

PARCOURS DE CYBERSÉCURITÉ

Prestataires terrain, mai 2021

Les Parcours de cybersécurité, une des réponses de l'ANSSI dans le cadre du volet cyber de France Relance



L'Agence nationale de la sécurité des systèmes d'information (ANSSI) pilote le volet cybersécurité de France Relance pour concevoir des offres de service destinées à élever le niveau de cybersécurité de l'État, des collectivités territoriales et des organismes au service des citoyens (social, santé, formation, audiovisuel, sécurité).

Accompagner les structures publiques dans la sécurisation des systèmes d'information...

Spécifiquement conçue par l'ANSSI, l'offre de service **Parcours de cybersécurité** constitue une réponse pragmatique et concrète aux besoins de mise à niveau du socle de cybersécurité des structures publiques.

Elle se base sur la modularité des services packagés permettant d'adapter la démarche à chaque bénéficiaire.

Chaque parcours s'articule autour de huit thèmes déclinés en fonction des enjeux de chaque bénéficiaire :

- Sensibilisation et organisation face au risque numérique
- Protection du réseau
- Maîtrise des accès au SI
- Intégration des enjeux de la sécurité numérique à la politique d'administration et d'exploitation
- Sécurisation des données, applications et services numériques
- Connaissance des vulnérabilités du SI
- Sécurisation des équipements de travail
- Capacité à détecter et à réagir aux évènements de sécurité

selon 4 parcours adaptés à leur contexte et leurs enjeux

Parcours Fondation

Adapté aux organisations disposant de ressources limitées (humaines, financières et techniques)

➔ Amorcer une démarche

Parcours Intermédiaire

Adapté aux organisations souhaitant recruter un référent en cybersécurité ou disposant en interne d'un référent junior à faire monter en compétence

➔ Se préparer à agir

Parcours Avancé

Adapté aux organisations qui disposent en interne et à temps plein d'un spécialiste en cybersécurité (ex : RSSI)

➔ Prendre les devants

Parcours Renforcé

Point de passage des organisations opérant un service de niveau comparable à celui d'un SI essentiel ou vital

➔ Prendre une longueur d'avance

Déroulement d'un parcours de cybersécurité



Pré-diagnostic

Sur la base d'un pré-diagnostic, l'ANSSI oriente le bénéficiaire vers le **parcours adapté à ses besoins et ses enjeux**. Elle établit les objectifs et le contenu du pack initial.

Le bénéficiaire contractualise alors avec **un ou plusieurs prestataire(s) terrain** de son choix pour lancer sa démarche de cybersécurité.



Pack initial

Le prestataire terrain est chargé de **dérouler les actions du pack initial**. En lien avec l'ANSSI, il **rédige un plan de sécurisation** formalisant et cadencant les mesures de cybersécurité à mettre en œuvre au sein de la structure bénéficiaire.

Un prestataire accompagnateur en **contact régulier avec l'ANSSI** assure un suivi de bout-en-bout du respect de la démarche, de la qualité des livrables et d'apport d'expertise si besoin.

L'ANSSI estime à l'issue du pack initial, l'**indice de cybersécurité** du bénéficiaire permettant de le positionner au sein de son parcours.



Pack(s) relais

L'accompagnement se poursuit avec des **prestations ciblées**. Le prestataire terrain met en œuvre des mesures de cybersécurité préalablement identifiées et met à jour le plan de sécurisation du bénéficiaire.

Interlocuteurs & outils à disposition



Des **livrables-types** permettant d'accélérer la mise en œuvre de la démarche et garantissant un **niveau homogène d'accompagnement**



Un **interlocuteur dédié**, expert de la démarche, **répondant à vos interrogations**, et en charge du suivi du bénéficiaire tout au long de son Parcours de cybersécurité



Un appui lors de la **co-rédaction du plan de sécurisation** et la définition du contenu du ou des pack relais.

