



INFRASTRUCTURE AND SERVICE DELIVERY DIVISION, Central Infrastructure Branch, Cyber Security Risk, Architecture and Special Projects Section

Senior Cyber Security Engineer

Grade: 17:A3

Post No.: IS-70

Original:	English		Clearance:	NATO SECRET
Date validated:	25 August 2026		Duty Location:	Capellen, LUX
Validated by:	J. Schimek		Job Code:	A622

SUMMARY

The incumbent reports to the Chief of Section and is responsible for performing major functions related to all aspects of Information Systems (IS) networks for the whole NSPA computing environment, ensuring that appropriate levels of availability and security are guaranteed in accordance with NATO and NSPA prescriptive documents, policies and procedures. More precisely, the incumbent is responsible for performing the following functions:

RESPONSIBILITIES

General Responsibilities

- Performing studies as assigned, to determine the cost/benefits and feasibility of developing/deploying improved Information Systems (IS), or rationalising existing systems in the area of Information and Communication Technologies (ICT) security.
- Designing, evaluating and implementing ICT security and network solutions in line with NATO security regulations to protect NSPA Information Systems against cyber threats, including feasibility studies, requirements analysis, specifications, user acceptance and review.
- Preparing written reports and describing the results of each study performed, with justified recommendations (i.e. developing a "business case") concerning ICT security for systems required as well as related support requirements.
- Preparing and planning the development/deployment of ICT security & network solutions, including feasibility studies, requirements analysis, specifications, user acceptance and review; actively participating in their planning and ensuring user satisfaction in the stages of testing, parallel operations, and deployment for user acceptance (project implementation plan).
- Executing project plans, including the monitoring/measuring of results against prescribed objectives, and ensuring that corrective action is taken as required.
- Conducting meetings with representatives to plan future activities, report progress and resolving problems, and to obtain approval for each stage of project development taking into account end-user change proposals as required.
- Writing Statements of Work (SOWs) and assisting in the technical administration and monitoring of contractor performance to ensure that contractual conditions are fulfilled, and proposing corrective actions where necessary.
- Overseeing management of assigned budgets in accordance with NSPA regulations.
- Performing other related functions as required in peacetime and any other appropriate functions assigned in times of crisis or war.
- In the event of crisis or war the incumbent will, subject to the agreement of their national authorities, remain in the service of the Agency.

Specific Responsibilities

- Collecting and analysing ICT security information to identify relevant threats and vulnerabilities
- Monitoring and analysing ICT security events from multiple sources to identify ICT security incidents.

- Performing in-depth technical analyses of ICT security threats and incidents.
- Managing ICT security incidents to ensure a coordinated, timely and effective response to security incidents.
- Performing network penetration testing.
- Analysing ICT security requirements of the various Information Systems in place or under development; designing, testing and implementing ICT security solutions directly or supervising the work of service providers.
- Specifying the ICT security system solution and system procedures and outlining the supporting manual procedures for later implementation by internal or external staff, as well as managing implementation.
- Ensuring that the knowledge of current ICT security tools and techniques is maintained and keeping up to date with state-of-the-art ICT security practices using all available means, including access to the Web, ICT security news groups, etc.
- Preparing documentation, liaising with CIS Security Senior Officer on Cyber security and also when applicable with the Site Security Section, NATO Office of Security and other NATO security elements and getting, if required, accreditation for the various ICT systems in place.
- Architecting, designing and implementing network, system and application security controls aligned with the cyber threat landscape.
- Analysing the Agency IT security risks and requirements, designing security architecture, designing and implementing IT solutions, overseeing vendor support and other security service contractors related to the Information Security Management System (ISMS), implementing IT hardware and software solutions, following up on designs, and maintaining and documenting Agency security controls and solutions.
- Ensuring the implementation of the risk management process and managing the risks raised in their area of responsibility in compliance with NSPA prescriptive documents on Risk Management.

