RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

RÉFÉRENTIEL DE COMPÉTENCES

WWW.CYBERMALVEILLANCE.GOUV.FR

Version 1.0 du 15/03/2023

SOMMAIRE

INTRODUCTION

Le Référentiel de Compétences Cyber pour les Prestataires (RCCP) répertorie l'ensemble des compétences indispensables pour un prestataire de services en cybersécurité, visant une labellisation de niveau « ExpertCyber ».

Basé sur le cadre méthodologique du NIST*, le RCCP constitue un état de l'art, en inventoriant de manière exhaustive toutes les compétences de sécurité sur un large spectre d'activité.

Il s'étend ainsi sur tout le cycle de la cybersécurité, de la chaîne de la sécurisation, au maintien en conditions opérationnelles et de sécurité jusqu'à la remédiation.

Aussi, celui-ci n'est pas nécessairement représentatif du niveau d'un prestataire labellisé ExpertCyber, *qui ne saurait intégrer de façon systématique* la totalité de ces compétences.

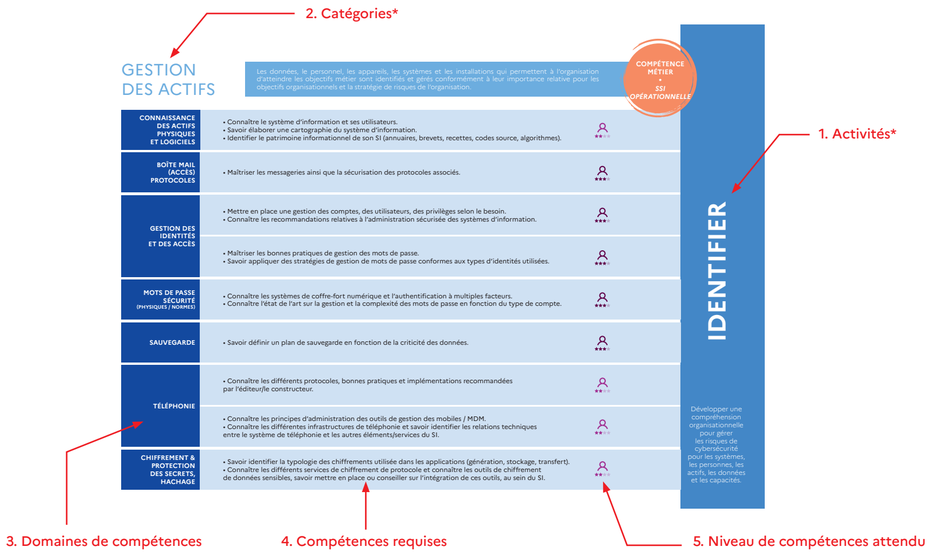
Destiné prioritairement aux organismes de formation, le RCCP a pour vocation de leur permettre de construire des modules ou des parcours d'apprentissage, correspondant aux besoins des prestataires souhaitant se spécialiser en cybersécurité et ainsi apporter un niveau de réponse adapté à une clientèle de TPE-PME, de petites et moyennes collectivités et d'associations.

Le groupe AFNOR, le Campus régional de Cybersécurité et de Confiance numérique (C3NA), le Centre de Formation de l'ANSSI (CFSSI) et Cybermalveillance.gouv.fr ont conçu le RCCP dans une démarche responsable, ayant pour but de contribuer à la montée en compétence des prestataires « terrain », qui constituent un maillon indispensable de la chaîne de sécurisation du tissu économique français sur l'ensemble de nos territoires.

**NIST : National Institute of Standards and Technology*

NOTICE
DU RÉFÉRENTIEL DE COMPÉTENCES CYBER POUR LES PRESTATAIRES (RCCP)

Afin de s'approprier au mieux le RCCP, voici une légende explicative présentant les différentes rubriques du référentiel pour en faciliter la lecture :



NIVEAU DE COMPÉTENCES ATTENDU

DÉBUTANT
•
Compréhension des principaux enjeux et problématiques liées à la compétence

INTERMÉDIAIRE
•
Actes simples liés à la compétence

EXPÉRIMENTÉ
•
Compétence confirmée

EXPERT
•
Haut niveau de maîtrise de la compétence

*Classification et définitions issues du cadre NIST (National Institute of Standards and Technology)

GESTION DES ACTIFS

Les données, le personnel, les appareils, les systèmes et les installations qui permettent à l'organisation d'atteindre les objectifs métier sont identifiés et gérés conformément à leur importance relative pour les objectifs organisationnels et la stratégie de risques de l'organisation.

