MINISTÈRE
DU TRAVAIL,
DU PLEIN EMPLOI
ET DE L'INSERTION
Liberté
Égalité
Fraternité

REFERENTIEL EMPLOI ACTIVITES COMPETENCES

DU TITRE PROFESSIONNEL

Administrateur d'infrastructures sécurisées

Niveau 6

Site : http://travail-emploi.gouv.fr

SOMMAIRE

Pages

Introduction

Présentation de l'évolution du titre professionnel

La version 2023 du titre professionnel « Administrateur d'infrastructures sécurisées » présente trois blocs de compétences, dont la configuration diffère de la version précédente, afin de tenir compte des évolutions de l'emploi :
- «Administrer et sécuriser les infrastructures»
- «Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution»
- «Participer à la gestion de la cybersécurité»

Contexte de l'examen du titre professionnel

L'analyse de l'emploi menée en 2022 montre que les fondamentaux du métier sont restés stables, l'administrateur d'infrastructures sécurisées réalise les tâches d'administrations qui ont pour objectifs de maintenir en condition opérationnelles et en condition de sécurité les infrastructures du système d'information. Il est également sollicité pour la conception et la mise en œuvre d'évolution des infrastructures.
Les activités d'administration et de conception sont clairement différentiées dans l'exercice du métier. Ce constat a donné lieu à une répartition des tâches d'administration et de conception dans deux blocs distincts:
-"Administrer et sécuriser les infrastructures"
-"Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution"
L'importance de la communication dans l'exercice de l'emploi est confirmée. L'administrateur est à l'écoute des clients et des responsables et il échange avec l'ensemble des acteurs du système d'information. Il est en mesure de proposer et d'argumenter des solutions en réponse à des besoins d'évolution auprès des décideurs. Il communique oralement et par écrit, en français et en anglais, et il adapte sa communication à ses différents interlocuteurs et contextes professionnels. C'est dans la compétences transversale intitulée "communiquer en francais et en anglais" que desormais la description et les critères de performance liés à la communication sont regroupés. La compétence intitulée "concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure" met également l'accent sur la présentation et l'argumentation d'une solution.
Deux éléments ont impactés l'exercice de l'emploi. Depuis 2018, date de la création du titre d'administrateur d'infrastructures sécurisées, les équipes en charge des systèmes d'informations n'ont cessé d'accroitre leurs recours aux services cloud, comme les logiciels en tant que services (Software as a service SaaS), les plateformes en tant que services (Plateform as a service PaaS) ou encore les infrastructures en tant que services (Infrastrucutre as a service IaaS). Cela a conduit à réduire les différences entre les taches d'administration locales et Cloud. Dans ce contexte l'administration des infrastructures virtuelles locales et Cloud ont été regroupées dans la compétence intitulée "Administrer et sécuriser les infrastructures virtualisées".
Une autre tendance importante est l'augmentation significative des risques cyber ces dernières années, qui a poussé les directions des systèmes d'information (DSI) à mettre en place des mesures de protection appropriées et à former le personnel aux bonnes pratiques en matière de sécurité numérique. Les administrateurs d'infrastructures sécurisées jouent un rôle clé dans la sécurisation des infrastructures du système d'information. Ils mettent en œuvre les aspects opérationnels de la politique de sécurité du système d'information, ils participent à l'analyse du niveau de sécurité et à la détection et au traitement des incidents de sécurité.
Ces compétences sont désormais regroupées dans une activité intitulée "Participer à la gestion de la cybersécurité"

Liste des activités

Ancien TP : Administrateur d'infrastructures sécurisées
Activités :

- Administrer et sécuriser les composants constituant l'infrastructure
- Intégrer, administrer et sécuriser une infrastructure distribuée
- Faire évoluer et optimiser l'infrastructure et son niveau de sécurité

Nouveau TP : Administrateur d'infrastructures sécurisées
Activités :
- Administrer et sécuriser les infrastructures
- Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution
- Participer à la gestion de la cybersécurité

Vue synoptique de l'emploi-type

N° Fiche AT	Activités types	N° Fiche CP	Compétences professionnelles
1	Administrer et sécuriser les infrastructures	1	Appliquer les bonnes pratiques dans l'administration des infrastructures
		2	Administrer et sécuriser les infrastructures réseaux
		3	Administrer et sécuriser les infrastructures systèmes
		4	Administrer et sécuriser les infrastructures virtualisées
2	Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution	5	Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
		6	Mettre en production des évolutions de l'infrastructure
		7	Mettre en œuvre et optimiser la supervision des infrastructures
3	Participer à la gestion de la cybersécurité	8	Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
		9	Participer à l'élaboration et à la mise en œuvre de la politique de sécurité
		10	Participer à la détection et au traitement des incidents de sécurité

FICHE EMPLOI TYPE

Administrateur d'infrastructures sécurisées

Définition de l'emploi type et des conditions d'exercice

L'administrateur d'infrastructures sécurisées (AIS) met en œuvre, administre et sécurise les infrastructures informatiques locales et dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution. Il implémente et optimise les dispositifs de supervision.
Il participe à la gestion de la cybersécurité en analysant les menaces et en mettant en place des mesures de sécurité et de réaction en cas d'incident.
L'administrateur d'infrastructures sécurisées met en œuvre, administre et sécurise les éléments actifs des réseaux, les serveurs, les services d'infrastructure et les plateformes de virtualisation situées dans les locaux de son entreprise ou dans des datacenters ainsi que les ressources et services de cloud public. Il effectue le suivi des tâches de maintenance et fournit un support de niveau 2 et 3 pour résoudre les incidents et les problèmes.
Il conçoit des solutions techniques pour répondre aux besoins d'évolution des infrastrucutures. Il définit les critères d'évaluation et met en place un environnement de test pour valider une solution, puis présente le dispositif choisi aux décideurs. Il planifie et implémente l'intégration de la solution dans l'environnement de production, en vérifiant que les plans de reprise et de continuité informatique (PRI, PCI) associés sont testés et validés. Il met en œuvre les outils de supervision, choisit les indicateurs et évènements associés et définit les tableaux de suivi des niveaux de performance et de disponibilité des infrastructures.
L'administrateur d'infrastructures sécurisées protège les infrastructures de l'entreprise contre les menaces informatiques. Il analyse les risques, identifie les vulnérabilités et effectue des audits de sécurité en interne. Il participe au choix et à la mise en place de solutions de sécurisation. Il sensibilise les utilisateurs et contribue à la formation des équipes d'exploitation en matière de cybersécurité. Il met en place et utilise des dispositifs de détection d'événements de sécurité et applique les mesures de réaction appropriées en cas d'incident. Il reste vigilant sur les nouvelles menaces et vulnérabilités et adapte les règles de détection et de gestion des incidents en conséquence.
Dans l'ensemble de ses activités il communique par écrit et à l'oral et adapte son expression à son interlocuteur.
De nombreuses sources d'informations techniques, forums et services support étant en anglais l'emploi requiert le niveau B1 pour la compréhension et l'expression écrite du cadre européen commun de référence pour les langues (CECRL).
L'autonomie et les responsabilités de l'administrateur d'infrastructures sécurisées peuvent varier selon l'organisation et l'environnement dans lesquels il travaille. Cependant, en général, il est responsable du maintien en condition opérationnelle (MCO) et du maintien en condition de sécurité (MCS) d'infrastructures systèmes ou réseau. Il prend des décisions dans les limites de sa délégation et de son périmètre de responsabilité. Il travaille en respectant les normes et les politiques de sécurité de l'entreprise. Le plus souvent, l'administrateur d'infrastructure sécurisée fait partie d'une équipe et il peut piloter les interventions des techniciens informatiques.
L'administrateur d'infrastructures sécurisées peut avoir comme interlocuteurs : le directeur et le responsable du système d'information (DSI, RSI), le responsable de la sécurité du système d'information (RSSI), les chefs de projets, les experts et acteurs de la cybersécurité, les techniciens, les utilisateurs, les clients, les prestataires et fournisseurs de services, de matériels et de logiciels.

Il travaille dans des entreprises de taille intermédiaire, des grandes entreprises, des collectivités et administrations ou des entreprises de services numériques. Les conditions d'exercice du métier, son champ d'intervention et son niveau de responsabilité varient en fonction de l'organisation de l'entreprise. L'emploi peut nécessiter le maintien d'une position statique assise prolongée devant des écrans, des horaires décalés et des astreintes.