QUALIFICATIONS

General Qualifications

- University degree in computer sciences with a specialisation in information security, equivalent education or relevant professional experience.
- Demonstrated organisational and project management abilities to successfully work as a member or leader of multi-national/multi-disciplinary teams (including consultants), dealing with complex, interrelated technical issues.
- Excellent analytical and financial/budget skills, which bridge the gap between technology and business.
- Very good analytical, writing, communication skills and the ability to conduct complex operational, compliance and performance assessments.
- Ability to maintain technological watch in order to propose continuous innovation.
- Understanding of the underlying concepts of IS/IT production.
- Sound digital literacy with experience in using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).

Specific Qualifications

- In-depth knowledge of ICT security and network concepts, policies and procedures, and large experience in developing, implementing, managing and maintaining ICT security and network.
- In-depth experience in designing, implementing and managing Firewall based architecture in a very compartmentalised network environment with Intrusion Prevention Systems (IPS); the knowledge of the Palo Alto® product would be an asset.
- Excellent understanding of complex and interrelated ICT security issues, including monitoring, troubleshooting and security incident/intrusion handling; the knowledge and use of a Security Information and Event Management (SIEM) product would be an asset (e.g. ArcSight, Splunk).
- Minimum five years of proven experience in the information systems security field; of which, minimum three years in a heterogeneous, complex environment with UNIX® systems, Windows servers and security appliances.

- Knowledge of digital forensics and malware analysis tools, techniques and procedures.
- Knowledge of the latest web technologies, including but not limited to: Hyper Text Markup Language (HTML), JavaScript, Extensible Markup Language (XML), Representational State Transfer (REST), Simple Object Access Protocol (SOAP) Application Programming Interface (API) and Progressive Web Apps (PWA).
- Proven practical experience establishing and configuring security controls for cloud infrastructure and Microsoft 365.
- Proven practical experience with container security.
- Proven practical experience with encryption technologies and key management.
- Broad technical background in the area of IT infrastructure and applications [including networking, Internet technology, security proxies for web, mail and file transfer, system analysis and design methods].
- Understanding of web and SAP application vulnerabilities and knowledge of common application security frameworks (e.g.: OWASP® Top 10, OWASP® Testing Guide).
- Proven experience in performing intrusion testing of web applications and identifying application security requirements and security controls.
- Knowledge of Public Key Infrastructure (PKI) concept and implementation, RSA and of authentication protocols [Kerberos, Security Assertion Mark-up Language (SAML), Single-Sign-On (SSO)].
- A recognised project management certification [e.g. PRINCE 2® Practitioner, Project Management Professional (PMP)].

LANGUAGE QUALIFICATIONS

- NATO's official languages are English and French. The work of this post requires fluency in English, while working knowledge of French is desirable.

DESIRABLE QUALIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Any vendor Architect certification (Microsoft SC100, Fortinet NSE7, etc)
- Any cloud vendor certification
- Information Technology Infrastructure Library (ITIL®) certification

PERSONAL CHARACTERISTICS

- All NSPA personnel are expected to conduct themselves in accordance with the current NATO Code of Conduct agreed by the North Atlantic Council (NAC), and thus display the core values of integrity, impartiality, loyalty, accountability, and professionalism.
- Honest, with positive "can-do" attitude and spirit of cooperation. Ability to empower teamwork toward established objectives.
- Passionate and motivated, equipped with strong communication skills, fostering an environment that encourages community involvement and engagement.
- Autonomy in delivering results and managing tasks in a fast-paced environment.
- Ability to develop resourceful and effective solutions to problems (including personnel), focus on team performance goals and track metrics to measure performance improvements.
- Displays emotional intelligence and self-control. Holds the capacity to remain calm in the face of adversity/conflict; identifies and works to remedy collaborative concerns in accordance with procedural guidelines.

ADDITIONAL INFORMATION

- The incumbent of this post will be required to work on-site, non-standard business hours, on weekends and national holidays to perform extended support and on-call duty. Using a communication device, they are expected to respond to off-hours incidents, on a team rotation basis.