COMPÉTENCE MÉTIER • *SSI OPÉRATIONNELLE*

CONNAISSANCE DES ACTIFS PHYSIQUES ET LOGICIELS	• Connaître le système d'information et ses utilisateurs. • Savoir élaborer une cartographie du système d'information. • Identifier le patrimoine informationnel de son SI (annuaires, brevets, recettes, codes source, algorithmes).
BOÎTE MAIL (ACCÈS) PROTOCOLES	• Maîtriser les messageries ainsi que la sécurisation des protocoles associés.
GESTION DES IDENTITÉS ET DES ACCÈS	• Mettre en place une gestion des comptes, des utilisateurs, des privilèges selon le besoin. • Connaître les recommandations relatives à l'administration sécurisée des systèmes d'information.
	• Maîtriser les bonnes pratiques de gestion des mots de passe. • Savoir appliquer des stratégies de gestion de mots de passe conformes aux types d'identités utilisées.
MOTS DE PASSE	• Connaître les systèmes de coffre-fort numérique et les différentes formes d'authentification à multiples facteurs. • Connaître l'état de l'art sur la gestion et la complexité des mots de passe en fonction du type de compte.
SAUVEGARDE	• Savoir définir un plan de sauvegarde en fonction de la criticité des données.
TÉLÉPHONIE	• Connaître les différents protocoles, bonnes pratiques et implémentations recommandées par l'éditeur/le constructeur.
	• Connaître les principes d'administration des outils de gestion des mobiles / MDM. • Connaître les différentes infrastructures de téléphonie et savoir identifier les relations techniques entre le système de téléphonie et les autres éléments/services du SI.
CHIFFREMENT & PROTECTION DES SECRETS, HACHAGE	• Savoir identifier la typologie des chiffrements utilisée dans les applications (génération, stockage, transfert). • Connaître les différents services de chiffrement de protocole et connaître les outils de chiffrement de données sensibles, savoir mettre en place ou conseiller sur l'intégration de ces outils, au sein du SI.

IDENTIFIER

Développer une compréhension organisationnelle pour gérer les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.

Développer une compréhension organisationnelle pour gérer les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

ENVIRONNEMENT MÉTIER

La mission, les objectifs, les parties prenantes et les activités de l'organisation sont compris et priorisés ; ces informations sont utilisées pour informer les rôles, les responsabilités et les décisions de gestion des risques en matière de cybersécurité.

CONNAISSANCE DE L'ÉCOSYSTÈME	• Connaître les acteurs étatiques impliqués dans la SSI (l'ANSSI, la BL2C, le ComCyberGend, Cybermalveillance.gouv.fr, la DGSI, la DRSD, l'OCLCTIC…).	★★☆☆
	• Connaître les associations ou les groupements du territoire en lien avec la SSI (Campus Cyber, Clusir, CESIN…).	★★☆☆
	• Connaître la typologie de clients et leur écosystème (public, privé, administration, OSE, OIV, FSN, acteurs de la chaîne d'approvisionnement…).	★★☆☆

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

GOUVERNANCE

Les politiques, procédures et processus pour gérer et surveiller les exigences réglementaires, juridiques, environnementales, opérationnelles et de risque de l'organisation sont comprises et informent la gestion du risque de cybersécurité.

CONNAISSANCE DES NORMES ET STANDARDS	• Connaître les principes généraux des normes ISO 27K, NIST.	★★★☆
	• Connaître les instructions régissant les systèmes d'information sensibles et classifiés (II 901 et IGI 1300).	★★☆☆
CONNAISSANCE JURIDIQUE ET RÉGLEMENTAIRE	• Connaître les fondamentaux du RGPD et de la législation concernant les atteintes aux STAD (CP 323-1 et 323-2).	★★☆☆
OBLIGATIONS DU PRESTATAIRE, RISQUES CLIENT	• Maîtriser les éléments d'un contrat de prestation incluant les niveaux de service et les champs de responsabilité. • Connaître les bases juridiques liées à l'externalisation d'un SI et les obligations en matière d'utilisation, de localisation et de transfert de données.	★★★☆
RECOMMANDATIONS DE BASE	• Maîtriser et appliquer les guides de bonnes pratiques de l'ANSSI. • Savoir adapter le niveau d'exigence en fonction de la nature de l'entité, de son exposition et de sa tolérance au risque numérique.	★★★☆

APPRÉCIATION DES RISQUES

Comprendre le risque de cybersécurité à tous les niveaux de l'entreprise (y compris la mission, les fonctions, l'image ou la réputation), tous les actifs de l'entreprise et les individus.

