispensables

- Gestion de projets
- Conception d'architectures informatiques complexes et hétérogènes
- Très bonne connaissance de la sécurité informatique
- Bonne compétence sur les infrastructures
- Technologies de virtualisation (vmware vSphere, NSX-T)
- Technologie de supervision système et réseaux

Compétences souhaitées

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

Les "+" du poste

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

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. De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso





2022-DPS-CDS

Ingénieur en architecture de détection d'intrusion système



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cyberdéfense **Erreur ! Signet non défini.**LID
TTP SOC IDS NIDS HIDS SIEM Cybersécurité
Erreur ! Signet non défini.Architecture

Description du poste (H/F)

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

Contexte :

La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une ingénieur(e) en architecture de détection d'intrusion système. Lors de votre première année de travail, si besoin, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité.

Compétences indispensables

- 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

Qualités personnelles :

- Travail en équipe et autonomie
- Curiosité, esprit de synthèse, créativité
- Adaptation à des contextes très différents

Compétences souhaitées

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

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-DPS-CPS

Ingénieur Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité Expertise technique
Architecture Système d'exploitation Système
d'information

Description du poste (H/F)

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

Contexte :

La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une ingénieur(e) en cybersécurité. Lors de votre première année de travail, si besoin, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité.

Compétences indispensables

- 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

Qualités personnelles :

- Travail en équipe et autonomie
- Curiosité, esprit de synthèse, créativité
- Savoir restituer une analyse technique à des interlocuteurs variés (profils techniques ou profils décideurs)
- Adaptation à des contextes très différents

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

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-DPS-CPSNUM

Ingénieur Architecte Solution Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité **Erreur ! Signet non défini.** Cloud privé DevSecOps Agile
Architecture

Description du poste (H/F)

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

Contexte : La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une architecte solution cybersécurité. Lors de votre première année de travail, si besoin, vous serez suivi par un référent technique.

Compétences indispensables

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

Qualités personnelles :

- Travail en équipe
- Esprit de synthèse
- Autonomie

Compétences souhaitées

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

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-DPS-CTD

Ingénieur en techniques de détection d'intrusion



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

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

Description du poste (H/F)

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

Contexte : La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une ingénieur(e) en techniques et produits de détection d'intrusion.

Compétences indispensables

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

Compétences souhaitées

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

Qualités personnelles :

- Autonomie, créativité, innovation, rigueur

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe jeune et 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.





2022-DPS-SOC Ingénieur Cyberdéfense SOC



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité **Erreur ! Signet non défini.**SOC
Expertise Détection SIEM IoC Administration
système

Description du poste (H/F)

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

Contexte : La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une ingénieur(e) Cyberdéfense SOC.

Compétences indispensables

- 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 expérimentée et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité. Lors de votre première année de travail, si besoin, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-IAP-01

Ingénieur Architecte produits de sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Architecte Cybersécurité Cyberprotection
Cyberdéfense Embarqué Cryptographie
Ingénierie

Description du poste (H/F)

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

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

Contexte : Dans le cadre du renfort de ses activités dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une Architecte produits de sécurité.

Compétences indispensables

Connaissances générales :

- Informatique et/ou électronique
- Conduite de projet (expérience, motivation)

Qualités personnelles :

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

Compétences souhaitées

Connaissances métier :

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

Les "+" du poste

En tant qu'architecte vous serez au cœur des programmes d'armement pour assurer leur protection contre les menaces cyber. A votre arrivée en poste, vous serez accompagné(e) pour monter en compétence en toute sérénité. En choisissant ce poste, vous profitez du savoir-faire et de l'excellence de DGA MI dans le domaine innovant de la cybersécurité et d'un cursus riche de formations internes et externes vous permettant de devenir rapidement autonome sur des projets d'envergure, et dans un environnement de qualité, idéal pour votre équilibre de vie pro / perso.





2022-SCY-CA-1

Ingénieur Cryptographie algorithmique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cryptographie Chiffrement symétrique
Protocoles Post-quantique

Description du poste (H/F)

Mission :

Développement algorithmique et expertise technique

Contexte :

Dans le cadre du développement de ses activités, le département « Services cryptographiques » recrute un ou une experte en cryptographie algorithmique.

Au sein de ce département, vous serez intégré dans le laboratoire de cryptographie algorithmique.

Votre mission consistera à :

- Spécifier et développer des algorithmes cryptographiques.
- Fournir une expertise technique en cryptographie au profit des programmes d'armement.
- Maintenir un état de l'art sur le domaine de la cryptographie.

Compétences indispensables

- Cryptographie symétrique
- Protocoles cryptographiques et preuves de sécurité
- Cryptographie post-quantique
- Programmation
- Anglais technique

Compétences souhaitées

Qualités personnelles :

- Autonomie
- Curiosité
- Adaptation
- Rigueur

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste.





2022-SCY-CL-1

Ingénieur Recherche de vulnérabilités cryptographiques dans des produits logiciels



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

C Cryptographie Analyse de code
Développement logiciel Debugger Ida
Ghidra Reverse Exploit

Description du poste (H/F)

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

Contexte : Dans le cadre du développement de ses activités, le département « Services cryptographiques » recrute un ou une experte en recherche et exploitation de vulnérabilités cryptographiques pour:

- 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 indispensables

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

Compétences souhaitées

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

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste.





2022-SCY-CL-2

Ingénieur Conception de logiciel cryptographique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

C Cryptographie Analyse de code
Développement logiciel Systèmes embarqués
Sécurité logicielle

Description du poste (H/F)

Mission : Développement de logiciels cryptographiques embarqués

Contexte : Dans le cadre du développement de ses activités, le département « Services cryptographiques » recrute un ou une experte en développement de logiciel cryptographique embarqué pour :

- 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 cryptographiques dans les implémentations.
- Garantir la sécurité des implémentations.
-

Compétences indispensables

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

Qualités personnelles :

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

Compétences souhaitées

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

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste.





2022-SCY-CM-1

Ingénieur Conception Matérielle cryptographie et Sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

FPGA Cryptographie Systèmes embarqués
ASIC Sécurité des composants

Description du poste (H/F)

Mission : Développement matériel ASIC/FPGA pour applications de sécurité

Contexte : Dans le cadre du développement de ses activités, le département « Services cryptographiques » recrute un ou une expert.e en développement matériel ASIC/FPGA pour applications de sécurité.

Au sein de ce département, vous serez intégré dans le laboratoire de cryptographie matérielle. Votre mission consistera à :

- Spécifier et développer des modules matériels cryptographiques.
- Participer aux différentes phases (pré-études, spécifications, architecture, conception, réalisation, validation) des projets de composants de sécurité réalisés en collaboration avec les industriels de la défense.
- Maintenir un état de l'art sur le domaine des composants et des fonctions de sécurité.

Compétences indispensables

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

Qualités personnelles :

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

Compétences souhaitées

- Architecture des composants
- Conception logicielle embarquée (langage C)

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste.