DIVISION "INFRASTRUCTURE ET PRESTATION DE SERVICES", Branche "infrastructure centrale", Section "risques, architecture et projets spéciaux en matière de cybersécurité"

Ingénieur(e) principal(e) en cybersécurité

Grade : 17:A3

Poste n° : IS-70

Original :	Anglais		Habilitation :	NATO SECRET
Date de validation :	25 août 2026		Lieu d'affectation :	Capellen, LUX
Validé par :	J. Schimek		Code poste :	A622

RÉSUMÉ

Responsable envers le/la chef de section, le/la titulaire exerce des fonctions importantes liées à tous les aspects des réseaux des systèmes d'information de l'ensemble de l'environnement informatique de la NSPA, afin de veiller à garantir des niveaux de disponibilité et de sécurité appropriés conformément aux documents réglementaires, aux politiques générales et aux procédures de l'OTAN et de la NSPA. Il/Elle exerce plus précisément les fonctions suivantes :

RESPONSABILITÉS

Responsabilités générales

- réaliser les études qui lui sont confiées en vue de déterminer les coûts et avantages ainsi que la faisabilité du développement et de la mise en service de systèmes d'information améliorés ou de la rationalisation des systèmes existants dans le domaine de la sécurité des technologies de l'information et de la communication (TIC) ;
- concevoir, évaluer et mettre en œuvre des solutions en matière de sécurité des TIC et de réseau en conformité avec les règlements de sécurité de l'OTAN afin de protéger les systèmes d'information de la NSPA contre les cybermenaces, ce qui comprend la réalisation d'études de faisabilité, l'analyse des besoins, l'élaboration des spécifications ainsi que la réception et la revue par les utilisateurs ;
- rédiger des rapports et exposer les résultats de chaque étude effectuée, accompagnés de recommandations étayées par des justifications (élaborer un dossier justificatif) concernant la sécurité relative aux TIC des systèmes nécessaires et les besoins correspondants en matière de soutien ;
- préparer et planifier le développement et la mise en place de solutions en matière de sécurité des TIC et de réseau, ce qui comprend les études de faisabilité, l'analyse des besoins, l'élaboration de spécifications ainsi que la réception et la revue par les utilisateurs ; participer activement à la planification de ces activités et veiller à la satisfaction des utilisateurs aux stades des tests, du fonctionnement en parallèle et de la mise en place des systèmes en vue de leur réception par les utilisateurs (plan de mise en œuvre du projet) ;
- exécuter les plans relatifs aux projets, notamment en contrôlant et en mesurant les résultats obtenus par rapport aux objectifs définis, et veiller à ce que des mesures correctives soient prises en cas de nécessité ;
- mener des réunions avec divers représentants en vue de planifier les activités futures, de rendre compte de l'avancement des travaux, de résoudre les problèmes et d'obtenir l'approbation à chaque stade du développement du projet en tenant compte des modifications proposées par les utilisateurs finaux, selon les besoins ;
- rédiger des cahiers des charges, aider à assurer l'administration technique et le suivi des prestations des titulaires de marché afin de veiller au respect des conditions contractuelles et proposer des mesures correctives en fonction des besoins ;
- superviser la gestion des budgets qui lui sont confiés conformément aux règlements de la NSPA ;
- exercer d'autres fonctions connexes selon les besoins en temps de paix et toute autre fonction appropriée qui lui sera confiée en période de crise ou en temps de guerre.
- En cas de crise ou de guerre, le/la titulaire restera au service de l'Agence, sous réserve de l'accord de ses autorités nationales.

Responsabilités particulières

- recueillir et analyser des informations liées à la sécurité des TIC afin de détecter les menaces et les vulnérabilités à prendre en considération ;
- assurer le suivi d'événements de sécurité des TIC provenant de plusieurs sources et les analyser pour détecter les incidents de sécurité en la matière ;