Secteurs d'activité et types d'emplois accessibles par le détenteur du titre

Les différents secteurs d'activités concernés sont principalement :
Entreprise de services numériques (ESN).
Toutes les organisations ou entreprises utilisatrices de taille intermédiaire et plus du secteur privé ou public.

Les types d'emplois accessibles sont les suivants :
Administrateur systèmes et réseaux (et sécurité).
Administrateur systèmes (et sécurité).
Administrateur réseaux (et sécurité)
Administrateur infrastructures.
Administrateur d'infrastructures et cloud
Administrateur cybersécurité
Responsable infrastructure systèmes et réseaux

Réglementation d'activités (le cas échéant)

Néant

Equivalences avec d'autres certifications (le cas échéant)

Sans objet

Liste des activités types et des compétences professionnelles

1. Administrer et sécuriser les infrastructures
Appliquer les bonnes pratiques dans l'administration des infrastructures
Administrer et sécuriser les infrastructures réseaux
Administrer et sécuriser les infrastructures systèmes
Administrer et sécuriser les infrastructures virtualisées

2. Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution
Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
Mettre en production des évolutions de l'infrastructure
Mettre en œuvre et optimiser la supervision des infrastructures

3. Participer à la gestion de la cybersécurité
Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
Participer à l'élaboration et à la mise en œuvre de la politique de sécurité
Participer à la détection et au traitement des incidents de sécurité

Compétences transversales de l'emploi

Communiquer en français et en anglais
Apprendre en continu

Niveau et/ou domaine d'activité

Niveau 6 (Cadre national des certifications 2019)
Convention(s) :
Code(s) NSF :
326--Informatique, traitement de l'information, réseaux de transmission (niv100)

Fiche(s) Rome de rattachement

M1802 Expertise et support en systèmes d'information
M1801 Administration de systèmes d'information
M1810 Production et exploitation de systèmes d'information

FICHE ACTIVITÉ TYPE N° 1

Administrer et sécuriser les infrastructures

Définition, description de l'activité type et conditions d'exercice

L'administrateur d'infrastructures sécurisées administre et sécurise l'infrastructure du système d'information sur site et dans le cloud, en respectant les bonnes pratiques et en veillant à la maintenir en condition opérationnelle selon les niveaux de service (disponibilité, performances, sécurité) contractualisés. Cette activité inclut la gestion des réseaux, des systèmes et des environnements de virtualisation.

L'administrateur d'infrastructures sécurisées administre et sécurise :
-Les éléments actifs des réseaux tels que les commutateurs, les routeurs ou points d'accès ainsi que les dispositifs de sécurité de type pare-feu, passerelle VPN, systèmes de prévention ou de détection d'intrusion;
- Les serveurs sous Windows, Linux ou Unix et les services d'infrastructure;
- Les infrastructures de virtualisation basées sur des hyperviseurs, des dispositifs de stockage et de mise en réseau situés localement ou dans des datacenters mtualisés;
- Les ressources et les services de type Infrastructure as a Service (IaaS), Platform as a Service (PaaS) et Software as a Service (Saas) fournis par les opérateurs de cloud public.
Il effectue l'ensemble des opérations dans le respect des bonnes pratiques et maintient en condition opérationnelle les éléments de l'infrastructure. Pour cela il vérifie que les dispositifs de reprise et de continuité informatique sont opérationnels, il planifie et documente les tâches d'exploitation de type sauvegardes, archivages, tests de restauration, mises à jour. Il assure le support de niveau 2 et 3 en participant au diagnostic et à la résolution des incidents et des problèmes sur les infrastructures. Il assure leur supervision et contrôle les niveaux de performance et de disponibilité des services.
L'administrateur d'infrastructures sécurisées travaille dans le respect des accords de niveaux de service (Service Level Agreement-SLA), et prend en compte les engagements contractuels avec les fournisseurs et prestataires.
Il respecte les recommandations émises par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il prend en compte les référentiels et réglementations tels que le règlement général sur la protection des données (RGPD), le référentiel général d'amélioration de l'accessibilité (RGAA) et les bonnes pratiques d'éco-conception et de sobriété énergétique.
L'activité a pour périmètre l'infrastructure constituée à la fois d'éléments internes à l'entreprise et de ressources externes (SaaS, PaaS, IaaS) hébergées dans le cloud.

L'exercice de l'activité peut nécessiter de travailler en horaires décalés et en astreintes.

L'administrateur d'infrastructures sécurisées prend des décisions dans les limites de sa délégation et de son périmètre de responsabilité et peut piloter les interventions de techniciens informatiques.

L'exercice de l'activité requiert le niveau B1 pour la compréhension et l'expression écrite du cadre européen commun de référence pour les langues (CECRL).

L'administrateur d'infrastructures sécurisées a comme interlocuteurs le directeur et le responsable du système d'information (DSI, RSI), le responsable de la sécurité du système d'information (RSSI), les autres administrateurs, les techniciens, les utilisateurs, les experts techniques, les opérateurs de télécoms, les constructeurs, les éditeurs et leurs distributeurs, ainsi que les fournisseurs de services dans le cloud.

Réglementation d'activités (le cas échéant)

Sans objet

Liste des compétences professionnelles de l'activité type

Appliquer les bonnes pratiques dans l'administration des infrastructures
Administrer et sécuriser les infrastructures réseaux
Administrer et sécuriser les infrastructures systèmes
Administrer et sécuriser les infrastructures virtualisées

Compétences transversales de l'activité type

Communiquer
Apprendre en continu

FICHE ACTIVITÉ TYPE N° 2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

Définition, description de l'activité type et conditions d'exercice

L'administrateur d'infrastructures sécurisées conçoit et met en production des solutions techniques répondant à des besoins d'évolution de l'infrastructure. Il implémente et optimise les dispositifs de supervision.

L'administrateur d'infrastructures sécurisées effectue des recherches afin de concevoir une solution technique répondant à un besoin d'évolution de l'infrastructure. Il définit les critères permettant d'évaluer la solution et met en place un environnement de test pour la valider. Il rédige une proposition argumentée du dispositif choisi et la présente aux décideurs.
Il planifie, implémente et valide l'intégration d'une solution dans l'environnement de production.
Il teste et valide les plans de reprise et de continuité informatique (PRI, PCI) associés aux dispositifs mis en production. Il effectue le transfert de compétences et met à jour les documents d'exploitation.
Il met en œuvre les outils de supervision, choisit les indicateurs et les évènements associés et met à disposition des équipes d'exploitation les tableaux de bord de suivis des niveaux de performances et de disponibilité.
Il respecte les recommandations émises par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il prend en compte les référentiels et réglementations telles que le règlement général sur la protection des données (RGPD), le référentiel général d'amélioration de l'accessibilité (RGAA) et les bonnes pratiques d'éco-conception et de sobriété énergétique.
L'administrateur travaille à partir d'un cahier des charges afin d'analyser les besoins et identifier les contraintes. Il dispose des accords de niveaux de services correspondant à la demande de changement, de la politique de sécurité du système d'information de l'entreprise et des réglementations en vigueur.
Il peut utiliser un outil de gestion de projet pour planifier les tâches et leurs affecter les ressources.

L'administrateur peut exercer cette activité à plein temps ou en temps partagé avec les tâches d'administration courantes.
Certaines parties de son activité peuvent l'amener à travailler en horaires décalés ou ponctuellement hors des périodes ouvrées de l'entreprise pour laquelle il exerce.
L'administrateur peut être intégré dans une équipe projet ou travailler sous le contrôle de son responsable et peut piloter les interventions de techniciens informatiques.
Il prend des décisions dans les limites de sa délégation et de son périmètre de responsabilité.
L'exercice de l'activité requiert le niveau B1 pour la compréhension et l'expression écrite du cadre européen commun de référence pour les langues (CECRL).

L'administrateur d'infrastructures sécurisées a pour interlocuteurs dans l'exercice de cette activité : le directeur et le responsable du système d'information (DSI, RSI), le responsable de la sécurité du système d'information (RSSI), le chef de projet et les membres de l'équipe, les techniciens, les utilisateurs, les clients, les experts techniques, les opérateurs de télécoms, les constructeurs, les éditeurs et leurs distributeurs, ainsi que les fournisseurs de services dans le cloud.

Réglementation d'activités (le cas échéant)

Liste des compétences professionnelles de l'activité type

Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
Mettre en production des évolutions de l'infrastructure
Mettre en œuvre et optimiser la supervision des infrastructures

Compétences transversales de l'activité type

Communiquer
Apprendre en continu

FICHE ACTIVITÉ TYPE N° 3

Participer à la gestion de la cybersécurité

Définition, description de l'activité type et conditions d'exercice

L'administrateur d'infrastructures sécurisées analyse le niveau de sécurité des infrastructures et met en place des mesures pour renforcer leur sécurité. Il analyse en temps réel les menaces et applique les mesures de réaction en réponse à un incident.