COMPÉTENCE MÉTIER • *PILOTAGE DE LA SSI*

IDENTIFICATION	• Définir les vulnérabilités et les menaces par rapport aux actifs de la structure. • Connaître les bases d'une analyse de risques (exemple : EBIOS RM, ISO 27K5…). • Concevoir un tableau des risques appliqués aux actifs et aux données de la structure dans son environnement.	★★★☆
TYPOLOGIE DES ATTAQUANTS	• Connaître les typologies d'attaquants (opportunistes, organisations criminelles, étatique…).	★★☆☆
GESTION DES VULNÉRABILITÉS	• Maîtriser les outils de contrôle de conformité, de configuration et de mise à jour.	★★★☆

STRATÉGIE DE GESTION DES RISQUES

Les priorités, les contraintes, les tolérances au risque et les hypothèses de l'organisation sont établies et utilisées pour appuyer les décisions relatives au risque opérationnel.

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

GESTION DE CRISE	• Connaître les acteurs, le principe d'activation et le mode de fonctionnement d'une cellule de crise. • Connaître l'environnement et les métiers de la structure en crise (administrés, acteurs, clients, domaines critiques).	★★★☆

GESTION DES RISQUES DE LA CHAÎNE D'APPROVISIONNEMENT

Les priorités, les contraintes, les tolérances au risque et les hypothèses sont établies et utilisées pour étayer les décisions relatives aux risques associées à la gestion des risques de la chaîne d'approvisionnement. L'organisation a établi et mis en œuvre les processus pour identifier, apprécier et gérer les risques liés à la chaîne d'approvisionnement.

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

RELATION CLIENT (CONNAISSANCE DE SON ÉCOSYSTÈME)	• Identifier toutes les actions liées à la chaîne d'approvisionnement et apprécier les risques associés.	★★☆☆
ANTICIPATION	• Savoir élaborer et appliquer une politique de veille sur les menaces et les risques liés aux attaques de chaîne d'approvisionnement (altération du code, diffusion massive de code malveillant, détournement d'applications légitimes).	★★☆☆

IDENTIFIER

Développer une compréhension organisationnelle pour gérer les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.

Élaborer et mettre en œuvre des mesures de protection appropriées pour assurer la prestation des services essentiels de l'organisation

COMPÉTENCE MÉTIER • *SSI OPÉRATIONNELLE*

L'accès aux actifs physiques et logiques et aux installations associées est limité aux utilisateurs, processus et appareils autorisés ; il est géré conformément au risque apprécié d'accès non autorisé aux activités et transactions autorisées.

GESTION DES IDENTITÉS ET CONTRÔLE D'ACCÈS

CHIFFREMENT & PROTECTION DES SECRETS, HACHAGE	• Connaître et maîtriser les différents modes de stockage et de distribution des identités et des mots de passe dans les applications et les OS (chiffrement, hachage, 2FA, clés publiques et privées). • Appliquer les recommandations de l'ANSSI.	★★★☆
SÉCURISATION	• Maîtriser les différents types d'accès aux systèmes (RDP, SSH) et leur sécurité renforcée. • Gestion des certificats et des autorités de certifications. • Savoir identifier et contrôler tout équipement et personne ayant une relation technique avec le SI.	★★★☆

COMPÉTENCE TRANSVERSALE • *TRAVAIL EN ÉQUIPE*

Le personnel et les partenaires de l'organisation reçoivent une formation sur la sensibilisation à la cybersécurité et sont formés pour s'acquitter de leurs tâches et responsabilités liées à la cybersécurité conformément aux politiques, procédures et accords connexes.