2022-EAP-AL

Ingénieur Architecture logicielle de produits de sécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Windows Architecture Hyperviseur OS
Vulnérabilités Sandbox Sécurité Conception
Rust

Description du poste (H/F)

Mission : Assurer la spécification et la conception des parties logicielles et bas niveau des produits de sécurité (Equipements embarqués ou fixes), effectuer une veille technologique sur l'efficacité des mécanismes de sécurité face à la menace actuelle et réaliser des maquettages de solutions.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ingénieur informatique (H/F) en Architecture Logicielle.

Compétences indispensables

- Connaissance globale de l'architecture d'OS et connaissances/curiosité pour les mécanismes des processeurs

Qualités personnelles :

- Synthétique : Capacité à comprendre et reformuler des besoins de sécurité
- Force de proposition : Capacité à maquetter et proposer des solutions de sécurisation adaptées à des contextes particuliers
- Forte Autonomie : Capacité à monter en compétence de façon autonome

Compétences souhaitées

- Conception ou évaluation d'architectures logicielles
- Vulnérabilités des logiciels
- Mécanismes de sécurité implémentés dans les systèmes d'exploitation et dans les processeurs

Les "+" du poste

En choisissant ce poste, vous expérimenterez les mécanismes de sécurité les plus récents et les plus évolués et vous profiterez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et dans un cadre proposant un équilibre de vie pro / perso.





2022-EAP-AP

Ingénieur Architecture de produits de sécurité embarqués



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Systèmes embarqués architecture SOC
Sécurité Conception POC

Description du poste (H/F)

Mission : Assurer la spécification et la conception d'équipements de sécurité embarqués pour la protection des informations, assurer une veille technologique sur l'efficacité des mécanismes de sécurité face à la menace actuelle et réaliser des maquettages de solutions.

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, la division « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ingénieur en architecture des produits de sécurité.

Compétences indispensables

Connaissances métier (au moins 2 des suivantes):

- Capacité à réaliser, développer un prototype afin de valider une solution de sécurisation
- Maîtrise du langage C, C++
- Capacité à spécifier, concevoir une architecture sécurisée pour un produit de sécurité à base de processeur, FPGA, SOC, ...

Qualités personnelles :

- Capacité d'analyse,
- Autonome,
- Curiosité, Intérêt pour l'innovation, Initiative

Compétences souhaitées

- Connaissance des mécanismes de sécurité permettant de renforcer la sécurité d'un réseau.
- Connaissance des mécanismes de boot sécurisés offerts par des plateformes matérielles (intrinsèque aux composants ou TPM) ;
- Connaissance des protocoles cryptographiques (mécanisme d'authentification, négociation de clés)
- Capacité à mettre en place et administrer une plateforme de tests

Les "+" du poste

En choisissant ce poste, vous expérimenterez les mécanismes de sécurité les plus récents et les plus évolués et vous profiterez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cybersécurité et dans un cadre proposant un équilibre de vie pro / perso.





2022-APC-laaS

Ingénieur Administration Système et réseaux



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

vSphere Nsx-T Serveurs EAR Stockage
Supervision Sécurité

Description du poste (H/F)

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

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

Compétences indispensables

- 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, switchs (HP, Cisco), pare-feux (Arkoon, Stormshield, Forcepoint, pfSense)
- Réseaux Fiber Channel, switch broade
- 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.

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm.

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.

De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.





Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Ansible Docker vSphere DevOps

Description du poste (H/F)

Mission : L'administrateur système DevOps assure le déploiement, la supervision, la gestion, la sécurisation, l'évolution et le maintien en conditions opérationnelles des environnements de développement au profit des activités de CyberDéfense, dans le strict respect des exigences du ministère des Armées et des activités liées au domaine.

Compétences indispensables

- Très bonne connaissance des cycles de développement et de l'intégration continue
- Conception d'architectures de développement complexes et hétérogènes
- Techniques de virtualisation (VMware vSphere et autres)
- Techniques de conteneurisation (Docker, Kubernetes)
- Gestion de configuration (Ansible)
- Orchestration (Tower)
- Supervision de sécurité et système (Wazuh, Logbeat, Check_MK)
- Réseaux IP, routeurs, pare-feux
- Scripts Python, bash
- Support aux utilisateurs
- Développement d'applications au profit des utilisateurs finaux (python, angular, node, ...)

Compétences souhaitées

- Très bonne connaissance de la sécurité informatique
- Qualités personnelles :
- Capacité d'analyse, ingéniosité, inventivité, curiosité, ténacité
 - Goût du travail en équipe, intérêt affirmé pour l'innovation.

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm. 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.

De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.





Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Linux Ansible Docker Win2k19 AD VDI

Description du poste (H/F)

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

L'administrateur système et réseau assure la supervision, la gestion, la sécurisation, l'évolution et le maintien en conditions opérationnelles des systèmes et services 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 indispensables

- Conception d'architectures système complexes et hétérogènes
- Maîtrise des systèmes d'exploitation (Windows, Linux)
- Gestionnaire de configuration (Ansible)
- Gestion d'un parc informatique Windows (GPO, MDT, SCCM)
- Supervision de sécurité et système
- Scripts Python, bash, PowerShell

Compétences souhaitées

- Très bonne connaissance de la sécurité informatique
- Techniques de virtualisation (VMware vSphere, Horizon)
- Techniques de conteneurisation (Docker, VMware Tanzu)
- Réseaux IP, switchs, pare-feux

Qualités personnelles :

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

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm. 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.

De plus, le cadre et l'activité extra-professionnelle du centre vous offrent une qualité et un équilibre de vie pro / perso.





2022-EDS1-1

Ingénieur Développeur Linux C/C++ Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

C/C++ Python Développeur Linux
Embarqué

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'assurer la sécurité logicielle des systèmes du Ministère des Armées.

Votre mission consistera à :

- Concevoir et développer des composants logiciels permettant d'améliorer le niveau de sécurité des systèmes ;
- Développer des démonstrateurs de vulnérabilités dans l'objectif de sensibiliser et de convaincre ;
- Participer au développement des outils métiers liés à l'activité.

Compétences indispensables

Sur l'un ou plusieurs des sujets suivants:

- Maîtrise du langage C ;
- Connaissance en langages C++, Python ;
- Maîtrise du développement sur Linux et en embarqué ;

Qualités personnelles :

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

Compétences souhaitées

- Familier avec les outils de développement (debugger applicatif et noyau, chaîne de compilation) ;
- Familier avec Git, Jenkins (intégration continue) et Jira.

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-EDS1-2

Ingénieur Développeur Android Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Android Kotlin Java C Python

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'assurer la sécurité logicielle des systèmes du Ministère des Armées.

Votre mission consistera à :

- Concevoir et développer des composants logiciels permettant d'améliorer le niveau de sécurité des systèmes Android;
- Développer des démonstrateurs de vulnérabilités dans l'objectif de sensibiliser et de convaincre ;
- Participer au développement des outils métiers liés à l'activité.