L'administrateur d'infrastructures sécurisées participe à l'analyse des risques et identifie les menaces qui peuvent affecter les infrastructures. Il audite et évalue le niveau de sécurité des éléments de l'infrastructure qui sont de sa responsabilité et rédige un rapport présentant la méthode d'analyse et les vulnérabilités identifiées.
Il participe à la rédaction de la lettre de mission destinée à la réalisation d'un audit de sécurité par une entreprise tierce. Il évalue le rapport d'audit produit.
Il participe aux choix des solutions de sécurisation et les met en œuvre. Il crée et rédige les procédures permettant la déclinaison opérationnelle de la politique de sécurité su système d'information (PSSI).
L'administrateur d'infrastructures sécurisées sensibilise les utilisateurs aux bonnes pratiques de sécurité informatique et participe à la montée en compétences dans le champ de la cybersécurité des équipes d'exploitation.
Il met en œuvre et exploite un dispositif de détection d'évènements de sécurité et il applique les mesures de réaction en réponse à un incident. À la suite d'un incident majeur il participe à la réalisation d'un retour d'expérience.
L'administrateur assure une veille technologique sur les menaces et les vulnérabilités des infrastructures informatiques afin d'adapter les règles de détection et de traitement des incidents.
Il respecte les recommandations émises par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il prend en compte les référentiels et réglementations telles que le règlement général sur la protection des données (RGPD), le référentiel général d'amélioration de l'accessibilité (RGAA) et les bonnes pratiques d'éco-conception et de sobriété énergétique.

Dans l'exercice de ses fonctions, l'administrateur utilise le document de la PSSI pour guider ses actions. Il utilise des outils pour identifier les vulnérabilités, détecter les menaces et réagir de manière adaptée.
Cette activité peut être réalisée à plein temps si l'administrateur est intégré à une équipe en charge de la sécurité ou en temps partagé avec ses tâches d'administration.
L'exercice de l'activité peut nécessiter de travailler en horaires décalés et en astreinte.
L'exercice de l'activité requiert le niveau B1 pour la compréhension et l'expression écrite du cadre européen commun de référence pour les langues (CECRL).
Il a pour interlocuteurs dans l'exercice de cette activité : le directeur et le responsable du système d'information (DSI, RSI), le responsable de la sécurité du système d'information (RSSI), les experts réponse à incident, les analystes cyber, les consultants cyber, les prestataires d'audit de la sécurité des systèmes d'information (PASSI), les techniciens, les utilisateurs, les experts techniques, les prestataires et fournisseurs.

Réglementation d'activités (le cas échéant)

Sans objet

Liste des compétences professionnelles de l'activité type

Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure

Participer à l'élaboration et à la mise en œuvre de la politique de sécurité
Participer à la détection et au traitement des incidents de sécurité

Compétences transversales de l'activité type

Communiquer
Apprendre en continu

FICHE COMPÉTENCE PROFESSIONNELLE N° 1

Appliquer les bonnes pratiques dans l'administration des infrastructures

Description de la compétence – processus de mise en œuvre

À partir du signalement de la dégradation d'un service issu d'un processus d'escalade ou de la supervision, identifier, classifier, et enregistrer un incident, le diagnostiquer et le résoudre afin de rétablir le service fourni au niveau attendu.
À partir des informations d'exploitation ou des éléments fournis par la supervision, établir, planifier et réaliser les tâches préventives de type mise à jour, sauvegarde, vérification des dispositifs de reprise et de continuité informatique, remplacement ou paramétrage d'un élément de configuration, afin de maintenir le niveau de service de l'infrastructure du système d'information à la valeur attendue.
À partir des informations d'exploitations rédiger une procédure dans le respect des bonnes pratiques afin de répondre à un besoin de production ou de résolution de problème.
À l'issue d'une intervention, documenter les actions et changements de configuration dans un outil de suivi afin d'être à même de fournir une information actualisée sur les éléments de l'infrastructure.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur mobilise cette compétence dans le cadre du traitement de niveau 2 ou 3 d'incidents standards, de problèmes et d'incidents majeurs ou dans le cadre d'activités planifiées ou de maintenance préventive. Il peut être amené dans l'exercice de cette compétence à échanger avec des intervenants internes ou externes.

Critères de performance

Les problèmes et incidents sont résolus
Les taches planifiées pour le maintien en condition opérationnelle des infrastructures sont réalisées dans le respect des bonnes pratiques.
Le niveau de qualité des services est maintenu à la valeur attendue
Les procédures établies sont conformes aux règles de bonne pratique
Les interventions et changements de configuration ainsi que les tâches planifiées pour le maintien en condition opérationnelle des infrastructures sont documentées dans un outil de suivi.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Utiliser un outil de gestion des actifs et des configurations de type GLPI
Exploiter les données d'un outil de gestion des incidents de type GLPI
Vérifier que la qualité de service mesurée correspond aux accords de niveaux de services (SLA)
Exploiter les informations fournies par un système de supervision
Mettre en œuvre une démarche structurée de diagnostic
Établir une procédure de traitement d'incident ou d'exploitation

Planifier et organiser les interventions d'administration et de MCO sur les infrastructures.

Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des principes généraux des normes et bonnes pratiques de la gestion des services (type iso 20000, ITIL, ITSM)

FICHE COMPÉTENCE PROFESSIONNELLE N° 2

Administrer et sécuriser les infrastructures réseaux

Description de la compétence – processus de mise en œuvre

À partir des demandes d'interventions et des informations d'exploitation ou de supervision, administrer et sécuriser, en appliquant les bonnes pratiques, les éléments des infrastructures réseaux afin de les maintenir en condition opérationnelle dans le respect des accords de niveau de service, des règles de sécurité et de la réglementation en vigueur.
Afin de s'adapter aux différents environnements techniques ou dans une démarche de résolution de problèmes, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur intervient sur les éléments virtuels ou physiques de l'infrastructure réseaux qui sont hébergés en local ou dans le Cloud.
Il travaille avec les fournisseurs dans le cadre de l'exploitation des services et des accès réseaux.
Il peut travailler en équipe et piloter des techniciens informatiques. Il collabore avec les différents acteurs du système d'information.

Critères de performance

L'infrastructure réseau est opérationnelle conformément aux accords de niveau de service.
Les tâches sont réalisées dans le respect des bonnes pratiques.
Les règles de sécurité sont appliquées.
La règlementation en vigueur est respectée.
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Réaliser un diagnostic et apporter une solution curative à un dysfonctionnement au niveau 2 et plus sur une infrastructure réseau.
Administrer et sécuriser des commutateurs de niveau 2 et 3 et des routeurs en mettant en œuvre les technologies de type vlan, redondance et agrégat de liens, sécurité des accès, routage statique et dynamique, monitoring.
Administrer et sécuriser les réseaux sans fil.
Administrer les dispositifs de sécurisation des accès réseaux de type pare feu, proxy, portail captif, bastion.
Administrer et sécuriser des solutions de prévention et détection d'intrusion (IPS, IDS)
Administrer les dispositifs réseaux en haute disponibilité utilisant des technologies de type HSRP, STP, agrégat de lien.
Administrer et sécuriser les accès distants des utilisateurs nomades et les connexions inter sites de type VPN
Administrer et sécuriser les accès au réseau des périphériques mobiles de type BYOD conformément à la politique de sécurité.
Adapter le plan d'adressage réseau aux besoins d'administration du MCO.
Configurer et contrôler la qualité de service au niveau des flux réseau (QoS).
Évaluer les performances du réseau : taux de disponibilité, temps de réponse, évolution des flux.
Utiliser un outil de gestion centralisé des équipements réseaux
Créer et faire évoluer la documentation technique et les procédures d'exploitation.

Appliquer les recommandations de l'ANSSI en matière de sécurité réseau.
Appliquer la politique de sécurité du système d'information de l'entreprise.
Tester les procédures des plans de reprises et de continuité informatique (PRI, PCI) associés aux infrastructures réseaux.
S'assurer du respect des SLA par les fournisseurs.
Prendre en compte la réglementation concernant les accès au réseau Internet. (Filtrage sites illégaux, gestion des journaux...)