Exemple d'un pack initial

Parcours Intermédiaire
Pour un conseil départemental
(1500 agents)

Etat des lieux organisationnel et plan de sécurisation

- Compréhension du contexte et des principaux enjeux
- Etat des lieux organisationnel et cartographie des zones de vulnérabilités
- Formalisation d'un plan de sécurisation adossé au parcours
- Sensibilisation et restitution aux dirigeants

Sensibilisation

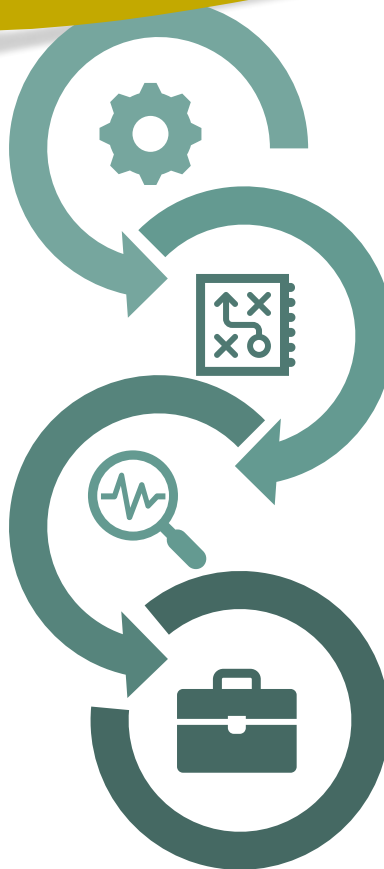
- Sensibilisation des administrateurs du système d'information
- Sensibilisation des équipes du service Achats

Etat des lieux technique

- Scans automatisés internes en boîte noire avec validation manuelle des vulnérabilités critiques et formalisation des constats
- Moins de 200 IP internes