Compétences indispensables

Sur l'un ou plusieurs des sujets suivants:

- Maîtrise des langages Java et C ;
- Connaissance en langages Kotlin, Python ;
- Maîtrise du développement d'applications Android;

Qualités personnelles :

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

Compétences souhaitées

- Familier avec les outils de développement (debugger, chaîne de compilation, Gradle, Andoid Studio) ;
- Familier avec Git, Jenkins (intégration continue) et Jira.

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-EDS1-3

Ingénieur Développeur iOS Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur iOS MacOS C ObjectiveC
Swift Python

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'assurer la sécurité logicielle des systèmes du Ministère des Armées.

Votre mission consistera à :

- Concevoir et développer des composants logiciels permettant d'améliorer le niveau de sécurité des systèmes iOS et MacOS;
- Développer des démonstrateurs de vulnérabilités dans l'objectif de sensibiliser et de convaincre ;
- Participer au développement des outils métiers liés à l'activité.

Compétences indispensables

Sur l'un ou plusieurs des sujets suivants:

- Maîtrise des langages C, ObjectiveC/Swift ;
- Connaissance en langages, Python ;
- Maîtrise du développement d'applications iOS

Qualités personnelles :

- Capacité à s'intégrer à une équipe ;
- Etre curieux et avoir un esprit de synthèse.

Compétences souhaitées

- Familier avec les outils de développement (debugger, chaîne de compilation, xCode) ;
- Familier avec Git, Jenkins (intégration continue) et Jira.

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-EDS2-1

Ingénieur développeur C/C++ Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Windows Cybersécurité C/C++
Python

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'assurer la sécurité logicielle des systèmes du Ministère des Armées.

Votre mission consistera à :

- Concevoir et développer des composants logiciels permettant d'améliorer le niveau de sécurité des systèmes ;
- Développer des démonstrateurs de vulnérabilités dans l'objectif de sensibiliser et de convaincre ;
- Participer au développement des outils métiers liés à l'activité.

Compétences indispensables

Sur l'un ou plusieurs des sujets suivants:

- Maîtrise du langage C ;
- Connaissance en langages C++, C#, Python ;
- Maîtrise du développement sur Windows ;

Qualités personnelles :

- Capacité à s'intégrer à une équipe ;
- Etre curieux et avoir un esprit de synthèse.

Compétences souhaitées

- Maîtrise d'outils de développement (debugger applicatif et noyau, chaîne de compilation) ;
- Maîtrise d'outils de gestion de projets / suivi de bugs (Jira, GIT).

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-EDS2-2 Ingénieur Cybersécurité Cloud Azure



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Cloud Azure Cybersécurité
Développement logiciel

Description du poste (H/F)

Mission :

Vous serez intégré dans une équipe dédiée à la sécurité logicielle des systèmes du Ministère des Armées. Votre mission consistera à :

- Assister les équipes XAAS dans l'installation et la configuration d'une plateforme Cloud Azure ;
- Concevoir et développer des démonstrateurs de vulnérabilités (logiciels) en vue d'améliorer le niveau de sécurité de la plateforme ;
- En tant que référent technique, assurer la formation des autres intervenants de l'équipe ;
- Assurer une veille technologique sur les solutions Microsoft Azure ou concurrentes.

Compétences indispensables

- Première expérience en tant qu'Administrateur et/ou utilisateur avancé du Cloud Azure ;
- Maîtrise d'au moins un langage de développement parmi C++, C#, Python ;
- Être force de proposition ;

Qualités personnelles :

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

Compétences souhaitées

- Connaissance du domaine Cyber ;
- Systèmes et infrastructure.

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. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-EDS3-1

Ingénieur développeur réseau Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Réseaux Cybersécurité C/C++
Python

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'assurer la sécurité logicielle des systèmes du Ministère des Armées. Votre mission consistera à :

- Concevoir et développer des composants logiciels permettant d'améliorer le niveau de sécurité des systèmes ;
- Développer des démonstrateurs dans l'objectif de sensibiliser et de convaincre ;
- Participer au développement des outils métiers liés à l'activité.

Les challenges auxquels vous serez confrontés :

- Produire du code de qualité, simple et maintenable.
- Proposer des solutions et architectures innovantes.
- Démêler sans cesse des difficultés techniques inédites.
- Rester au courant sur les nouvelles versions des langages et environnements.
- Concevoir des outils simples à utiliser.

Compétences indispensables

Sur l'un ou plusieurs des sujets suivants:

- Bonne connaissance du langage C/C++
- Connaissance des couches transport TCP/UDP et des protocoles réseau courants
- Maîtrise de l'environnement Linux

Compétences souhaitées

- Familier avec Git, Jenkins (intégration continue) et Jira.
- Notion en python et GO

Les "+" du poste

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





2022-EDS3-2

Ingénieur développeur fullstack Cybersécurité



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Développeur Cybersécurité Fullstack
Python RESTApi Docker

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'assurer la sécurité logicielle des systèmes du Ministère des Armées. Votre mission consistera à :

- Concevoir et développer des composants logiciels permettant d'améliorer le niveau de sécurité des systèmes
- Développer des démonstrateurs dans l'objectif de sensibiliser et de convaincre
- Participer au développement des outils métiers liés à l'activité.

Les challenges auxquels vous serez confrontés :

- Produire du code de qualité, simple et maintenable.
- Proposer des solutions et architectures innovantes.
- Démêler sans cesse des difficultés techniques inédites.
- Rester au courant sur les nouvelles versions des langages et environnements.
- Concevoir des outils simples à utiliser.

Compétences indispensables

Sur l'un ou plusieurs des sujets suivants:

- A l'aise avec un framework back-end tel que Symfony ou autre.
- Bonne connaissance de la technologie front-end (JavaScript, Angular, ReactJS).
- Bonne connaissance du langage python.
- Maîtrise de l'environnement Linux.

Compétences souhaitées

- Sensibilisé à l'api REST,
- Notion sur les bases de données,
- Familier avec Git, Jenkins (intégration continue) et Jira.
- A l'aise avec les outils de containerisation type docker.

Les "+" du poste

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





2022-XIN-AIN

Ingénieur Expert en Investigation Numérique



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Forensic R&D Investigation numérique DFIR

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est d'analyser la furtivité des outils de test d'intrusion au profit des besoins de DGA-MI.

Dans un contexte de R&D en investigation numérique, votre mission sera de caractériser l'empreinte de ces outils (mémoire, disque, réseau, etc.) sur des environnements multiples.

Contexte :

La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une expert(e) technique en investigation numérique. Lors de votre première année de travail, si besoin, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité.

Compétences indispensables

- Fonctionnement des OS standard (Windows, Linux, Android)
- Artefacts forensiques
- Fonctionnement de TCP/UDP et des protocoles réseau courant
- Outils d'investigation numérique (The Sleuth Kit, Volatility, Wireshark)

Qualités personnelles :

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

Compétences souhaitées

- Sécurité Informatique
- Connaissance approfondie des OS standard (Windows, Linux, Android)
- Développement de preuve de concept (C/C++, Python)
- Matrice ATT&CK et implémentation des techniques associées
- Connaissances DFIR

Les "+" du poste

Vous profiterez d'un cursus de formations internes et externes riche vous permettant de devenir rapidement autonome sur un ou plusieurs projets d'envergure, et ce, dans un environnement idéal pour votre équilibre de vie pro / perso.