- réaliser des analyses techniques approfondies des menaces et des incidents liés à la sécurité des TIC ;
- gérer les incidents de sécurité des TIC pour pouvoir réagir de façon coordonnée, rapide et efficace aux incidents de sécurité ;
- effectuer des tests de pénétration du réseau ;
- analyser les exigences en matière de sécurité des TIC pour les différents systèmes d'information en place ou en cours de développement ; concevoir, tester et mettre en œuvre des solutions de sécurité liées aux TIC directement ou en supervisant le travail de fournisseurs de services ;
- préciser le système à mettre en œuvre pour garantir la sécurité des TIC et les procédures applicables à ce système, exposer les procédures manuelles d'accompagnement qui seront ensuite mises en œuvre par des personnels internes ou externes, et gérer cette mise en œuvre ;
- veiller à entretenir la connaissance des techniques et outils de sécurité des TIC les plus récents ; suivre les pratiques de sécurité les plus avancées dans ce domaine en utilisant tous les moyens disponibles, dont le web et les groupes de discussion sur la sécurité des TIC ;
- élaborer de la documentation, assurer la liaison avec le/la responsable principal(e) de la sécurité des systèmes d'information et de communication au sujet de la cybersécurité et, s'il y a lieu, avec la Section "sécurité du site", le Bureau de sécurité de l'OTAN et d'autres services de l'OTAN chargés de la sécurité, et obtenir, en fonction des besoins, l'homologation des différents systèmes de TIC en place ;
- organiser, concevoir et mettre en œuvre des contrôles de sécurité portant sur les réseaux, les systèmes et les applications et qui soient adaptés au paysage de la cybermenace ;
- analyser les risques et les besoins de l'Agence en matière de sécurité informatique, assurer la conception de l'architecture de sécurité, concevoir et mettre en œuvre des solutions informatiques, superviser le soutien assuré par les fournisseurs et par d'autres prestataires de services de sécurité en rapport avec le système de management de la sécurité de l'information, mettre en œuvre des solutions informatiques (matériels et logiciels), assurer le suivi des travaux de conception ainsi qu'assurer la tenue à jour des solutions et des contrôles adoptés par l'Agence en matière de sécurité et tenir la documentation correspondante ;
- veiller à la mise en œuvre du processus de gestion des risques et gérer les risques signalés dans son domaine de responsabilité conformément aux documents réglementaires de la NSPA en matière de gestion des risques.

QUALIFICATIONS

Qualifications générales

- Diplôme d'études supérieures en informatique avec une spécialisation dans le domaine de la sécurité de l'information, formation équivalente ou expérience professionnelle pertinente.
- Compétences confirmées dans le domaine de l'organisation et de la gestion de projet, permettant de travailler de manière efficace en tant que membre ou chef d'équipes multinationales et pluridisciplinaires (qui peuvent inclure des consultants) traitant de questions techniques complexes et interdépendantes.
- Excellentes aptitudes en matière d'analyse de questions financières et budgétaires, assurant le lien entre la technologie et l'activité de l'Agence.
- Très bonnes compétences en matière d'analyse, de rédaction et de communication ainsi qu'aptitude à mener des évaluations complexes dans les domaines opérationnels, de la conformité et de la performance.
- Aptitude à assurer une veille technologique afin de proposer des innovations de façon continue.
- Compréhension des concepts sous-tendant la production informatique.
- Solide maîtrise des outils numériques assortie d'une expérience de l'utilisation des systèmes et des logiciels de bureautique [p. ex. la suite Microsoft Office (Word, Excel et PowerPoint)].

Qualifications particulières

- Connaissance approfondie des concepts, politiques et procédures en matière de réseaux et de sécurité des TIC et vaste expérience du développement, de la mise en œuvre, de la gestion et de la tenue à jour des réseaux et de la sécurité des TIC.
- Expérience approfondie de la conception, de la mise en œuvre et de la gestion des architectures comportant des enceintes de sécurité dans un environnement en réseau très compartimenté doté de systèmes de prévention des intrusions ; la connaissance de produits Palo Alto® constituerait un atout.
- Excellente compréhension des questions de sécurité des TIC complexes et interdépendantes, ce qui comprend le suivi, le dépannage et le traitement des incidents et des intrusions compromettant la sécurité ; la connaissance théorique et pratique d'un produit de gestion des informations et des événements de sécurité (SIEM) constituerait un atout (p. ex. ArcSight, Splunk).
- Au moins cinq années d'expérience confirmée dans le domaine de la sécurité des systèmes d'information, dont au moins trois dans un environnement hétérogène et complexe comportant des systèmes UNIX®, des serveurs Windows et des dispositifs de sécurité.