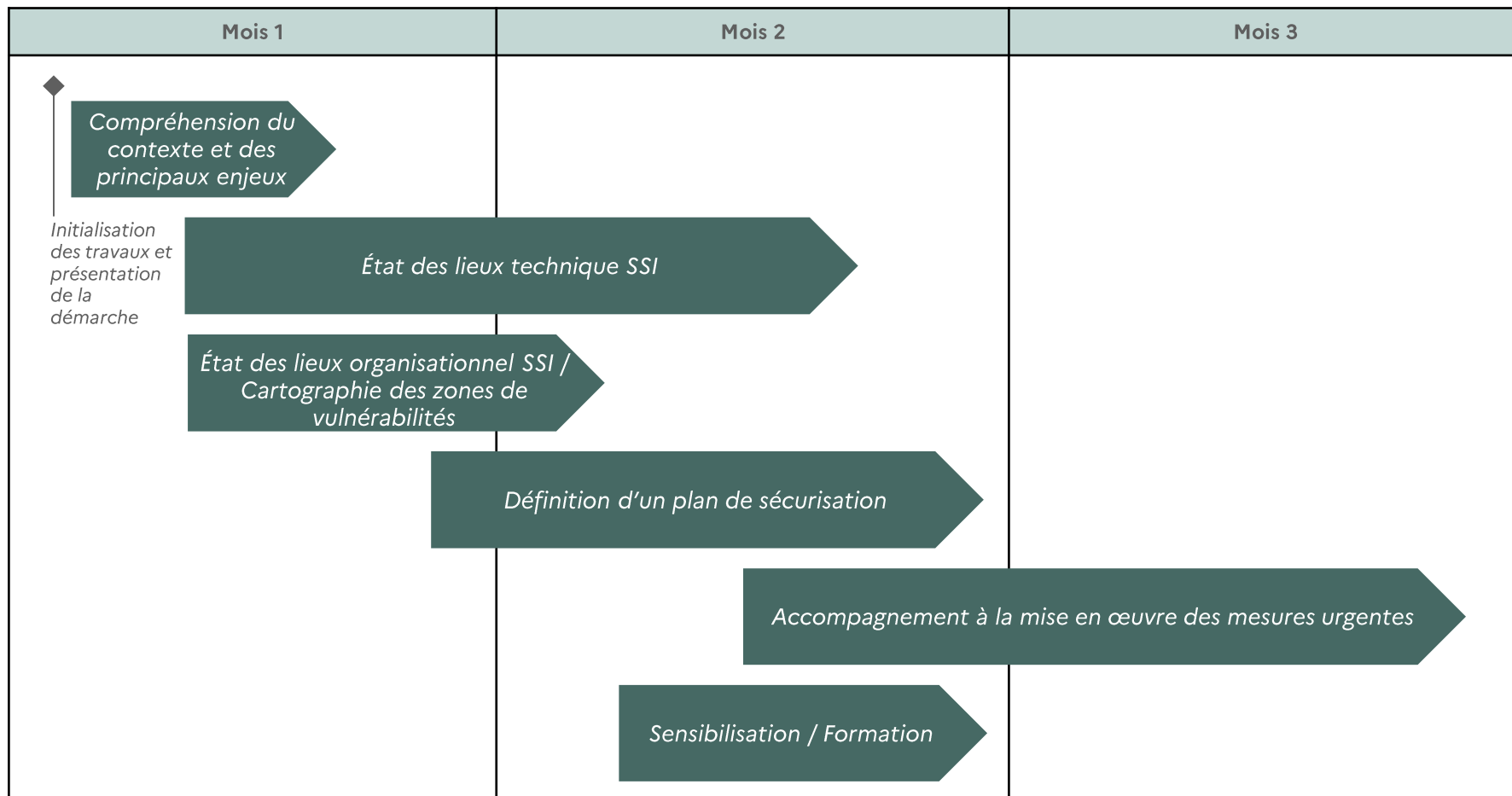
Accompagnement MOE

- Accompagnement à la mise en œuvre des mesures urgentes de sécurisation opérationnelle



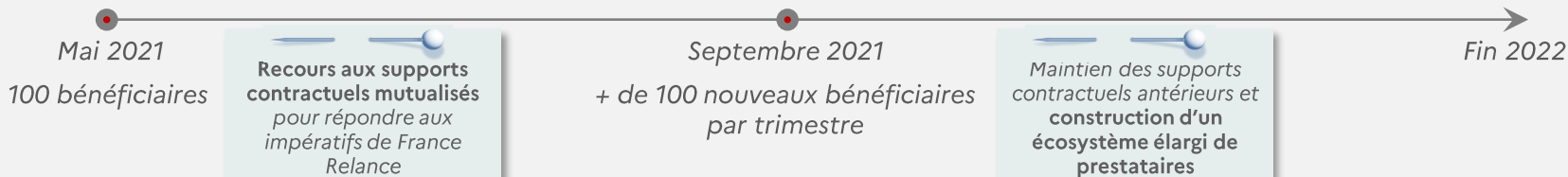
Les prestations des Parcours de cybersécurité sont adaptées en fonction des enjeux, des besoins et de la taille de la structure publique bénéficiaire.

Exemple calendaire d'un pack initial



Devenir prestataire terrain

Calendrier de mise en œuvre



Profil et compétences attendues

Les prestataires terrain disposent des compétences nécessaires pour accompagner les bénéficiaires au plus près du terrain, conformément à l'ambition du plan de relance.

Ils interviennent sur des missions de gouvernance, d'audit et de sécurité opérationnelle.



Contractualisation

Le bénéficiaire choisit son ou ses prestataire(s) terrain grâce aux différents vecteurs contractuels à sa disposition et qui peuvent lui être suggérés par l'ANSSI. S'il le souhaite, il peut procéder à son propre processus de contractualisation tel qu'un marché à procédure adaptée (MAPA) ou de gré-à-gré.

Les engagements du prestataire terrain



Réaliser des livrables de qualité conformément aux attendus des cadrages des pack initiaux et relais



Faire des retours réguliers à l'ANSSI et au prestataire accompagnateur sur le déroulement du parcours et l'évolution du bénéficiaire



Définir un cadre de pilotage et des modes de fonctionnement « projet » avec l'organisation de la réunion de lancement et de restitution notamment