Collaborer avec les différents acteurs de la direction des systèmes d'information.
Communiquer de façon adaptée à l'écrit et à l'oral, avec les clients ou les différents acteurs du système d'information.
Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des objectifs et des usages des plans de reprise et de continuité d'activité et informatique (PRA, PCA, PRI, PCI).
Connaissance des caractéristiques et limites techniques des équipements réseaux.
Connaissance des principales technologies et des normes utilisées dans les réseaux convergents (voix, données, images)
Connaissance des risques et principales menaces sur les infrastructures réseau, et des moyens de protection associés
Connaissance des solutions d'interconnexion proposées par les opérateurs

FICHE COMPÉTENCE PROFESSIONNELLE N° 3

Administrer et sécuriser les infrastructures systèmes

Description de la compétence – processus de mise en œuvre

À partir des demandes d'interventions et des informations d'exploitation ou de supervision, administrer et sécuriser, en appliquant les bonnes pratiques, les infrastructures systèmes afin de les maintenir en condition opérationnelle dans le respect des accords de niveau de service, des règles de sécurité et de la réglementation en vigueur.
Afin de s'adapter aux différents environnements techniques ou dans une démarche de résolution de problèmes, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur intervient sur des systèmes qui sont hébergés en local ou dans le Cloud.
Il travaille avec les fournisseurs dans le cadre de l'exploitation des systèmes hébergés dans le cloud.
Il peut travailler en équipe et piloter des techniciens. Il collabore avec les différents acteurs du système d'information.

Critères de performance

L'infrastructure système est opérationnelle conformément aux accords de niveau de service.
Les tâches sont réalisées dans le respect des bonnes pratiques.
Les règles de sécurité sont appliquées
La règlementation en vigueur est respectée
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Réaliser un diagnostic et apporter une solution curative à un dysfonctionnement sur les systèmes au niveau 2 et plus.
Administrer et sécuriser un système d'exploitation serveur (Windows, Linux, Unix)
Administrer et sécuriser les services réseaux type DNS, DHCP, certificats
Administrer et sécuriser les services de type bureau à distance de Microsoft
Administrer et sécuriser un annuaire de réseau de type LDAP, Active Directory (AD), Azure AD,
Administrer et sécuriser la synchronisation d'annuaires dans un modèle de cloud hybride.
Administrer et sécuriser une solution Saas de type MS 365 ou Google Workspace
Administrer et sécuriser les outils et les ressources d'accessibilité à destination des personnes en situation de handicap.
Administrer et sécuriser les échanges entre systèmes hétérogènes en utilisant des protocoles de type SSH, SFTP, IPsec, TLS, SMB chiffré
Administrer des systèmes d'authentification forte de type Multifactor Authentication (MFA), One Time Password (OTP)
Administrer et sécuriser une infrastructure à clés publiques (PKI)
Automatiser et planifier une tâche d'administration par script basé sur un langage type Python, PowerShell, Bash.
Administrer et sécuriser une solution de gestion des mises à jour systèmes
Administrer et sécuriser une solution de sauvegarde de type Veritas Backup Exec, VEEAM.
Analyser et exploiter les évènements systèmes à partir de la supervision et des journaux
Évaluer les performances des systèmes : taux de disponibilité, charges de calcul, temps de réponse, etc.

Créer et faire évoluer la documentation technique et les procédures d'exploitation.
Appliquer les recommandations de l'ANSSI dans le domaine des systèmes.
Appliquer la politique de sécurité du système d'information de l'entreprise.
Tester et valider les procédures des plans de reprises et de continuité informatique (PRI, PCI) associés aux infrastructures systèmes et applicatives.
Prendre en compte le Règlement général sur la protection des données (RGPD)
Prendre en compte la règlementation relative à l'accessibilité du Référentiel général d'amélioration de l'accessibilité (RGAA)
Prendre en compte les bonnes pratiques d'éco-conception et de sobriété énergétique
S'assurer du respect des SLA par les fournisseurs.

Collaborer avec les différents acteurs de la direction des systèmes d'information.
Communiquer de façon adaptée à l'écrit et à l'oral, avec les clients ou les différents acteurs du système d'information.
Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
Connaissance des spécificités de chaque environnement système
Connaissance des dispositifs relatifs aux accès sécurisés (authentification multi facteur, OTP, web application firewall (WAF), modèle Zero trust, SASE)
Connaissance des principes d'une infrastructure à clés publiques (PKI)
Connaissance des règles de gestion relatives aux licences systèmes et logicielles

FICHE COMPÉTENCE PROFESSIONNELLE N° 4

Administrer et sécuriser les infrastructures virtualisées

Description de la compétence – processus de mise en œuvre

À partir des demandes de services et des informations d'exploitation ou de supervision, administrer et sécuriser, en appliquant les bonnes pratiques, les éléments de l'infrastructure virtualisée (On-premise et cloud) afin de les maintenir en condition opérationnelle dans le respect des accords de niveau de service, des règles de sécurité et de la réglementation en vigueur.
Afin de s'adapter aux différents environnements techniques ou dans une démarche de résolution de problèmes, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur intervient aussi bien sur des éléments physiques situés dans des salles serveurs et des datacenters, que des infrastructures virtuelles hébergées dans le Cloud privé et public.
Il travaille avec les fournisseurs dans le cadre de l'exploitation des services de cloud public.
Il peut travailler en équipe et piloter des techniciens. Il collabore avec les différents acteurs du système d'information.

Critères de performance

L'infrastructure virtualisée (on-premise et cloud) est opérationnelle conformément aux accords de niveaux de service.
Les tâches sont réalisées dans le respect des bonnes pratiques.
Les règles de sécurité sont appliquées
La règlementation en vigueur est respectée
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Réaliser un diagnostic et apporter une solution curative à un dysfonctionnement sur une infrastructure virtuelle.
Administrer la haute disponibilité et la répartition de charge au niveau des hyperviseurs.
Administrer et sécuriser les dispositifs de stockage type SAN, VSAN, NAS, DAS.
Administrer et sécuriser les réseaux virtuels dans des infrastructures virtualisées
Ajouter, configurer, administrer et sécuriser des ressources (VM, Conteneurs, accès réseaux ...) dans un cloud public (Azure, AWS …) à partir des différentes interfaces proposées.
Configurer, administrer et sécuriser les sauvegardes et la restauration des environnements Cloud et locaux avec un outil de type (VEEAM Backup, Veritas NetBackup …)
Déplacer des services (VM, conteneur) locaux vers le cloud et inversement.
Administrer et sécuriser les environnements virtualisés locaux et distribués en ligne de commandes et par scripts du type PowerShell, Bash, Python.
Implémenter, administrer et sécuriser des conteneurs.
Publier une image sur un dépôt de conteneurs (Docker Hub Registery, Azure Container Registry ..)
Créer et faire évoluer la documentation technique et les procédures d'exploitation
Suivre les « consommations à l'usage »
Appliquer les recommandations de l'ANSSI en matière de sécurité des infrastructures virtualisée
Appliquer la politique de la sécurité du système d'information de l'entreprise

Tester les procédures des plans de reprises et de continuité informatique (PRI, PCI) associés aux infrastructures virtualisées.
Prendre en compte le Règlement général sur la protection des données (RGPD)
Prendre en compte les bonnes pratiques d'éco-conception et de sobriété énergétique
S'assurer du respect des SLA par les fournisseurs.

Collaborer avec les différents acteurs de la direction des systèmes d'information
Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
Comprendre les différents types de cloud public, privé, hybride et multicloud
Comprendre les modèles de service Cloud IaaS, PaaS et SaaS
Connaissances des principes, des enjeux et des risques du cloud-computing
Connaissance des principales solutions de gestion d'environnements virtualisés
Connaissance des fonctions avancées de la gestion des environnements virtualisés (clustering, stockage, migration)
Connaissance des solutions convergentes ou hyper-convergentes
Connaissance de l'impact de la virtualisation sur la consommation d'énergie et l'optimisation des équipements
Connaissance des spécificités d'un datacenter (énergie, refroidissement, réseau, sécurité d'accès)
Connaissance des équipements matériels du cluster (serveurs, baies de stockage, switch)
Connaissance des risques inhérents à l'infogérance et à l'externalisation des systèmes d'information
Connaissances des techniques de virtualisation basées sur les conteneurs
Connaissance des principes des environnements de déploiement des infrastructures de cloud computing de type OpenStack, AzureStack, OpenNebula.
Connaissance des pratiques d'intégration continue de la démarche DEVOPS.
Connaissance des usages des solutions d'orchestration des conteneurs de type Kubernetes.