2022-XIN-IN

Ingénieur Expert Investigation Numérique & Détection d'Intrusion



Niveau requis

Contrat

Mots-clés

Ingénieur CTI
Master 2

Contractuel civil
CDI à Bruz (35)

Forensic LID TTP IDS HIDS SIEM

Description du poste (H/F)

Mission :

Vous serez intégré à une équipe dont l'objectif est de mener des analyses d'investigation numérique sur des environnements multiples, d'expertiser des architectures de détection d'intrusion système et des stratégies de Lutte Informatique.

Contexte :

La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une expert(e) technique en investigation numérique/détection d'intrusion. Lors de votre première année de travail, si besoin, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité.

Compétences indispensables

- Sondes de détection d'intrusion, honeypot, sandbox, collecteurs d'évènements, SIEM
- Réalisation de preuve de concept
- Connaissance du comportement des malwares et de techniques d'exploitation
- Framework d'exploitation et d'automatisation (atomic-redteam, metasploit, Robot)
- Architecture bas niveau et mécanismes internes de Windows/Linux
- Outils d'investigation numérique (The Sleuth Kit, Volatility, Sysinternals, Jadx ...)

Compétences souhaitées

- Systèmes d'exploitation (Windows, Linux, Android ...)
- Sécurité informatique
- Réseau/Télécommunication
- Techniques de virtualisation
- Développement informatique : C, C++, C#
- Scripting (bash, python, powershell, ...).

Qualités personnelles :
Autonomie, créativité, innovation, rigueur.

Les "+" du poste

En choisissant ce poste, vous intégrez une équipe jeune et dynamique, vous profitez de formations internes et externes, 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.





2022-XEO

Ingénieur Cyberdéfense Tests et Automatisation



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cyberdéfense Test Automatisation

Description du poste (H/F)

Mission :

Tester et qualifier des logiciels de cybersécurité. Pour chaque projet, vous travaillerez dans une équipe pluridisciplinaire en collaboration étroite avec les analystes et les développeurs du logiciel à qualifier.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur tests et automatisation.

Compétences indispensables

- Définition de stratégie de test
- Rédaction de plan de test
- Création et configuration de plateforme de test
- Exécution de tests manuels
- Automatisation de tests
- Veille technique

Qualités personnelles :

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

Compétences souhaitées

- Android, iOS, ...
- Python, C, Javascript, ...
- VmWare (ESX, vCenter), Docker, Ansible, ...
- Réseaux IP, réseaux mobiles, ...
- Linux, Windows, MacOS...
- DNS, DHCP, Proxy, Firewall, IDS, bases de données, ...
- Git, JIRA, Testlink, ...

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, et ce, dans un environnement idéal pour votre équilibre de vie pro / perso. Vous intégrerez des équipes projets à échelle humaine (3 à 6 personnes), travaillerez en méthodes Agiles et serez accompagné(e) par les experts et collègues pour votre montée en compétence.





2022-XCS

Ingénieur Cyberdéfense -Vulnérabilités Composants



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Electronique Vulnérabilités Composants

Description du poste (H/F)

Mission : Analyser le niveau de sécurité de composants et sous modules électroniques. Rechercher des vulnérabilités en définissant et exécutant un plan de test. Développer et mettre en œuvre des outils pour rechercher ces vulnérabilités (développement de cartes, tests spécifiques).

Au sein du département eXpertise et évaluation de Composants Sécurisés (XCS), vous serez chargé de définir, spécifier et réaliser des expertises de sécurité à l'état de l'art du domaine ainsi qu'à participer à la définition et la mise en place de nouvelles méthodes et moyens d'investigation de composants électroniques pour la Cyberdéfense. Vous interviendrez sur l'ensemble des fonctions du composant (du niveau transistor au logiciel embarqué en passant par les fonctions électroniques) afin d'évaluer la sécurité des composants vis-à-vis d'attaques matérielles et logicielles.

Votre travail vous amènera à nouer des contacts avec tous les acteurs publics ou privés du domaine.

Compétences indispensables

- Electronique numérique et informatique (firmware)
- Composants électroniques : CPLD/FPGA, ASICs, microcontrôleur, cartes à puce, ...
- Langages VHDL, Python, C

Qualités personnelles :

- Rigueur
- Autonomie et Initiative
- Persévérance

Compétences souhaitées

- Algorithmes et protocoles cryptographiques
- Intelligence artificielle

Les "+" du poste

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

Enfin, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-XIP-ES1

Ingénieur développement logiciel systèmes embarqués Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Embarqué Vulnérabilités Logiciel Sécurité
Cybersécurité

Description du poste (H/F)

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

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

Compétences indispensables

- Maîtrise de langages de programmation (C, C++, asm, Python...) et de leurs environnements (OS, hyperviseur, cross-compileur...) sur systèmes embarqués.
- CPLD/FPGA, langage VHDL.
- Protocoles courants pour le fonctionnement des services réseaux (ARP, IPv4/IPv6, TCP/UDP, SNMP) et des protocoles de sécurité (IPSEC).
- Outils de type émulateur, débogueur et analyseur de protocoles.
- Méthodologies de revue de code.

Compétences souhaitées

- Mise en œuvre de méthodologies de tests dans l'objectif de rechercher des vulnérabilités.
 - Mise en œuvre d'outils de fuzzing de protocole.
 - Lecture de schémas électroniques, analyse du routage.
- Qualités personnelles :
- Capacité d'analyse,
 - Initiative, Goût du travail en équipe
 - Curiosité, Intérêt pour l'innovation.

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm.





2022-XIP-ES2

Ingénieur électronique embarquée Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Embarqué Radio-Navigation Electronique

Description du poste (H/F)

Mission : Expertiser la sécurité des équipements de radio-navigation par satellites intégrés dans les systèmes d'armes. Analyser l'architecture des équipements et leur intégration dans les systèmes. Réaliser des essais chez le maître d'œuvre industriel. Auditer le processus industriel.

Contexte : Intégré à une équipe dynamique dont la mission est d'évaluer le niveau de sécurité d'équipements de systèmes d'information du Ministère des Armées, vous réaliserez principalement, avec un collaborateur, des contrôles de conformité de récepteurs GPS militaire et de leur intégration sur des porteurs, sous l'angle de la sécurité des systèmes d'information. Cette activité nécessite une dizaine de déplacements annuels en France métropolitaine, d'une durée de 3 jours à 1 semaine. Ce poste requiert polyvalence et connaissances en informatique embarquée, électronique, cybersécurité et des notions de cryptographie. Il sera amené à évoluer vers le traitement des nouveaux récepteurs liés aux programmes Galiléo et OMEGA.