SENSIBILISATION ET FORMATION

RECOMMANDATIONS DE BASE	• Mettre à disposition des supports d'information à destination des clients pour sensibiliser aux bonnes pratiques d'hygiène informatique.	★★★☆
RELATION CLIENT	• Élaborer des formations relatives aux bonnes pratiques d'hygiène informatique dans un format synthétique (exemple 1h à 2h) à destination des utilisateurs des structures clients. • Évaluer le niveau de sécurité des utilisateurs (test, campagne de faux phishing…).	★★★☆

SÉCURITÉ DES DONNÉES

Les informations et les enregistrements (données) sont gérés conformément à la stratégie de gestion des risques de l'organisation pour protéger la confidentialité, l'intégrité et la disponibilité des informations.

COMPÉTENCE MÉTIER • *SSI OPÉRATIONNELLE*

SÉCURITÉ PHYSIQUE	• Connaître les points de contrôles sur les accès physiques (clefs, badge). • Protection environnement (détection incendie, vidéo surveillance, fluides). • Savoir identifier les risques associés à l'utilisation d'un accès physique aux différents équipements d'un SI.	★★☆☆
TÉLÉPHONIE	• Savoir identifier les risques associés à une utilisation d'un téléphone personnel. • Connaître le mode de fonctionnement d'un gestionnaire de configuration pour terminaux mobiles et les règles à appliquer. • Connaître le mode de fonctionnement d'un IPBX (trunk, annuaire, protocoles).	★★☆☆
ARCHITECTURE	• Maîtriser les protocoles de sécurité des réseaux physiques et des réseaux sans fil. • Maîtriser les VLANs et les listes de contrôles d'accès réseau. • Déployer et cloisonner des infrastructures de réseaux en conformité avec leurs rôles et objectifs respectifs.	★★★☆
SÉCURISATION	• Maîtriser les outils de protections des applicatifs en lignes (WAF, Anti-DDOS…). ainsi que les outils de contre-mesures (IPS…). • Maîtriser les outils de chiffrements de disque (Bitlocker, LUKS…).	★★★☆
ANTIVIRUS	• Maîtriser le déploiement d'un antivirus, sa gestion centralisée et son mode de mise à jour des bases virales. • Connaître le rôle d'un EDR et d'un XDR. • Définir une politique et des procédures de gestion des alertes.	★★★☆
ADMINISTRATION SYSTÈMES (VM, OS)	• Savoir durcir un OS, limiter la surface d'attaque systèmes et services réseaux. • Maîtriser l'analyse des logs et l'administration courante des systèmes comme Windows, MAC et Linux.	★★★☆
DISPONIBILITÉ	• Maîtriser les principes d'architecture redondante par grappes, les équilibreurs de charges et les services anti-DDoS. • Être en capacité de répondre à des problématiques de redirection de flux via des liens tiers.	★★★☆

PROTÉGER

Élaborer et mettre en œuvre des mesures de protection appropriées pour assurer la prestation des services essentiels de l'organisation

PROTÉGER

Élaborer et mettre en œuvre des mesures de protection appropriées pour assurer la prestation des services essentiels de l'organisation

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

PROCESSUS ET PROCÉDURES DE PROTECTION DES INFORMATIONS

Les politiques de sécurité (qui concernent l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction et la coordination entre les entités organisationnelles), des processus et des procédures sont maintenus et utilisés pour gérer la protection des systèmes d'information et des actifs.

PROCÉDURE INTERNE	• Savoir rédiger ou faire rédiger une charte d'utilisation des moyens informatiques. • Savoir rédiger ou faire rédiger une politique de sécurité des systèmes d'information. • Avoir une connaissance des documents afférents à la SSI au sein d'une organisation (PRA/PCA).	★★☆☆

COMPÉTENCE MÉTIER • *SSI OPÉRATIONNELLE*

MAINTENANCE

La maintenance et les réparations du système d'information sont effectuées conformément aux politiques et procédures.

MCO / MCS	• Maîtriser des outils de gestion de parc et de déploiement automatique de logiciels. • Savoir appliquer un plan de continuité opérationnel incluant la supervision, la maintenance système et les modes opératoires applicatifs du client. • Être en mesure de maintenir des OS et des infrastructures tout en conservant un niveau de sécurité adéquat par le maintien des versions logicielles et des politiques de mises à jour.	★★★☆

COMPÉTENCE MÉTIER • *SSI OPÉRATIONNELLE*

TECHNOLOGIE DE PROTECTION

Les solutions de sécurité technique sont gérées pour assurer la sécurité et la résilience des systèmes et des actifs, conformément aux politiques, procédures et accords connexes.