FICHE COMPÉTENCE PROFESSIONNELLE N° 5

Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure

Description de la compétence – processus de mise en œuvre

À partir des besoins et contraintes définis dans le cahier des charges fourni dans le cadre d'un projet d'évolution de l'infrastructure, concevoir et proposer dans les délais impartis une solution technique évolutive qui tient compte des contraintes budgétaires, environnementales, de production et de sécurité ainsi que des réglementations en vigueur.
Définir les critères et mettre en œuvre les moyens qui permettent de vérifier que la solution technique est conforme au cahier des charges.
Présenter et argumenter dans un rapport ou une présentation la solution technique afin de la soumettre à la validation des décideurs.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur peut exercer cette compétence à plein temps ou de façon intermittente en parallèle avec les tâches d'administration courantes.
Il peut être intégré dans une équipe projet ou travailler sous le contrôle de son responsable.
Selon la situation il peut mettre en œuvre cette compétence pour des besoins internes à son entreprise ou pour un client.

Critères de performance

Les contraintes budgétaires, environnementales, de production et de sécurité sont prises en compte
La réglementation en vigueur est respectée.
La solution proposée est évolutive.
La solution proposée est conforme au cahier des charges et respecte les délais.
La solution est présentée et argumentée de façon claire et structurée.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Repérer, tester et évaluer préalablement une solution technique en réalisant des maquettes ou des bancs d'essai comparatifs.
Définir les critères à retenir pour évaluer une solution.
Mettre en oeuvre un environnement de test ou de simulation
Évaluer l'impact d'une solution technique sur le système d'information.
Définir, planifier et ordonnancer les tâches du projet.
Prendre en compte les aspects de la sécurité dès la phase de conception (Security by design).
Intégrer les recommandations de l'ANSSI dans les solutions techniques étudiées.
Appliquer la politique de sécurité du système d'information de l'entreprise.
Prendre en compte les plans de reprise et de continuité informatique (PRI, PCI) dans l'élaboration de la solution.
Prendre en compte le Règlement général sur la protection des données (RGPD)
Prendre en compte la Règlementation relative à l'accessibilité du Référentiel général d'amélioration de l'accessibilité (RGAA)
Prendre en compte les bonnes pratiques d'éco-conception et de sobriété énergétique
Rédiger une proposition de solution argumentée et la présenter.
Réaliser une veille et se tenir informé de l'évolution des techniques et des offres des prestataires, fournisseurs et opérateurs.
S'assurer de la fiabilité des informations utilisées pour la recherche de solutions.

Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
Connaissance des solutions techniques de sécurisation d'une infrastructure informatique.
Connaissance des pratiques ou processus du développement, de la construction, de la transition et de l'assurance qualité des services type iso 20000 ou ITIL
Connaissance de méthodes de gestion de projet de type classique ou agile.
Connaissance des éléments constitutifs du TCO (Total Cost of Ownership)

FICHE COMPÉTENCE PROFESSIONNELLE N° 6

Mettre en production des évolutions de l'infrastructure

Description de la compétence – processus de mise en œuvre

À partir d'une solution, élaborée et testée en amont et répondant à une demande de changement, planifier, réaliser et valider son intégration en appliquant les bonnes pratiques afin qu'elle soit mise en production dans le respect des accords de niveau de service, des règles de sécurité et de la réglementation en vigueur.
Évaluer et valider chaque étape de la mise en production afin de limiter les risques sur la fourniture des services.
Tester et valider les procédures des plans de reprise et de continuité informatique (PRI, PCI) associés aux dispositifs mis en production.
Assurer le transfert de compétences et mettre à jour les documents d'exploitation.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur met en œuvre cette compétence en mode projet lors des scénarios d'évolution de l'entreprise.
Il peut travailler en équipe et piloter des techniciens. Il collabore avec les différents acteurs du système d'information.
Pour certaines phases de l'intégration, il peut être amené à travailler en horaires décalés ou ponctuellement les jours non ouvrés.

Critères de performance

L'intégration proposée respecte les bonnes pratiques et prend en compte les contraintes de production et de sécurité.
Chaque étape de la mise en production est évaluée et validée.
Les procédures des PRI et PCI associés aux dispositifs mis en production sont testés et validés.
La solution est mise en production conformément aux accords de niveau de service
Les documents d'exploitation sont mis à jour.
Le transfert de compétences est assuré.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Appliquer les bonnes pratiques et normes de type ITIL et iso 20000 dans la mise en production et déploiement des services.
Élaborer les procédures de test et de validation des plans de reprises et de continuité informatique (PRI, PCI).
Evaluer et valider une solution dans un environnement qui prend en compte l'environnement de production.
Minimiser l'impact sur la disponibilité du SI lors la planification et de de la mise en production.
Participer à la définition et la planification des tâches d'un projet.
Suivre et contrôler l'avancement des tâches de mise en production et en rendre compte.
Utiliser un outil de gestion de projets
Créer ou mettre à jour les informations et procédures d'exploitation.
Assurer le transfert de compétences aux personnes en charge de l'exploitation.
Prendre en compte l'accompagnement des utilisateurs dans le changement.
Piloter les intervenants internes et externes lors des différentes étapes de mise en production.
Appliquer la politique de sécurité du système d'information de l'entreprise.

Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
Connaissance des pratiques ou processus de gestion du déploiement, des mises en production, de la disponibilité, de la continuité et de la capacité de type ITIL et iso 20000.
Connaissance de méthodes de gestion de projet de type classique ou agile.

FICHE COMPÉTENCE PROFESSIONNELLE N° 7

Mettre en œuvre et optimiser la supervision des infrastructures

Description de la compétence – processus de mise en œuvre

A partir des accords de niveaux de service et des besoins de contrôle des infrastructures, choisir les indicateurs et évènements associés à la disponibilité, aux performances, à la consommation de services qui doivent être supervisés.
Mettre en œuvre ou optimiser les outils de supervision nécessaires au suivi des indicateurs et des évènements, en respect de la réglementation et des règles de sécurité, afin de mettre à disposition des équipes d'exploitation et d'administration les tableaux de bords et les informations indispensables au support et au pilotage des infrastructures du système d'information.

Afin de s'adapter aux différents environnements techniques, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur intervient aussi bien sur des éléments physiques situés dans des salles serveurs et des datacenters, que sur des infrastructures virtuelles hébergées dans le Cloud privé et public.
Il travaille avec les fournisseurs dans le cadre de la supervision des services de cloud public.
Il peut travailler en équipe et piloter des techniciens. Il collabore avec les différents acteurs du système d'information.

Critères de performance

Les indicateurs et les évènements choisis sont pertinents.
Les outils de supervisons sont fonctionnels et respectent la réglementation et les règles de sécurité.
Les tableaux de bords et les informations présentés sont structurés et exploitables.
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Définir les éléments de l'infrastructure qui doivent être suivis.
Définir les seuils d'alerte et les indicateurs principaux et les configurer.
Définir et mettre en œuvre les sondes, capteurs et les moniteurs à utiliser pour suivre les indicateurs de performance, de disponibilité et de consommation des services.
Mettre en œuvre et exploiter une solution de supervision dans une infrastructure distribuée
Mettre en œuvre une solution de centralisation et d'analyse des journaux d'événements.
Élaborer des tableaux de bord de suivi de production informatique
Appliquer les recommandations en matière de sécurisation des données de supervision et de journalisation
Appliquer les recommandations de l'ANSSI en matière de sécurité des dispositifs de supervision.
Prendre en compte le Règlement général sur la protection des données (RGPD)
Rédiger et mettre à jour la documentation et les procédures d'exploitation

Présenter par écrit ou lors d'un exposé les résultats de la production informatique.
Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des solutions de centralisation et d'analyse des journaux d'événements d'une infrastructure distribuée
Connaissance de la gestion des niveaux de services
Connaissance des bases de données de série temporelles
Connaissance du protocole SNMP
Connaissance du standard WBEM et sa déclinaison WMI Connaissance du protocole Syslog
Connaissance des protocoles d'analyse de flux réseaux de type Netflow

FICHE COMPÉTENCE PROFESSIONNELLE N° 8

Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure

Description de la compétence – processus de mise en œuvre

A partir d'une demande d'évaluation de la sécurité sur un périmètre défini de l'infrastructure, planifier et spécifier les points de contrôle et effectuer les mesures afin d'évaluer le niveau de sécurité dans le respect de la réglementation.
Rédiger un rapport présentant les contrôles, les mesures effectuées et l'évaluation du niveau de sécurité.
Participer à une démarche d'analyse de risques afin d'identifier les menaces, les vulnérabilités et la criticité des risques pouvant affecter les composants de l'infrastructure.
Participer à l'élaboration d'une lettre de mission en vue d'un audit de sécurité réalisé par un tiers.
A partir du rapport d'audit de sécurité du système d'information réalisé par un tiers, vérifier si les exigences de la lettre de mission ont été respectées afin de qualifier le travail effectué.
Exploiter les sources d'information, les logiciels et échanger par écrit avec les professionnels y compris en anglais.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur d'infrastructures sécurisées peut travailler en équipe et il collabore avec les différents acteurs du système d'information.