Compétences indispensables

- Langages (C, C++, asm, Python, ...) et environnements (OS, interfaces, ...) de programmation sur systèmes embarqués.
- Electronique (Bus, cartes, composants, ...)
- Protocoles courants sur équipements embarqués (Ethernet, RS232, RS422, MIL-STD-1553, ARINC 429 ...).
- Outils de type émulateur, debugueur et analyseur de protocoles.
- Méthodologies de revue de code.
- Protocoles et architectures cryptographiques

Compétences souhaitées

- Fonctionnement des systèmes de radio-navigation par satellites (GPS, ...)
- Lecture de schémas électroniques, analyse du routage.
- Cryptographie (Principes, Architecture, protocoles)

Qualités personnelles :

- Rigueur.
- Réactivité
- Goût du travail en équipe
- Capacité d'analyse

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm.





2022-XIP-XPI

Ingénieur radio-logicielle Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

RF Radiofréquence Radiologique SDR
Vulnérabilité Software radio Traitement du
signal

Description du poste (H/F)

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

Intégré dans une équipe dynamique dont la principale mission est de mener une activité de Recherche et Développement en Cyberdéfense pour le compte du Ministère des Armées dans le domaine de l'analyse de la sécurité des interfaces radio, vous mènerez des analyses sur les couches basses protocolaires de systèmes de communication. Vous serez ainsi amené à étudier, développer des protocoles d'échange de données et à les mettre en œuvre sur des plateformes radio-logicielles lors d'expérimentations.

Compétences indispensables

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

Compétences souhaitées

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

Qualités personnelles :

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

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm.





2022-XIP-XT

Ingénieur électronique radio



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

RF Radiofréquence Radiologique SDR
Vulnérabilité Electromagnétisme TEMPEST
Traitement du signal SPC

Description du poste (H/F)

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

Intégré dans une équipe dynamique dont la principale mission est de mener une activité d'évaluation, de recherche et de développement en Cyberdéfense pour le compte du Ministère des Armées dans le domaine des phénomènes électromagnétiques, vous piloterez des campagnes de tests TEMPEST sur des matériels et plateformes en laboratoire ou sur le territoire national et à l'étranger, vous réaliserez des outils à base de récepteurs radiofréquence ou radio-logiciel, vous participerez à des projets de recherche et d'ingénierie dans le domaine de la radio. Permis de conduire de véhicules de catégorie B indispensable.

Compétences indispensables

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

Compétences souhaitées

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

Qualités personnelles :

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

Les "+" du poste

A votre arrivée en poste, vous serez accompagné(e) par vos collègues et référents métiers dans votre montée en compétence et en connaissance du domaine de la Cyber au sein du MinArm.





2022-XEL-1

Ingénieur Expert en Sécurité logiciel



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Expertise Développement Sécurité logiciel
Analyse statique Analyse dynamique C/C++
Python Rust Java Android iOS Windows Linux

Description du poste (H/F)

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

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

Dans le cadre de vos travaux, vous interviendrez également auprès des industriels de défense et pourrez échanger avec les spécialistes académiques des domaines concernés et être amené.e à publier le résultat de vos travaux.

Compétences indispensables

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

Compétences personnelles :

Curiosité, Autonomie, Persévérance, Esprit d'équipe

Compétences souhaitées

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

Les "+" du poste

Intégré.e dans une équipe possédant de multiples compétences, vous serez formé.e sur de nombreux sujets répondant aux enjeux techniques actuels. Vous profiterez du savoir-faire et des moyens de la DGA-MI dans le domaine porteur de la cybersécurité, tout en bénéficiant d'un cadre de travail privilégié.





2022-XEL-2

Ingénieur Infra compilation



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

DevSecOps Compilation Build CI/CD

Description du poste (H/F)

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

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

Compétences indispensables

- Polyvalence
- Autonomie
- Bonne connaissance de Python, de PowerShell et de Bash
- Maîtrise Windows et Linux

Compétences personnelles :

Curiosité, Autonomie, Persévérance, Esprit d'équipe

Compétences souhaitées

- Sensibilisé à la sécurité des systèmes d'information
- Familier Git et Jenkins
- Docker, Packer, Terraform
- Ansible

Les "+" du poste

Intégré.e dans une équipe possédant de multiples compétences, vous serez formé.e sur de nombreux sujets répondant aux enjeux techniques actuels. Vous profiterez du savoir-faire et des moyens de la DGA-MI dans le domaine porteur de la cybersécurité, tout en bénéficiant d'un cadre de travail privilégié.





2022-SECU-1

Ingénieur Analyste supervision de sécurité Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité Supervision SIEM
Investigations Analyses SOC Administration
système Expertise

Description du poste (H/F)

Mission : Contribuer à la supervision de la sécurité, à la détection et l'analyse des événements ou informations collectés des moyens opérationnels de Cyberdéfense de DGA MI. Intégrer des outils de collecte et de détection et assurer le maintien en condition de sécurité de moyens techniques en cyberdéfense.

Contexte :

La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une ingénieur(e) Cyberdéfense analyste de supervision de sécurité.

Compétences indispensables

- 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
- Connaissance de modes opératoires d'attaquants
- Connaissance des techniques d'exploitation de vulnérabilités
- 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 jeune et dynamique, vous profitez du savoir-faire et des moyens de DGA MI dans le domaine innovant de la cyberdéfense. Lors de votre arrivée vous serez accompagné par un collaborateur afin d'appréhender en toute sérénité votre nouveau poste. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-SECU-2

Ingénieur Expert Cybersécurité ASSI/RSSI Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Cybersécurité Analyse de risques ISO 27001
EBIOS Synthèse RSSI Audit Risk Manager

Description du poste (H/F)

Mission : Assurer la maîtrise de la sécurité des moyens opérationnels de Cyberdéfense de DGA MI dans un environnement de management des risques. Piloter les processus d'homologation de sécurité et assurer le rôle de RSSI de système. Rédaction de documents de sécurité et analyse de risques.

Contexte :

La Direction Générale de l'Armement, site de Bruz (près de Rennes), recrute un ou une expert(e) sécurité Adjoint SSI/RSSI Cyberdéfense.

Compétences indispensables

- Investigations SSI techniques et organisationnelles
- Réglementation sécurité : Protection du secret, du patrimoine scientifique et technique, homologation des SI
- Normes sécurité : ISO 27xxx, Certification CISSP, Risk manager..., analyse de risques
- Ingénierie de la SSI
- Droit du numérique

Compétences souhaitées

- Analyse documentaire, synthèse et présentation de résultat
- Connaissances générales des architectures de SI

Qualités personnelles :

- Autonome tout en sachant travailler en équipe
- Très bon relationnel
- Rigoureux
- Curieux

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 cyberdéfense. Lors de votre arrivée vous serez accompagné par un collaborateur afin d'appréhender en toute sérénité votre nouveau poste. De plus, nous vous offrons une qualité et un équilibre de vie pro / perso.





2022-ICM-01

Ingénieur analyste en Cyberdéfense



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Menace Modélisation Attaque Information

Description du poste (H/F)

Mission : Analyse de systèmes avec le point de vue de l'attaquant, conception de scénarii et contribution à l'identification de vulnérabilités résiduelles.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un. ou une ingénieur pluridisciplinaire pour analyser la sécurité des systèmes d'information et des systèmes d'armes.