CONNAISSANCE DES SOLUTIONS ET TECHNOLOGIES DE SÉCURISATION EXISTANTES	• Maîtriser la gestion d'un équipement de sécurité et savoir documenter les règles appliquées à la gestion des mises à jour et des accès. • Savoir filtrer les principaux flux associés à un SI pour respecter le principe de moindre privilège.	★★★☆
	• Connaître les outils EDR/XDR et les pare-feux applicatifs. • Savoir identifier le niveau de maturité de l'organisation pour lui conseiller une solution adaptée (EDR, SIEM…).	★★★☆

DÉTECTER

Développer et mettre en œuvre des activités appropriées pour identifier l'occurrence d'un événement de cybersécurité.

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

ANOMALIES ET ÉVÉNEMENTS

Une activité anormale est détectée et l'impact potentiel des événements est compris.

IDENTIFICATION	• Avoir la connaissance des phases d'attaques (MITRE ATT&CK) . • Connaître les vecteurs possibles de compromission et leurs capacités/conséquences. • Savoir définir un comportement jugé non conforme en fonction du vecteur de compromission.	★★★☆
GESTION DES VULNÉRABILITÉS	• Maîtriser les outils et les méthodes de détection de vulnérabilités (CVE). • Être en capacité d'associer sur un délai court des solutions de remédiation ou des mesures palliatives sur des vulnérabilités connues et encore non corrigées. • Savoir appliquer et anticiper les conséquences de l'installation de ces mesures.	★★★☆

COMPÉTENCE MÉTIER • *SUPERVISION*

SURVEILLANCE CONTINUE DE LA SÉCURITÉ

Le système d'information et les actifs sont surveillés pour identifier les événements de cybersécurité et vérifier l'efficacité des mesures de protection.

ANALYSE (RÉSEAUX, LOGS, OUTILS D'ANALYSE)	• Établir une procédure de collecte et de consolidation sécurisée des journaux, des systèmes et des équipements.	★★☆☆
SUPERVISION SSI	• Maîtriser un système de SIEM pour consolider les évènements de sécurité et la détection d'attaques, de comportements anormaux et des signaux faibles. • Connaître et distinguer les principaux outils de supervision. • Savoir identifier les objectifs attendus des solutions de supervision. • Savoir les mettre en production dans un cadre respectant les attendus en matière de sécurité.	★★★☆
ATTAQUES	• Être au fait des principaux vecteurs de compromission du moment, associés aux vulnérabilités découvertes. • Savoir réagir aux conséquences de l'exploitation de ces compromissions.	★★☆☆

COMPÉTENCE TRANSVERSALE • *SSI OPÉRATIONNELLE*

PROCESSUS DE DÉTECTION

Les processus et procédures de détection sont maintenus et testés pour assurer la prise de conscience des événements anormaux.

DÉTECTION	• Être en mesure de déployer et maintenir des outils de détection au sein d'un SI. • Connaître et savoir interpréter les relations entre un événement détecté et les menaces possibles associées.	★★★☆

PLAN D'INTERVENTION

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

Les processus et procédures d'intervention sont exécutés et maintenus pour garantir la réponse aux incidents de cybersécurité détectés.

GESTION DE CRISE	• Identifier les rôles et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cyber : l'ANSSI, le CERT-FR, Cybermalveillance.gouv.fr, la Gendarmerie nationale (le C3N, les NTECH), la Police nationale (la SDLC, l'OCLCTIC), la Préfecture de Police de Paris (BL2C) , etc.	★★★☆
RÉPONSE À INCIDENTS	• Identifier le vecteur de compromission et mesurer l'étendue de la compromission. • Savoir effectuer des relevés techniques sans modifier le SI existant. • Savoir rechercher des traces de compromission sur des systèmes actifs ou éteints. • Effectuer les opérations de réponse à incident sans destruction de données ou de traces. • Savoir identifier des Indicateurs de compromission. • Maîtriser le processus de remontée d'information auprès d'un CERT et les actions coordonnées. • Savoir documenter les actions réalisées afin de fournir un rapport d'incident détaillé.	★★★☆

COMMUNICATION

COMPÉTENCE TRANSVERSALE • *TRAVAIL EN ÉQUIPE*

Les activités d'intervention sont coordonnées avec les parties prenantes internes et externes (p. ex. avec le soutien des forces de l'ordre).