Critères de performance

Les points de contrôle sont pertinents
Les vulnérabilités des composants sont identifiées
Les risques et leurs menaces associées sont caractérisés.
Le rapport de contrôle est clair et exploitable.
La lettre mission comporte l'ensemble des exigences liées à un audit de sécurité.
La conformité du rapport d'audit à la lettre de mission est évaluée correctement.
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Caractériser les types de risques informatiques encourus (intrusion, piratage, malveillance, fraude).
Participer à une analyse des risques avec une méthode ou un guide de type EBIOS, ISO 27005
Identifier les différents types de menaces redoutées.
Analyser le scénario d'une menace.
Evaluer la criticité d'une vulnérabilité
Réaliser un audit de sécurité interne.
Utiliser des outils de détection de vulnérabilité.
Utiliser et adapter des scripts dans le cadre d'audit et d'évaluation du niveau de sécurité.
Réaliser des tests d'intrusion sur un système informatique de type WhiteBox.
Utiliser des outils de test et d'analyse de la sécurité inclus dans des distributions de type Kali linux
Réaliser une veille sur les menaces, les failles et les vulnérabilités.
Utiliser les common vuneralbility and exposure (CVE) et common weakness enumeration (CWE)

Communiquer avec l'ensemble des acteurs de la cybersécurité.

Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des risques informatiques encourus et leurs causes
Connaissance de base sur les organismes et la réglementation relatifs à la protection des données en France et en Europe (CNIL, RGPD)
Connaissance des organismes de lutte et d'information contre les risques Cyber ANSSI, CESIN, CLUSIF, MITRE, NIST, CIS...
Connaissance des principes d'une méthode de gestion des risques comme ISO 27005, EBIOS, MEHARI.
Connaissance des principaux intervenants dans le domaine de la cybersécurité.
Connaissance des principes d'un SOC (Security Operations Center).
Connaissance des principes des différents outils de mesures et d'analyse dédiés à la sécurité IDS/IPS, SIEM (Security Information and Event Management), UEBA (User and Entity Behavior Analytics), XDR (eXtended Detection and Response),
Connaissance des scripts Python, PowerShell, Bash
Connaissance des offres des prestataires spécialisés en cybersécurité

FICHE COMPÉTENCE PROFESSIONNELLE N° 9

Participer à l'élaboration et à la mise en œuvre de la politique de sécurité

Description de la compétence – processus de mise en œuvre

A partir des règles de sécurité retenues dans la politique de sécurité du système d'information (PSSI), contribuer, dans son périmètre d'intervention, au choix, à l'implantation et l'évaluation des solutions permettant leur mise en œuvre.
Participer à la définition, rédaction et la validation de procédures permettant la déclinaison opérationnelle de la PSSI.
S'assurer de la formation des utilisateurs au respect des bonnes pratiques de sécurité informatique et participer à la mise à niveau des équipes techniques afin de contribuer à l'application de la PSSI.
Afin de s'adapter aux différents environnements techniques, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur peut participer à un groupe de travail dans le cadre de l'élaboration de la PSSI. Il est alors sollicité pour son expertise technique.

Critères de performance

La solution choisie répond aux règles de sécurité retenues par la PSSI.
La solution choisise est mise en oeuvre et évaluées
Les procédures sont rédigées dans le respect des bonnes pratiques et validées
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Participer à l'élaboration des mesures à prendre et des dispositifs à mettre en œuvre dans le cadre du plan de reprise informatique et de continuité informatique (PRI, PCI).
Appliquer les recommandations des organismes de lutte et d'information contre les risques Cyber de type ANSSI.
Prendre en compte la Règlement général sur la protection des données (RGPD).
Prendre compte les environnements et les conditions de travail des utilisateurs afin de choisir des solutions de sécurité adaptées et compatibles.
Sécuriser et gérer les accès avec des méthodes et outils de type Pare-feu, Bastion, authentification multi facteur, méthode Zéro trust
Sécuriser les systèmes d'exploitation. Durcissement des systèmes Microsoft, Linux, Android …
Sécuriser les échanges avec des solutions de chiffrement, de VPN et de signatures.
Mettre en œuvre une stratégie de sauvegarde, en réaliser les procédures et tester les restaurations.
Mettre en œuvre la haute disponibilité pour des infrastructures réseaux, systèmes et pour les applications.
Identifier et proposer des systèmes de détection de menace type EDR, IPS/IDS, XDR, SIEM adaptés à l'entreprise.
Rédiger des procédures dans le respect des bonnes pratiques.
Réaliser une veille sur les menaces et les dispositifs de protection.
Réaliser une veille et analyser les offres des prestataires de services de sécurité managés.
Préparer une action de formation courte conforme aux objectifs et adaptée a destination des équipes techniques.

Communiquer avec l'ensemble des acteurs de la cybersécurité.

Animer une action de sensibilisation ou de formation courte.
Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des menaces et vulnérabilité.
Connaissance des normes et recommandations ISO27000 attachées à son domaine d'activité.
Connaissance des principes d'une méthode de gestion des risques de type EBIOS, ISO27005
Connaissance des solutions de sécurisation type IPS/IDS, EDR, XDR, SIEM, SOAR
Connaissance des offres des prestataires spécialisés en cybersécurité
Connaissance de la structure de la PSSI et de sa méthodologie d'élaboration.
Connaissance des concepts, objectifs et usages des PRA, PCA, PRI, PCI
Connaissance des principes de haute disponibilité et des systèmes redondants

FICHE COMPÉTENCE PROFESSIONNELLE N° 10

Participer à la détection et au traitement des incidents de sécurité

Description de la compétence – processus de mise en œuvre

En s'apputant sur les documents d'exploitation, configurer et exploiter un dispositif de détection d'évènements de sécurité afin de détecter et qualifier un incident.
Appliquer les mesures de réaction en réponse à un incident afin de minimiser l'impact sur les actifs de l'entreprise et d'informer les parties concernées.
Assurer la préservation des traces et des preuves numériques afin de les transmettre aux analystes cyber.
À la suite d'un incident de sécurité majeur, participer à la réalisation d'un retour d'expérience (RETEX) afin de capitaliser et renforcer la sécurité de l'entreprise.
Assurer sa veille en cybersécurité afin d'adapter les règles de détection et de traitement des incidents aux nouvelles menaces.
Afin de s'adapter aux différents environnements techniques, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais.

Contexte(s) professionnel(s) de mise en œuvre

L'administrateur est amené à travailler dans des conditions qui nécessitent réactivité et sang-froid notamment lorsque survient une situation critique suite à un incident de sécurité.
Il exerce cette compétence au sein d'une équipe et il collabore avec l'ensemble des acteurs en charge de la cybersécurité à l'interne et à l'externe.

Critères de performance

Le système est configuré afin de détecter les incidents de sécurité.
Les incidents sont identifés et qualifiés.
Les mesures de réponse à incident sont appliquées.
Les éléments de preuves et les traces numériques sont transmis aux analystes Cyber.
Les règles de détection et le traitement des incidents sont adaptés à l'évolution des menaces.
Un compte rendu du RETEX est réalisé.
Les moyens mis en place pour assurer sa veille en matière de cybersécurité sont pertinents.
Les informations et les documentations techniques sont comprises, y compris lorsqu'elles sont en anglais.
Les échanges par écrit avec les professionnels sont clairs, concis, structurés et adaptés aux destinataires, y compris lorsqu'ils se font en anglais.

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Appliquer les recommandations des organismes de lutte et d'information contre les risques Cyber de type ANSSI, NIS.
Configurer et exploiter un système de détection ou réponse à incident de sécurité (SIEM, SOAR, XDR)
Adapter les règles de détection des vulnérabilités aux différents environnements.
Qualifier un incident de sécurité.
Appliquer les mesures de réaction en réponse à un incident de sécurité
Assurer la préservation et la disponibilité des journaux d'évènements et de traces.
Transmettre les informations nécessaires aux analystes ou aux équipes de réponse sur incidents (CERT)
Réaliser la veille sur les menaces et les dispositifs de protection.
Réaliser un compte rendu d'incident.
Réaliser une veille et analyser les offres des prestataires de services de sécurité managés.