Compétences indispensables

- Maîtrise des architectures des systèmes d'information sur différents types de systèmes ;
- Expérience dans la recherche d'information et l'analyse de documentation ;
- Sécurité des systèmes d'information

Compétences souhaitées

- Méthodes de modélisation ;
- Capacité de synthèse et de présentation de résultat d'étude.

Qualités personnelles :

- Autonomie, créativité, curiosité, innovation

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.





2022-ICM-02

Ingénieur Web sémantique / Graphe de connaissances



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

KnowledgeGraph LinkedData

Description du poste (H/F)

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

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cybersécurité, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur Web sémantique/ Graphe de Connaissances.

Compétences indispensables

- Maîtrise des normes RDF, RDFS, OWL 2, SPARQL;
- Connaissance des normes SHACL, R2RML, outil et norme de raisonnement;
- Connaissances en base graphes de type triple stores

Compétences souhaitées

- Le développement informatique : python, java ;
- Des connaissances en développement IHM JavaScript

Qualités personnelles :

- Autonomie, créativité, innovation

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.





2022-ICM-07

Ingénieur Analyste en Cyberdéfense Cloud



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Menace Modélisation Attaque Information
Cloud

Description du poste (H/F)

Mission : La personne titulaire du poste sera intégrée dans une équipe dédiée à la conception de plateformes d'exploitation des données d'intérêt pour la Cyberdéfense. Elle sera chargée de l'analyse de systèmes de type « informatique en nuage » (cloud) avec le point de vue de l'attaquant, conception de scénarii et contribution à l'identification de vulnérabilités résiduelles.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur pluridisciplinaire pour analyser la sécurité des systèmes d'information de type cloud.

Compétences indispensables

- Expérience dans la mise en œuvre d'une architecture cloud (OpenStack, vmware ...) ;
- Expérience dans l'administration de la sécurité d'une architecture cloud (OpenStack, vmware...) ;
- Expérience dans la recherche d'information et l'analyse de documentation ;
- Sécurité des systèmes d'information

Compétences souhaitées

- Méthodes de modélisation ;
- Capacité de synthèse et de présentation de résultat d'étude.

Qualités personnelles :

- Autonomie, créativité, curiosité, innovation

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.





2022-ICM-09

Ingénieur cyber / Lutte informatique d'Influence



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

L2I IA OSINT NLP

Description du poste (H/F)

Mission : La personne recrutée sera intégrée à une jeune équipe en cours de création et contribuera au développement et à la structuration de l'activité de lutte informatique d'influence (L2I) du ministère des armées.

Contexte :

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

Les moyens de veilles, détection et caractérisation des menaces qu'il est nécessaire de mettre en œuvre dans ce cadre s'appuient sur des technologies innovantes dans un environnement complexe et en mutation technologique rapide et permanent.

DGA-MI cherche donc des ingénieurs dans des domaines aussi variés que le développement full-stack, les data-sciences, l'intelligence artificielle, la conduite de projets, l'évaluation et les tests, etc..

Compétences indispensables

- Curiosité ;
- Esprit d'initiative, autonomie, dynamisme
- Travail en équipe ;
- Adaptabilité et appétence aux nouvelles technologies

Compétences souhaitées

Les "+" du poste

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





2022-ICM-10

Ingénieur cyber d'essais /lutte informatique d'influence



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

L2I ESSAIS OSINT

Description du poste (H/F)

Mission : La personne sera chargée d'assurer les fonctions d'évaluation et de test de produits développés par une maîtrise d'œuvre industrielle dans le cadre de projets de collecte de données OSINT. Elle aura en charge :

- L'évaluation fonctionnelle et technique des produits proposés par la maîtrise d'œuvre industrielle ;
- L'évaluation de l'adéquation du produit fournit par l'industriel avec les spécifications initiales ;
- Les relations avec les experts métiers de DGA-MI et les opérationnels du Ministère des Armées.

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) Cyber pour développer une équipe d'experts spécialisés dans le domaine de la Lutte Informatique d'Influence (L2I).

A ce titre, vous assurerez des prestations d'analyse du besoin, de spécification, de pilotage de travaux liés à la collecte d'informations en source ouverte (internet, réseaux sociaux, darkweb, ...), ainsi que l'évaluation et les essais associés :

- En établissant et en déroulant les plans de tests nécessaire à la validation des produits livrés par la maîtrise d'œuvre industrielle ;
- En assurant la vérification de l'adéquation fonctionnelle et technique de la solution proposée par la maîtrise d'œuvre industrielle aux spécifications initiales ;
- En participant en collaboration avec les experts et opérationnels du ministère des Armées à l'adaptation des spécifications des versions ultérieures des produits ;

Compétences indispensables

- Architectures systèmes et réseaux en nuage ;
- VMWare (ESX, Vcenter), Ansible, Kubernetes, Docker ;
- Sécurisation des systèmes d'information ;
- Outils de développement logiciel, suivi de bug et de versions (JIRA, Git,...)

Compétences souhaitées

- Dynamisme, autonomie, relationnel ;
- Rigueur, organisation
- Travail en équipe ;
- Adaptabilité, et appétence aux nouvelles technologies.





2022-ICM-11

Ingénieur cyber OSINT / lutte informatique d'influence



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

OSINT L2I NLP IA Big Data

Description du poste (H/F)

Mission : La personne sera chargée d'assurer les fonctions d'expertise en OSINT dans le cadre du développement des activités de lutte informatique d'influence. Elle aura en charge :

- La spécification des besoins liés à la collecte d'informations en sources ouvertes;
- La veille liée aux techniques de collecte en source ouverte ;
- La prescription, le suivi et l'évaluation des travaux confiés aux industriels ;
- Les relations avec les experts métiers de DGA-MI et du Ministère des Armées.

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une ingénieur(e) Cyber pour développer une équipe d'experts spécialisés dans le domaine de la Lutte Informatique d'Influence (L2I).

Le(a) candidat(e) devra posséder des compétences dans le domaine de la collecte de données en sources ouvertes. Il (elle) devra également faire preuve de dynamisme, d'initiative, de curiosité et avoir un goût prononcé pour le travail en équipe.

A ce titre, vous assurerez des prestations de veille, de conseil, de spécification et de suivi de travaux liés à la collecte d'informations en source ouverte :

- En contribuant à assurer une veille sur la connaissance du domaine, permettant d'assurer les orientations dans le choix des technologies à utiliser pour les outils de collecte OSINT ;
- En participant en collaboration avec les experts et opérationnels du ministère des Armées à la spécification des produits ;
- En identifiant les techniques émergentes et outils civils disponibles et leurs adaptations aux applications spécifiques défense
- - En assurant la spécification des exigences techniques dans le cadre de la réalisation de produits par une maîtrise d'œuvre industrielle ;

Compétences indispensables

- Technologies Big Data (HDFS, Hadoop, NoSQL, Neo4j, elasticsearch...);
- Environnement Cloud (outils de déploiement : Ansible, Kubernetes, Docker)

Compétences souhaitées

- Curiosité, initiative, autonomie, dynamisme ;
- Travail en équipe ;
- Adaptabilité et appétence aux nouvelles technologies.