CONNAISSANCE JURIDIQUE ET RÉGLEMENTAIRE	• Connaître le principe de conservation des preuves en vue d'une analyse par les autorités.	★★☆☆
	• Connaître la procédure de dépôt de plainte auprès des autorités et des déclarations auprès de la CNIL.	★★☆☆

ANALYSE (1/2)

COMPÉTENCE MÉTIER • *INVESTIGATION NUMÉRIQUE*

Une analyse est menée pour assurer une intervention efficace et soutenir les activités de récupération.

IDENTIFICATION	• Savoir analyser et lier les événements trouvés pendant les opérations de réponse à incident. • Savoir orienter les recherches en fonction de ces remontées. • Maîtriser l'identification des vecteurs de compromission (MITTRE ATT&CK).	★★★☆
CONSERVATION DE LA PREUVE	• Maîtriser la collecte des preuves avec un système d'horodatage et de hashing sur un environnement sécurisé et sain (Fichiers, Mémoire, Disques Dur, E-mail) Norme ISO 27037. • Pouvoir mettre en œuvre un système de blocage en écriture physique ou logique.	★★★☆

Développer et mettre en œuvre des activités appropriées pour prendre des mesures concernant un incident de cybersécurité détecté.

ANALYSE (2/2)

COMPÉTENCE MÉTIER • *INVESTIGATION NUMÉRIQUE*

Une analyse est menée pour assurer une intervention efficace et soutenir les activités de récupération.

ANALYSE (RÉSEAUX, LOGS, OUTILS D'ANALYSE)	• Maîtriser l'analyse des journaux d'activités des équipements, des systèmes et des applications pour rechercher des compromissions.	★★★☆
ANALYSE MATÉRIELLE (CLIENT, SERVEUR)	• Maîtriser la collecte de la mémoire et des systèmes de stockage des serveurs et des clients (Snapshot VM).	★★★☆

ATTÉNUATION

COMPÉTENCE TRANSVERSALE • *POSTURE PERSONNELLE & SSI OPÉRATIONNELLE*

Les activités sont effectuées pour empêcher l'expansion d'un événement, atténuer ses effets et résoudre l'incident

ACCOMPAGNEMENT	• Savoir interagir avec les responsables pour respecter leurs contraintes opérationnelles sans répercussion sur la recherche de preuves. • Prendre en compte la dimension psychologique d'une crise chez les victimes (postures personnelles à adopter, prise en compte du stress…).	★★★☆
REMÉDIATION	• Savoir appliquer les mesures de remédiation adéquates en fonction des vecteurs de compromission détectés et de son étendue. • Maîtriser les procédures pour contenir les effets de l'attaque (segmentation d'urgence, fiche réflexe à jour, bascule en PRA et/ou application du PCA). • Connaître les conséquences opérationnelles de l'application de ces mesures.	★★★☆
	• Maîtriser la mise en place d'un système de contrôle renforcé des flux entrants et sortants ou l'isolation des différents SI.	★★★☆

AMÉLIORATION

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

Les activités de réponse organisationnelle sont améliorées en incorporant les leçons tirées des activités de détection/réponse actuelles et précédentes.

PROCÉDURE INTERNE	• Consolider ses propres connaissances pour améliorer les processus de réponses aux incidents et le partage des informations avec les acteurs de la SSI.	★★★☆

RÉPONDRE

Développer et mettre en œuvre des activités appropriées pour prendre des mesures concernant un incident de cybersécurité détecté.

Développer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience et pour restaurer les capacités ou les services qui ont été altérés en raison d'un incident de cybersécurité

COMPÉTENCE TRANSVERSALE • *SSI OPÉRATIONNELLE*

Les processus et procédures de récupération sont exécutés et maintenus pour garantir la restauration des systèmes ou des actifs affectés par des incidents de cybersécurité.