- Connaissance de la criminalistique numérique et des outils, techniques et procédures d'analyse des logiciels malveillants.
- Connaissance des dernières technologies web, notamment (mais pas exclusivement) : langage de balisage hypertexte (HTML), JavaScript, langage extensible de balisage (XML), architecture REST (*Representational State Transfer*), protocole SOAP (*Simple Object Access Protocol*), interface de programmation d'application (API) et applications web progressives (PWA).
- Expérience confirmée de la mise en place et de la configuration de contrôles de sécurité pour les infrastructures en nuage ("cloud") et Microsoft 365.
- Expérience confirmée de la sécurité des conteneurs.
- Expérience confirmée des technologies de chiffrement et de la gestion de clés.
- Expérience technique étendue dans les domaines de l'infrastructure et des applications informatiques [dont les réseaux, la technologie Internet, les serveurs mandataires (proxies) pour Internet, le transfert de courrier électronique et de fichiers et les méthodes d'analyse et de conception des systèmes].
- Compréhension des vulnérabilités des applications web et SAP et connaissance des cadres courants de sécurité des applications (p. ex. OWASP® Top 10, OWASP® Testing Guide).
- Expérience démontrée de la réalisation de tests d'intrusion d'applications web et de l'identification d'exigences et de contrôles de sécurité pour les applications.
- Connaissance du concept d'infrastructure à clés publiques et de sa mise en œuvre, du chiffrement RSA et des protocoles d'authentification [Kerberos, SAML (*Security Assertion Mark-up Language*), SSO (*Single-Sign-On*)].
- Certification reconnue en gestion de projet [p. ex. PRINCE2® Practitioner ou Project Management Professional (PMP)].

CONNAISSANCES LINGUISTIQUES

- Les langues officielles de l'OTAN sont l'anglais et le français. Une bonne maîtrise de l'anglais est nécessaire pour le travail effectué à ce poste, et une connaissance pratique du français est souhaitable.

QUALIFICATIONS SOUHAITABLES

- Certificat de professionnel certifié de la sécurité des systèmes d'information (CISSP).
- Certification en tant qu'architecte de tout fournisseur (Microsoft SC100, Fortinet NSE7, etc.).
- Certification de tout fournisseur de "cloud".
- Certification ITIL® (bibliothèque pour l'infrastructure des technologies de l'information).

QUALITÉS PERSONNELLES

- Il est attendu de tous les membres du personnel de la NSPA qu'ils se comportent conformément au texte en vigueur du Code de conduite de l'OTAN adopté par le Conseil de l'Atlantique Nord et qu'en conséquence, ils incarnent les valeurs fondamentales que sont l'intégrité, l'impartialité, la loyauté, le sens des responsabilités et le professionnalisme.
- Honnêteté, attitude positive et volontaire, et esprit de coopération. Capacité à valoriser le travail d'équipe dans le but de réaliser les objectifs fixés.
- Passion et motivation alliées à une solide aptitude à communiquer, capacité à promouvoir un climat de travail favorisant la participation ainsi que l'engagement des parties prenantes.
- Capacité à atteindre des résultats et à gérer des tâches de manière autonome dans un environnement caractérisé par un rythme de travail rapide.
- Aptitude à mettre au point des solutions ingénieuses et efficaces aux problèmes (notamment en ce qui concerne le personnel), à se concentrer sur les résultats visés par l'équipe et à suivre les indicateurs afin de mesurer l'évolution des prestations.
- Intelligence émotionnelle et maîtrise de soi. Capacité à garder son calme face à l'adversité ou dans des situations conflictuelles. Aptitude à détecter les difficultés liées au travail en commun et à œuvrer pour y remédier conformément aux procédures.

INFORMATIONS COMPLÉMENTAIRES

- Le/La titulaire de ce poste devra travailler sur site en dehors des heures de bureau ainsi que les week-ends et les jours fériés, afin d'assurer un soutien étendu et un service d'astreinte. En étant joignable via un dispositif de communication, il/elle devra intervenir en cas d'incident survenant en dehors des heures de travail normales, conformément à un programme de rotation d'équipes.