Accompagner le bénéficiaire dans une logique pérenne et une vision à long terme

ANNEXE



OBJECTIFS OPÉRATIONNELS À L'ISSUE DES PARCOURS

Annexe | Objectifs opérationnels à l'issue des parcours*



	A l'issue du parcours Fondation	A l'issue du parcours Intermédiaire	A l'issue du parcours Avancé	A l'issue du parcours Renforcé
<p>1. Je m'organise et je sensibilise face au risque numérique</p>	<ul style="list-style-type: none"> • Ma structure a un référent à la sécurité des systèmes d'informations (SSI), désigné par la direction et identifié comme tel par les agents et formé à la SSI • Je sensibilise mon équipe dirigeante aux risques numériques et elle est un soutien actif de la démarche de sécurisation • Je sensibilise l'ensemble des agents aux risques liés au phishing (courriels piégés) • Je sensibilise et réalise des actions de formation aux problématiques et bonnes pratiques de la SSI pour les acteurs à privilèges de la DSI (exploitation, assistance,...) • J'ai identifié mes principaux fournisseurs de services numériques et je leur impose des clauses SSI adaptées en fonction des prestations menées • Je pilote et je mets en œuvre les recommandations de mes audits à l'aide d'un plan de sécurisation 	<ul style="list-style-type: none"> • Ma structure a un responsable de la SSI (RSSI) à temps plein • J'ai une politique SSI (PSSI), validée par la direction • Je connais les principales zones de risques de mon infrastructure et de mon écosystème SI • Je sensibilise l'ensemble des agents aux risques numériques au moins une fois par an • Je réalise des tests de phishing régulièrement • Je mets en place des moyens d'encadrement renforcés des prestations (p. ex. Plan d'Assurance Sécurité, audits) • J'ai formalisé une charte applicable aux utilisateurs que ces derniers ont ensuite signée 	<ul style="list-style-type: none"> • Ma structure dispose de ressources dédiées à la sécurité opérationnelle • J'ai formalisé et attribué l'ensemble des responsabilités internes et externes (prestataires, partenaires, etc.) à l'égard de la SSI • J'ai un référentiel documentaire • J'applique un processus maîtrisé de gestion des dérogations/exceptions • Je dispose d'un comité régulier de pilotage des risques numériques auquel participe la direction • Je mène des actions structurées et récurrentes de sensibilisation et de formation aux risques numériques et je vérifie l'efficacité de mes campagnes 	<ul style="list-style-type: none"> • Ma structure a positionné le RSSI à un niveau hiérarchique proche du niveau décisionnel • Je définis mes orientations stratégiques en matière de sécurité et les décline sous la forme d'une feuille de route pluriannuelle, validée par la direction • Je détecte les écarts à la PSSI et met en œuvre des actions d'amélioration • Je mesure l'efficacité de mes démarches de sécurisation à l'aide d'un nombre maîtrisé d'indicateurs

*Référentiel susceptible d'évoluer dans le cadre de l'amélioration continue du dispositif

Annexe | Objectifs opérationnels à l'issue des parcours*


	A l'issue du parcours Fondation	A l'issue du parcours Intermédiaire	A l'issue du parcours Avancé	A l'issue du parcours Renforcé
 <p>2. Je maîtrise les accès à mon système d'information</p>	<ul style="list-style-type: none"> J'utilise un outil de gestion centralisée d'identification et d'authentification (p. ex. AD) J'identifie nommé-ment chaque utilisateur accédant au système (absence de compte générique) Je mets en œuvre des dispositifs garantissant la robustesse des mots de passe utilisés J'utilise des mécanismes d'authentification pour protéger les accès à mon SI depuis l'extérieur 	<ul style="list-style-type: none"> Je dispose de procédures de gestion des habilitations liées au cycle de vie des agents (arrivée, départ, changement de fonction, etc.) Je sécurise le stockage des mots de passe ou de leurs hashes 	<ul style="list-style-type: none"> J'attribue les droits d'accès aux ressources sensibles du SI selon les principes du moindre privilège et en évitant les combinaisons toxiques Je revois les comptes et les droits d'accès de mes périmètres les plus sensibles annuellement J'ai généralisé l'authentification forte sur les périmètres les plus sensibles Je n'autorise la connexion au réseau de l'entité qu'aux seuls équipements maîtrisés 	<ul style="list-style-type: none"> Je revois l'ensemble de mes comptes et droits d'accès annuellement Je favorise les dispositifs limitant le nombre d'authentifiants utilisés par les agents (p. ex. SSO)
 <p>3. Je sécurise mes données, mes applications et services numériques</p>	<ul style="list-style-type: none"> Je dispose d'une cartographie de mes services les plus sensibles au regard de leurs besoins de sécurité et les plus vulnérables par rapport à leur exposition aux menaces J'ai mis en place des mesures de protection de la messagerie professionnelle J'ai mis en place des mesures de protection des services exposés sur Internet (p. ex. serveur mandataire inverse / reverse proxy) 	<ul style="list-style-type: none"> J'intègre la sécurité dans tout le cycle de vie de mes projets SI (étude d'opportunité, architecture, recette, production, fin de vie...) Je mets en œuvre des principes de développement sécurisé dans mes projets SI J'utilise des protocoles sécurisés pour les flux de données applicatifs dès qu'ils sont pertinents J'utilise des solutions de chiffrement (p. ex. conteneur chiffré) lorsque je transmets des données non structurées (p. ex. fichiers) sensibles via Internet J'applique une politique efficace de mise à jour de sécurité pour les applications 	<ul style="list-style-type: none"> J'homologue mes nouveaux SI sensibles Je contrôle le niveau de sécurité des projets les plus sensibles (p. ex. audit, scan, revue de code, etc.) avant leur mise en production Je protège mes applications exposées les plus sensibles contre les attaques au niveau applicatif (p. ex. utilisation d'un WAF) Je mets en œuvre un dispositif adapté d'effacement sécurisé des supports de données (en cas de dé-commissionnement, de maintenance matérielle, etc.) 	<ul style="list-style-type: none"> Je dispose d'une cartographie des données de mon SI J'ai homologué tous mes SI sensibles Je contrôle régulièrement le niveau de sécurité des SI les plus sensibles (p. ex. audit, scan, revue de code, etc.) après leur mise en production J'ai déployé et configuré des dispositifs permettant de bloquer les ressources infiltrées (p. ex. sandboxing) ou exfiltrées du SI (p. ex. Data Loss Prevention - DLP) Je sécurise les fichiers et bases de données les plus sensibles qui le nécessitent ainsi que leurs sauvegardes (p. ex. DRM/gestion des droits numériques, chiffrement, etc.)