PLANIFICATION DE LA RÉCUPÉRATION

GESTION DE CRISE	• Participer à la mise en place de la cellule de crise en apportant, au besoin, des outils de communication et de partage d'information, indépendants du système attaqué. • Accompagner le client jusqu'à la sortie de crise. • S'assurer du bon fonctionnement des outils durant toute la durée de la crise. • Prendre en compte la dimension psychologique d'une crise chez les victimes (postures personnelles à adopter, prise en compte du stress…).
SAUVEGARDE	• Maîtriser le plan de restauration des sauvegardes dans un environnement sain ou assaini suivant les priorités liées à l'activités du client. • Effectuer les tâches de restauration et de récupération dans le respect des principes de sanctuarisation et des contraintes opérationnelles. • Savoir définir si les sauvegardes peuvent être considérées comme compromises ou de confiance dans le cadre d'une restauration complète ou partielle.
PCA / PRA	• Savoir définir et appliquer un PCA/PRA dans un contexte de crise. • Connaître les procédures de PCA et de PRA établies dans le contexte du client.

COMPÉTENCE TRANSVERSALE • *PILOTAGE DE LA SSI*

La planification et les processus de récupération sont améliorés en incorporant les leçons apprises dans les activités futures.

AMÉLIORATION

PROCÉDURE INTERNE	• Savoir évaluer le contenu et la pertinence des procédures PCA et PRA utilisées par le client pour amélioration. • Amender les procédures (clients et prestataires) utilisées pendant la crise en prenant en compte les difficultés observées et les optimisations envisagées dans le déroulement de la crise. • Être en capacité de valoriser les expériences issues d'une compromission pour améliorer les processus internes de décision et de gestion de crise mais également pour augmenter le niveau de sécurité global du client au regard des éléments recueillis pendant la réponse à incidents.
VEILLE TECHNO / EXPLOITATION, VULNÉRABILITÉS, MENACES	• Capitaliser sur les connaissances obtenues et les partager avec le CERT impliqué lors de la crise. • Mettre à jour les outils suivant les informations recueillies lors de l'analyse de l'attaque. • Connaître les principales sources d'information sur les vulnérabilités, être en capacité d'anticiper et de mesurer leur dangerosité en fonction d'un SI.

COMMUNICATION

Les activités de restauration sont coordonnées avec les parties internes et externes [p. ex. les centres de coordination, les fournisseurs d'accès Internet, les propriétaires de systèmes d'attaque, les victimes, les autres CSIRT et les fournisseurs].

COMPÉTENCE TRANSVERSALE • *TRAVAIL EN ÉQUIPE*

RELATION CLIENT	• Fournir aux clients les éléments techniques nécessaires pour assurer sa communication à destination de ses partenaires, de ses clients, des institutions, de la presse…
GESTION DE CRISE	• Aide à la construction d'un retour d'expérience partagé avec tous les partenaires impliqués lors de la crise (communication interne et externe adaptée en fonction des éléments de menace détectés et les conséquences prévisibles) .

RÉFÉRENCES

IDENTIFIER	**Connaissance des actifs physiques et logiciels**	• https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/ • https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/ • https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
	Environnement métier	• https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-protection-des-systemes-dinformation-essentiels/ • https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022L2555&qid=1673197235473&from=en
	Gouvernance	• https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-interministerielle-n-901/ • https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministe-rielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/ • https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/ • https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf
	Appréciation des risques	• https://www.ssi.gouv.fr/entreprise/principales-menaces/
	Gestion des risques de la chaîne d'approvisionnement	• https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management
PROTÉGER	**Gestion des identités et contrôle d'accès**	• https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite
	Sensibilisation et formation	• https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
	Processus et procédures de protection des informations	• https://www.ssi.gouv.fr/guide/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques/
RÉPONDRE	**Analyse**	• https://attack.mitre.org/matrices/enterprise/ • https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:fr
RÉTABLIR	**Planification de la récupération**	• https://www.iso.org/fr/standard/75106.html • http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf • https://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf
	Amélioration	• https://cert.ssi.gouv.fr/uploads/CERT-FR_RFC2350_EN.pdf
	Communication	• https://www.ssi.gouv.fr/guide/anticiper-et-gerer-sa-communication-de-crise-cyber/

REMERCIEMENTS

Ce Référentiel de Compétences Cyber pour les Prestataires (RCCP) est le fruit de la collaboration d'un groupe de travail réuni par Cybermalveillance.gouv.fr et composé du groupe AFNOR, du Campus régional de Cybersécurité et de Confiance numérique (C3NA) et du Centre de Formation de l'ANSSI (CFSSI).

GIP ACYMA
6 rue Bouchardon, 75010 Paris
www.cybermalveillance.gouv.fr

Suivez-nous sur :