Utiliser l’anglais à l’écrit et à l’orale dans son activité professionnelle.(Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)

Connaissance des menaces et vulnérabilité.
Connaissance des règles d’organisation d’un RETEX
Connaissance des solutions de sécurisation type IPS/IDS, EDR, MDR, XDR, SIEM, SOAR, UEBA
Connaissance de l’organisation et des rôles au sein d’un SOC.
Connaissance de tous les acteurs de la cybersécurité
Connaissance des offres des prestataires spécialisés en cybersécurité

FICHE DES COMPÉTENCES TRANSVERSALES DE L'EMPLOI TYPE

Communiquer en français et en anglais

Description de la compétence – processus de mise en œuvre

Au cours d'un processus de résolution d'incident interroger les parties prenantes afin de collecter les éléments nécessaires au diagnostic. Rédiger des procédures de résolutions ou des comptes rendu d'incidents dans un langage adapté au destinataire. Afin de s'adapter aux différents environnements techniques ou dans une démarche de résolution de problèmes, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais. Afin de connaître les besoins et contraintes définis dans une demande de changement, analyser le cahier des charges et solliciter si nécessaire des informations complémentaires auprès d'interlocuteurs divers.
Présenter et argumenter de façon claire et structurée une solution technique répondant à une demande ou un compte rendu d'action dans un rapport écrit ou à l'oral.
Lors des réunions techniques, en face-à-face ou à distance, suivre activement les échanges, s'exprimer devant les participants de manière structurée et constructive et argumenter ses propositions.
Rédiger des dossiers techniques dans un langage adapté au destinataire et formuler ses courriels professionnels de manière claire et concise.
Rechercher des informations dans des documents techniques et communiquer si besoin au sujet des contenus.
Animer une session de formation ou de sensibilisation à une pratique ou à une technologie dépendant de son domaine de compétence en utilisant des moyens et niveaux de communication adaptés aux participants.

Critères de performance

Des informations complémentaires sont sollicitées si nécessaire auprès d'interlocuteurs divers
La solution est présentée à l'interlocuteur, oralement ou par écrit, de manière structurée et adaptée au contexte
La documentation technique est comprise
La communication orale est claire, concise, structurée, et adaptée au destinataire et au contexte
La communication écrite est claire, concise, structurée, et adaptée au destinataire et au contexte
Niveaux requis en anglais selon le Cadre européen commun de référence pour les langues (CECRL) :
Compréhension orale et expression orale niveau A2, compréhension écrite et expression écrite niveau B1.

Apprendre en continu

Description de la compétence – processus de mise en œuvre

Pour maintenir ses compétences et sa capacité opérationnelle dans l'emploi, mettre en place un système de veille technologique permettant de suivre l'actualité des évolutions technologiques et des problématiques de sécurité.?
Pour résoudre des problèmes, s'auto-former en recherchant des informations sur Internet ou dans des documentations techniques, y compris en anglais, et en sollicitant l'appui des personnes compétentes.

Critères de performance

Le système de veille mis en place permet de suivre l'actualité de la profession, les principales évolutions technologies et les problématiques de sécurité en lien avec le métier?
Les informations issues de l'auto-formation et de la veille technologique sont exploitables pour résoudre un problème?
Les publications en anglais sont comprises (niveau B1 CECRL)

Glossaire technique

ANSSI

L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Prévention, protection, réaction, formation et labellisation de solutions et de services pour la sécurité numérique de la Nation.

BYOD

Abréviation de l'anglais « bring your own device » (« apportez vos appareils personnels ») ; est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette) dans un contexte professionnel. Cette pratique pose des questions relatives à la sécurité de l'information et à la protection des données.

CECRL : Cadre européen commun de référence pour les langues

UTILISATEUR EXPÉRIMENTÉ
C2 : Maîtrise
C1 : Autonomie
UTILISATEUR INDÉPENDANT
B2 : Avancé
B1 : Indépendant. Peut comprendre les points essentiels quand un langage clair et standard est utilisé et s'il s'agit de choses familières dans le travail. Peut se débrouiller dans la plupart des situations rencontrées en voyage dans une région où la langue cible est parlée. Peut décrire un espoir ou un but et exposer brièvement des raisons ou explications pour un projet ou une idée.
Rechercher des informations dans des documents techniques. Rédiger des dossiers techniques dans un langage adapté au destinataire et formuler ses courriels professionnels de manière claire et concise.?Lors des réunions techniques, en face-à-face ou à distance, suivre activement les échanges.

UTILISATEUR ÉLÉMENTAIRE
A2 : Élémentaire. Peut communiquer lors de tâches simples et habituelles ne demandant qu'un échange d'informations simple et direct sur des sujets familiers et habituels. Peut décrire avec des moyens simples sa formation, son environnement immédiat et évoquer des sujets qui correspondent à des besoins immédiats.
Lors des réunions techniques, en face-à-face ou à distance, s'exprimer devant les participants de manière structurée et constructive et argumenter ses propositions.
A1 : Introductif ou découverte

CERT

CERT (Computer Emergency Response Team) est un terme utilisé pour décrire une équipe de professionnels de la sécurité informatique qui sont chargés de gérer les incidents de sécurité et de répondre aux menaces de sécurité.

CIS

Le CIS (center for internet security) est un organisme à but non lucratif crée en 2000.

Cloud Computing

Le cloud computing, en français l'informatique en nuage (ou encore l'infonuagique au Canada), est la pratique consistant à utiliser des serveurs informatiques à distance et hébergés sur internet pour stocker, gérer et traiter des données, plutôt qu'un serveur local ou un ordinateur personnel (source Wikipedia 20/12/2022).
Clusif

Conteneur

l virtualise le système d'exploitation sous-jacent et fait en sorte que l'application en conteneur "pense" qu'elle dispose pour elle seule du système d'exploitation, y compris le processeur, la mémoire, le stockage de fichiers et les connexions réseau. Il peut être déployé et exécuté sur n'importe quel serveur. (Source : https://azure.microsoft.com/)

EBIOS

EBIOS signifie « Expression des Besoins et Identification des Objectifs de Sécurité » et désigne une méthode de référence qui consiste à évaluer et à traiter les risques de sécurité des systèmes d'information. L'objectif est de déterminer les risques sur un périmètre à auditer.

EDR

EDR (Endpoint Detection and Response) est un terme utilisé pour décrire une approche de gestion de la sécurité qui vise à détecter et à répondre aux menaces de sécurité sur les terminaux de l'entreprise, comme les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles.

IaaS

Infrastructure as a Service « C'est un modèle où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur. Cela peut représenter pour certaines directions des systèmes d'information (DSI) un moyen de réaliser des économies, principalement en transformant des investissements en contrats de location » (source Wikipedia 5/10/2017).
Dans ce modèle, l'administration des serveurs reste à la main de l'entreprise. Seule la gestion du matériel est sous la responsabilité du fournisseur de service.Seule la gestion du matériel est sous la responsabilité du fournisseur de service.

IDS

Processus de surveillance du trafic réseau et d'analyse de celui-ci pour détecter des signes d'éventuelles intrusions.

IPS

Intrusion Prevension System: Système de prévention des intrusions qui consiste à effectuer une détection des intrusions réseaux puis à arrêter les incidents détectés, généralement en supprimant des paquets ou en mettant fin à des sessions.

ITIL

Information Technology Infrastructure Library "ITIL® est un référentiel de bonnes pratiques orienté processus destiné aux organisations informatiques qui délivrent des services complets à ses clients." (Source ITILFrance)

MCO

Le maintien en condition opérationnelle (abrégé MCO) est l'ensemble des mesures prises pour garantir que la bascule vers un environnement dégradé n'entraîne pas une altération inacceptable des conditions de travail habituelles.

MCS

Le maintien en condition de sécurité (MCS) est une approche de gestion de la sécurité qui vise à assurer que les équipements, les installations et les systèmes de sécurité d'une organisation sont en bon état de fonctionnement et prêts à être utilisés en cas de besoin. Le MCS comprend toutes les activités nécessaires pour maintenir l'efficacité et la fiabilité des équipements et des systèmes de sécurité, ainsi que pour gérer les risques associés à leur utilisation.

MDR

MDR (Managed Detection and Response) est un terme utilisé pour décrire un service de gestion de la sécurité informatique proposé par une entreprise tierce.