2022-ICM-12
Data Engineer



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Bigdata Spark Hadoop Elasticsearch Java
Scala Iceberg

Description du poste (H/F)

Mission :

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

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un Data Engineer.

Compétences indispensables

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

Compétences souhaitées

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

Les "+" du poste

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.





2022-ICM-13
Big Data Administrator



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Bigdata Spark Hadoop ElasticsearchAnsible
Docker Prometheus

Description du poste (H/F)

Mission :

La personne titulaire du poste sera intégrée dans une équipe dédiée à la conception de plateformes Big Data hébergeant des données d'intérêt pour la Cyberdéfense. Elle travaillera conjointement avec les équipes « Data » (Engineering/Analysts/Science) sur la définition, l'implémentation et l'exploitation de plateformes Big Data reposant sur une pile logicielle interne.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un Administrateur Big Data

Compétences indispensables

- Bon relationnel.
- Automatisation et déploiement (Ansible, CI/CD, ...).
- Maîtrise des solutions de conteneurisation (Docker, Swarm, Kubernetes, ...).
- Administration système (linux, supervision, ...).

Compétences souhaitées

- Administration de composants Big Data (Hadoop, Spark, Elasticsearch, ...).
- Connaissance du domaine Cyber.

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.





2022-ICM-14 Data Analyst



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Analyse Fingerprint Hacking Big Data

Description du poste (H/F)

Mission :

La personne titulaire du poste sera intégrée dans une équipe dédiée à la conception de plateformes Big Data permettant d'exploiter les données d'intérêt pour la Cyberdéfense. Elle sera chargée de contribuer à l'analyse des données et à l'amélioration continue des outils et méthodes de détection.

Contexte :

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

Le poste consiste à :

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

Compétences indispensables

- 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

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.





2022-VIM-VSE-1

Ingénieur Cyberdéfense–Reverse-engineering en système d'exploitation Windows



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Exploit Windows Fuzzing ROP

Description du poste (H/F)

Mission : Les missions de rétro-ingénierie consistent en l'étude de programmes complexes pour en comprendre les fonctionnalités, les documenter afin de rechercher des vulnérabilités. Cela peut également mener au développement d'une preuve de concept concernant son exploitation.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une experte en Reverse-engineering en système d'exploitation Windows.

Compétences indispensables

Connaissances générales :

- Maîtrise de Windows
- Développement C/C++, Python
- Développement driver bas niveau Windows
- Désassembleurs et débogueurs

Qualités personnelles :

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

Compétences souhaitées

Connaissances métier :

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

Les "+" du poste

Vous rejoindrez une équipe soudée, heureuse de transmettre et avide d'apprendre. Vous bénéficierez également d'une formation interne spécifique aux métiers reverse-engineering/analyse de malware dispensée par les experts de DGA-MI.





2022-VIM-VSE-2

Ingénieur Cyberdéfense–Reverse-engineering en système d'exploitation Linux/Android



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Exploit Linux Android Fuzzing
ROP

Description du poste (H/F)

Mission : Les missions de rétro-ingénierie consistent en l'étude de programmes complexes pour en comprendre les fonctionnalités, les documenter afin de rechercher des vulnérabilités. Cela peut également mener au développement d'une preuve de concept concernant son exploitation.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une experte en Reverse-engineering en système d'exploitation Linux/Android.

Compétences indispensables

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

Qualités personnelles :

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

Compétences souhaitées

Connaissances métier :

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

Les "+" du poste

Vous rejoindrez une équipe soudée, heureuse de transmettre et avide d'apprendre. Vous bénéficierez également d'une formation interne spécifique aux métiers reverse-engineering/analyse de malware dispensée par les experts de DGA-MI.





2022-VIM-VSE-3

Ingénieur Cyberdéfense-Reverse-engineering en système d'exploitation iOS



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA Exploit iOS Fuzzing ARM ROP

Description du poste (H/F)

Mission : Les missions de rétro-ingénierie consistent en l'étude de programmes complexes pour en comprendre les fonctionnalités, les documenter afin de rechercher des vulnérabilités. Cela peut également mener au développement d'une preuve de concept concernant son exploitation.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une experte en Reverse-engineering en système d'exploitation iOS.

Compétences indispensables

- Maîtrise d'iOS
- Développement C/C++, Python
- Développement driver bas niveau iOS
- Désassembleurs et débogueurs

Qualités personnelles :

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

Compétences souhaitées

Connaissances métier :

- Recherche de vulnérabilités
- Connaissance en assembleur ARM
- Développement d'outils d'aide à la rétro ingénierie
- Veille technologique régulière

Les "+" du poste

Vous rejoindrez une équipe soudée, heureuse de transmettre et avide d'apprendre. Vous bénéficierez également d'une formation interne spécifique aux métiers reverse-engineering/analyse de malware dispensée par les experts de DGA-MI.





2022-VIM-VSE-4

Ingénieur Cyberdéfense–Reverse-engineering en produits logiciels



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA/Ghidra Exploit Fuzzing ROP

Description du poste (H/F)

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

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une experte en Reverse-engineering en produits logiciels.

Compétences indispensables

- Connaissance en assembleur (x86, ARM, MIPS...)
 - Développement C, python
 - Désassembleurs, debuggers
- Qualités personnelles :
- Curieux, innovant, à la recherche de nouveaux défis
 - Tenace, persévérant

Compétences souhaitées

- Connaissances métier :
- Techniques de recherche de vulnérabilités
 - Méthodes de protection logicielles et contournement
 - Architecture d'OS standards et embarqués
 - Veille technologique régulière

Les "+" du poste

Vous rejoindrez une équipe soudée, heureuse de transmettre et avide d'apprendre. Vous bénéficierez également d'une formation interne spécifique aux métiers reverse-engineering/analyse de malware dispensée par les experts de DGA-MI.





2022-VIM-VSE-5

Ingénieur Cyberdéfense–Reverse-engineering en systèmes embarqués



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse IDA/Ghidra Exploit Fuzzing ROP

Description du poste (H/F)

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

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un ou une experte en Reverse-engineering en systèmes embarqués.

Compétences indispensables

- Connaissance en assembleur (ARM, MIPS...)
 - Développement C, python
 - Désassembleurs, debuggers
- Qualités personnelles :
- Curieux, innovant, à la recherche de nouveaux défis
 - Tenace, persévérant

Compétences souhaitées

- Connaissances métier :
- Techniques de recherche de vulnérabilités
 - Systèmes embarqués, temps réel
 - Méthodes de protection logicielles
 - Architecture d'OS embarqués, cross-compilation
 - Radio logicielle

Les "+" du poste

Vous rejoindrez une équipe soudée, heureuse de transmettre et avide d'apprendre. Vous bénéficierez également d'une formation interne spécifique aux métiers reverse-engineering/analyse de malware dispensée par les experts de DGA-MI.