Annexe | Objectifs opérationnels à l'issue des parcours*

	A l'issue du parcours Fondation	A l'issue du parcours Intermédiaire	A l'issue du parcours Avancé	A l'issue du parcours Renforcé
 <p>4. Je sécurise mes équipements de travail</p>	<ul style="list-style-type: none"> J'ai inventorié l'ensemble de mes postes de travail et équipements mobiles J'ai déployé et configuré des solutions de protection sur les postes de travail (p. ex. anti-virus, pare-feu local) J'applique une politique efficace de mise à jour de sécurité pour les postes de travail 	<ul style="list-style-type: none"> J'ai renforcé la configuration de mes terminaux/postes de travail pour limiter leur surface d'exposition J'ai mis en œuvre une solution de gestion centralisée des téléphones mobiles (p. ex. MDM) J'ai mis en œuvre les bonnes pratiques liées à la configuration et l'usage de mes imprimantes et copieurs multifonctions 	<ul style="list-style-type: none"> Je limite au strict besoin opérationnel les droits d'administration sur les postes de travail J'ai chiffré les terminaux/postes de travail nomades contenant des données sensibles J'ai déployé et configuré des dispositifs permettant de détecter et investiguer des intrusions sur mon poste de travail (p. ex. Endpoint Détection and Response (EDR), IPS ,etc.) 	<ul style="list-style-type: none"> J'ai formalisé une charte dédiée à l'usage des équipements mobiles
 <p>5. Je protège mon réseau</p>	<ul style="list-style-type: none"> Je dispose d'une cartographie de mon réseau et de ses interconnexions avec mes partenaires et prestataires J'ai mis en place une protection des réseaux d'accès Wi-Fi (accès par compte nominatif, certificats, etc.) et j'ai mis en place une séparation des usages (interne, invité, etc.) J'ai déployé et configuré une passerelle d'accès sécurisé à Internet (p. ex. proxy) J'ai cloisonné les ressources visibles depuis Internet du reste du système d'information Je filtre les flux réseaux vers mes partenaires et prestataires La connexion des postes nomades à mon SI se fait au travers de connexions réseaux sécurisées (p. ex. VPN) 	<ul style="list-style-type: none"> J'ai défini des zones réseau selon la sensibilité de leur contenu et mis en place des dispositifs de filtrage / segmentation entre celles-ci 	<ul style="list-style-type: none"> J'ai sécurisé les interconnexions réseau dédiées avec des tiers (p. ex. partenaires, prestataires, etc.) Je définis clairement et je tiens à jour les règles de filtrage des flux implémentées J'ai mis en place une protection contre les attaques par déni de service (DDOS) 	<ul style="list-style-type: none"> Je cloisonne physiquement ou logiquement les SI les plus sensibles vis-à-vis des autres systèmes d'information internes ou tiers J'ai déployé et configuré des sondes (p. ex. IDS, IPS) permettant de détecter ou bloquer les événements suspects sur mon réseau