MFA

Le MFA (Multi-Factor Authentication, ou authentification à plusieurs facteurs en français) est une technique de sécurité qui vise à renforcer la sécurité des systèmes d'authentification en exigeant la vérification de plusieurs éléments d'identification avant de permettre l'accès à un compte ou à un système.

MITRE

MITRE est une organisation à but non lucratif américaine dont l'objectif est de travailler pour l'intérêt public. Ses domaines d'intervention sont l'ingénierie des systèmes, la technologie de l'information, les concepts opérationnels, et la modernisation des entreprises.

NAS

NAS (Network Attached Storage) est un terme qui désigne un système de stockage de données qui est connecté à un réseau local et qui peut être utilisé par plusieurs ordinateurs ou appareils connectés au réseau pour stocker et accéder aux données.

NIST

Le National Institute of Standards and Technology (NIST) en français : « Institut national des normes et de la technologie », est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des normes de concert avec l'industrie.

On-Premises

Les solutions « On-premises » (sur site) s'opposent au modèle « As a Service » dans le sens où elles sont détenues, gérées ou hébergées physiquement par l'entreprise utilisatrice.

OTP

L'OTP (One-Time Password, ou mot de passe à usage unique en français) est un type de mot de passe qui ne peut être utilisé qu'une seule fois pour s'authentifier sur un système ou accéder à un compte.

PaaS

Platform as a Service : « est l'un des types de cloud computing, principalement destiné aux entreprises, où l'entreprise cliente maintient les applications proprement dites ; le fournisseur cloud maintient la plate-forme d'exécution de ces applications » (source Wikipédia 5/10/2017).
La plateforme comprend le matériel, le système d'exploitation le réseau et le stockage.

PASSI

Prestataires d'audit de la sécurité des systèmes d'information qualifiés

PCA

Plan de continuité d'activité

PCI

Plan de Continuité Informatique

PDCA

PDCA (Plan-Do-Check-Act) est un modèle de gestion utilisé pour améliorer les processus et atteindre des objectifs précis.

PRA

Plan de reprise d'activité.

PRI

Plan de Reprise Informatique

RETEX

Le Retour d'Expérience (également appelé RETEX ou REX) est une méthode visant à identifier et analyser les anomalies, les écarts et tous les événements, qu'ils soient positifs ou négatifs, en identifiant les causes et les conséquences, et en tirant des leçons de ces événements.

SaaS

Software as a Service : « est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent librement le service en ligne ou, plus généralement, payent un abonnement. » (Source Wikipédia 5/10/2017)

SAN

AN (Storage Area Network) est un terme qui désigne un réseau de stockage de données qui permet de connecter des serveurs de stockage de données à des serveurs de calcul

SIEM

Un SIEM ou Security Information & Event Management est une solution de cybersécurité combinant la gestion d'informations de sécurité (SIM) et la gestion des évènements de sécurité (SEM).

SLA

Un SLA (Service Level Agreement) est un contrat entre une entreprise et un fournisseur de services qui définit les objectifs de qualité et les niveaux de service que le fournisseur s'engage à fournir. Il décrit généralement les paramètres de performance du service, tels que la disponibilité, la fiabilité, la qualité de service et les temps de réponse, ainsi que les modalités de gestion des incidents et de résolution des problèmes.

SOAR

SOAR (Security Orchestration, Automation and Response) est un terme utilisé pour décrire une approche pour la gestion de la sécurité informatique qui vise à automatiser et à orchestrer les processus de sécurité de l'entreprise.

SOC

Un Security Operations Center (SOC), dans une entreprise, est une division qui assure la sécurité de l'organisation et surtout le volet sécurité de l'information.

UEBA

UEBA (User and Entity Behavior Analytics) est un terme utilisé pour décrire une approche de gestion de la sécurité qui vise à surveiller et à analyser le comportement des utilisateurs et des entités (comme les appareils et les applications) dans l'environnement informatique de l'entreprise.

WAF

Un WAF (Web Application Firewall) est un type de pare-feu qui protège les applications Web contre les attaques de cybercriminels. Il s'agit d'un dispositif de sécurité qui analyse et filtre le trafic Web entrant et sortant d'une application Web, afin de bloquer les menaces telles que les attaques par injection de code, les attaques par déni de service (DoS), les attaques par force brute, etc.

WBEM

WBEM (Web-Based Enterprise Management), qui pourrait se traduire par « Gestion de l'entreprise s'appuyant sur le Web », est un ensemble de techniques et de standards Internet de gestion servant à unifier la gestion des environnements d'informatique distribuée.

White Box

Un audit de sécurité white box — boite blanche (parfois boite de cristal) signifie qu'un maximum d'information est transmis aux pentesters avant l'audit. Les informations nécessaires au bon déroulement de l'audit sont partagées en toute transparence. Le fonctionnement de la cible est ainsi connu et rendu visible, d'où le terme boite blanche.

XDR

XDR (eXtended Detection and Response) est un terme utilisé pour décrire une approche de gestion de la sécurité qui vise à étendre la détection et la réponse aux menaces de sécurité à l'ensemble de l'environnement informatique de l'entreprise.

Glossaire du REAC

Activité type

Une activité type est un bloc de compétences qui résulte de l'agrégation de tâches (ce qu'il y a à faire dans l'emploi) dont les missions et finalités sont suffisamment proches pour être regroupées. Elle renvoie au certificat de compétences professionnelles (CCP).

Activité type d'extension

Une activité type d'extension est un bloc de compétences qui résulte de l'agrégation de tâches qui constituent un domaine d'action ou d'intervention élargi de l'emploi type. On la rencontre seulement dans certaines déclinaisons de l'emploi type. Cette activité n'est pas dans tous les TP. Quand elle est présente, elle est attachée à un ou des TP. Elle renvoie au certificat complémentaire de spécialisation (CCS).

Compétence professionnelle

La compétence professionnelle se traduit par une capacité à combiner un ensemble de savoirs, savoir-faire, comportements, conduites, procédures, type de raisonnement, en vue de réaliser une tâche ou une activité. Elle a toujours une finalité professionnelle. Le résultat de sa mise en œuvre est évaluable.

Compétence transversale

La compétence transversale désigne une compétence générique commune aux diverses situations professionnelles de l'emploi type. Parmi les compétences transversales, on peut recenser les compétences correspondant :

- à des savoirs de base,
- à des attitudes comportementales et/ou organisationnelles.

Critère de performance

Un critère de performance sert à porter un jugement d'appréciation sur un objet en termes de résultat(s) attendu(s) : il revêt des aspects qualitatifs et/ou quantitatifs.

Emploi type

L'emploi type est un modèle d'emploi représentatif d'un ensemble d'emplois réels suffisamment proches, en termes de mission, de contenu et d'activités effectuées, pour être regroupées : il s'agit donc d'une modélisation, résultante d'une agrégation critique des emplois.

Référentiel d'Emploi, Activités et Compétences (REAC)

Le REAC est un document public à caractère règlementaire (visé par l'arrêté du titre professionnel) qui s'applique aux titres professionnels du ministère chargé de l'emploi. Il décrit les repères pour une représentation concrète du métier et des compétences qui sont regroupées en activités dans un but de certification.

Savoir

Un savoir est une connaissance mobilisée dans la mise en œuvre de la compétence professionnelle ainsi qu'un processus cognitif impliqué dans la mise en œuvre de ce savoir.

Savoir-faire organisationnel

C’est un savoir et un savoir-faire de l’organisation et du contexte impliqués dans la mise en œuvre de l’activité professionnelle pour une ou plusieurs personnes.

Savoir-faire relationnel

C’est un savoir comportemental et relationnel qui identifie toutes les interactions socioprofessionnelles réalisées dans la mise en œuvre de la compétence professionnelle pour une personne. Il s’agit d’identifier si la relation s’exerce : à côté de (sous la forme d’échange d’informations) ou en face de (sous la forme de négociation) ou avec (sous la forme de travail en équipe ou en partenariat, etc.).

Savoir-faire technique

Le savoir-faire technique est le savoir procéder, savoir opérer à mobiliser en utilisant une technique dans la mise en œuvre de la compétence professionnelle ainsi que les processus cognitifs impliqués dans la mise en œuvre de ce savoir-faire.

Titre professionnel

La certification professionnelle délivrée par le ministre chargé de l'emploi est appelée « titre professionnel ». Ce titre atteste que son titulaire maîtrise les compétences, aptitudes et connaissances permettant l'exercice d'activités professionnelles qualifiées. (Article R338-1 et suivants du Code de l’Education).