2022-VSP-REVS

Ingénieur Retro-Conception et Recherche de vulnérabilités



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Reverse Exploit Windows Linux Réseau
Protocoles

Description du poste (H/F)

Mission : Retro-conception et recherche de vulnérabilités sur des applications serveurs ; de l'analyse de la surface d'attaque au développement d'exploits et démonstrations techniques.

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 « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un expert en Retro-conception et recherche de vulnérabilités.

Compétences indispensables

- Développement C/C++, Java, C#, Python
- Protocoles réseaux
- Systèmes Windows ou Linux

Qualités personnelles :

- Inventif, curieux, passionné, esprit d'équipe

Compétences souhaitées

Connaissances métier :

- Recherche de vulnérabilités
- Développement, analyse, débogage et rétro-conception d'applications natives, .NET ou Java EE
- Décompilateurs, désassembleurs et débogueurs
- Connaissance en assembleur x86/x64

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste.

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





2022-VSP-TH

Ingénieur Cyberdéfense en tests d'intrusion



Niveau requis

Ingénieur CTI
Master 2

Contrat

Contractuel civil
CDI à Bruz (35)

Mots-clés

Test d'intrusion Pentest Vulnérabilités
TTP Sécurité offensive

Description du poste (H/F)

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

Contexte :

Dans le cadre du renfort de ses activités de recherche et développement dans les domaines de la sécurité informatique et de la Cyberdéfense, les divisions « Sécurité des Systèmes d'Information » de la Direction Générale de l'Armement, site de Bruz (près de Rennes), recrutent un expert en tests d'intrusion.

Compétences indispensables

- Systèmes d'exploitation et leur administration (Windows, Linux, Android...);
- Connaissances applicatives (Active Directory, LDAP, Serveurs Web, Serveurs de messagerie, DNS, SGBD, applications de sécurité (HIDS, NIDS, Antivirus, produit de supervision...), etc.)
- Technologies réseaux et protocoles associés;
- Développement Python, C/C++, Java, C#

Qualités personnelles :

- Inventif, curieux, passionné, esprit d'équipe

Compétences souhaitées

Connaissances métier :

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

Les "+" du poste

Lors de votre arrivée, vous serez accompagné par un collaborateur afin de vous guider au cours des différentes étapes de prise de poste.





**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*



DGA

DIRECTION GÉNÉRALE
DE L'ARMEMENT





Index

AD.....	32
Administration système	21, 50
Agilité	12, 19
AMD64.....	63, 64, 65
AMOA.....	12
Analyse.....	60
Analyse de code	25, 26
Analyse de risques.....	51
Analyse dynamique.....	48
Analyse statique	48
Analyses.....	50
Android.....	34, 48
Ansible.....	31, 32, 59
APT.....	13
Architecte	22
Architecture.....	17, 18, 19, 28, 29, 41
ASIC.....	27
Attaque.....	52, 54
Audit	14, 15, 51
Automatisation.....	42
Big Data.....	57, 58, 59, 60
Build.....	49
C.....	20, 25, 26, 34, 35
C/C++.....	33, 36, 38, 48
Chiffrement symétrique	24
CI/CD	49
Cloud	54
Cloud Azure	37
Cloud Privé	19





Compilation.....	49
Composants	43
Conception	28, 29
Cryptographie.....	22, 24, 25, 26, 27
Cyberdéfense.....	22
Cyberdéfense.....	16
Cyberprotection.....	22
Cybersécurité	22
Debugger	25
Détection.....	21
Détection intrusion	13, 20
Développement.....	48
Développement logiciel	25, 26, 37
Développeur.....	33, 34, 35, 36, 37, 38, 39
DevOps.....	31
DevSecOps	19, 49
DFIR	40
Docker	31, 32, 39, 59
EAR.....	30
EBIOS	12, 51
Elasticsearch.....	58, 59
Electromagnétisme.....	47
Electronique	43, 45
Embarqué	22, 33, 44, 45
ESSAIS	56
Expertise Technique.....	18
Exploit.....	25, 61, 64, 65, 66
Fingerprint.....	60
Forensic.....	40, 41
FPGA.....	27
Fullstack.....	39
Fuzzing.....	61, 62, 63, 64, 65, 66, 67
Ghidra	25





MINISTÈRE DES ARMÉES

Liberté
Égalité
Fraternité



Hacking.....	60
Hadoop.....	58, 59
HIDS.....	17, 20, 41
Honeypot.....	20
Hyperviseur.....	28
IA.....	55, 57
Iceberg.....	58
ICS.....	14
IDA.....	25, 61, 62, 63, 64, 65
IDS.....	17, 41
Information.....	52, 54
Ingénierie.....	22
Investigation numérique.....	40
Investigations.....	50
IoC.....	21
iOS.....	35, 48
ISO 27001.....	12, 51
IT.....	12, 13
Java.....	34, 48, 58
KnowledgeGraph.....	53
Kotlin.....	34
L2I.....	55, 56, 57
LID.....	17, 41
LinkedData.....	53
Linux.....	20, 28, 31, 32, 33
Logiciel.....	44
MacOS.....	35
Menace.....	52
Modélisation.....	52, 54
NIDS.....	17, 20
NLP.....	55, 57
Nsx-T.....	30
ObjectiveC.....	35





OS.....	28
OSINT.....	55, 56, 57
POC.....	29
Post-quantique.....	24
Projet.....	16
Prometheus.....	59
Protocoles.....	24
Python.....	20, 33, 34, 35, 36, 38, 39, 48
Radiofréquence.....	46, 47
Radiologicielle.....	46, 47
Radio-Navigation.....	45
Réponse à incidents.....	13
Réseaux.....	38
RESTApi.....	39
Reverse.....	25, 61, 62, 63, 64, 65, 66
RF.....	46, 47
Risk Manager.....	51
ROP.....	61, 62, 63, 64, 65, 66, 67
RSSI.....	51
Rust.....	28, 48
Sandbox.....	20, 28
SCADA.....	12, 14
Scala.....	58
SCI.....	14
SDR.....	46, 47
Sécurité.....	14, 15, 26, 28, 29, 30
Sécurité des composants.....	27
Sécurité informatique.....	13
Serveurs.....	16, 30
SIEM.....	17, 20, 21, 41, 50
Snort.....	20
SOC.....	13, 17, 21, 29, 50
Spark.....	58, 59





MINISTÈRE DES ARMÉES

Liberté
Égalité
Fraternité



SPC.....	47
SSI	14, 15
Stockage.....	30
Supervision.....	30, 50
Suricata	20
Swift	35
Système d'exploitation.....	18
Système d'information	18
Systèmes embarqués.....	26, 27, 29
TEMPEST	47
Test.....	42
Traitement du signal	46
TTP	17, 41
VDI	32
vSphere	16, 30, 31
Vulnérabilités	14, 15, 28, 43, 44
Win2k19	32
Windows.....	20, 28, 36, 61, 64, 65, 66