*Référentiel susceptible d'évoluer dans le cadre de l'amélioration continue du dispositif

Annexe | Objectifs opérationnels à l'issue des parcours*

	A l'issue du parcours Fondation	A l'issue du parcours Intermédiaire	A l'issue du parcours Avancé	A l'issue du parcours Renforcé
 <p>6. J'intègre les enjeux de la sécurité numérique à ma politique d'administration et d'exploitation</p>	<ul style="list-style-type: none"> • Je dispose d'un inventaire exhaustif et à jour des comptes à privilèges, qui sont distincts des comptes utilisateurs • J'ai déployé un dispositif d'authentification pour tout accès aux ressources de mon SI et j'ai changé les éléments d'authentification par défaut • J'utilise des protocoles sécurisés pour mes flux d'administration • J'ai déployé et configuré des solutions de protection contre les codes malveillants (p. ex. anti-virus) sur les serveurs qui le nécessitent (p. ex. non recommandé sur un AD) • J'applique une politique efficace de mise à jour de sécurité pour les infrastructures • J'anticipe la fin de la maintenance des logiciels et systèmes • Je prends en compte les enjeux de sécurité dans l'identification des périmètres éligibles au Cloud (IaaS/PaaS/SaaS) • J'ai un dispositif de sauvegarde opérationnel et mes sauvegardes sont stockées indépendamment du reste du SI 	<ul style="list-style-type: none"> • Je dispose d'une cartographie de l'infrastructure de mon SI • J'ai renforcé la configuration de l'ensemble de mes serveurs/infrastructures pour limiter la surface d'exposition des services d'administration • Je maîtrise l'activité des comptes de service utilisés par les machines • Je définis et j'applique systématiquement des configurations de sécurité dans mes services Cloud (IaaS/PaaS) • Je contrôle et protège l'accès physique aux salles serveurs et aux locaux techniques • J'ai formalisé une charte applicable aux utilisateurs à privilèges de la DSI que ces derniers ont ensuite signée • J'ai déployé des dispositifs afin d'augmenter la disponibilité de mes ressources les plus sensibles (p. ex. cluster) • Je suis en capacité de restaurer rapidement mes services d'infrastructure critiques (AD-DNS-DHCP-Console AV-SCCM- ...) en cas de besoin 	<ul style="list-style-type: none"> • J'utilise un réseau logique dédié et cloisonné pour l'administration du système d'information, déconnecté d'Internet • J'attribue les droits administrateurs dans le respect du principe du moindre privilège • Je centralise et je trace les accès des administrateurs (p. ex. serveur de rebond, bastion, etc.) • Je teste régulièrement mes sauvegardes • J'ai un Plan de Reprise d'Activité (PRA) en cas de sinistre physique de mon centre informatique, couvrant mes ressources les plus sensibles et testé annuellement 	<ul style="list-style-type: none"> • J'ai déployé et configuré des dispositifs permettant de détecter et investiguer des intrusions sur mes serveurs (p. ex. IPS, EDR) • J'automatise les fonctionnalités de sécurité dans le cadre de mes déploiements d'infrastructure dans le cloud (IaaS/PaaS) • J'ai un Plan de Reprise d'Activité (PRA) en cas de cyberattaque, couvrant mes ressources les plus sensibles et testé annuellement

*Référentiel susceptible d'évoluer dans le cadre de l'amélioration continue du dispositif

Annexe | Objectifs opérationnels à l'issue des parcours*

	A l'issue du parcours Fondation	A l'issue du parcours Intermédiaire	A l'issue du parcours Avancé	A l'issue du parcours Renforcé
 <p>7. Je connais les vulnérabilités de mon système d'information</p>	<ul style="list-style-type: none"> Je réalise des scans de vulnérabilité de mon SI exposé sur Internet Je mène un audit organisationnel adapté à mon niveau de maturité 	<ul style="list-style-type: none"> Je réalise des scans de vulnérabilité de tout mon SI Je réalise un audit régulier de mon système de gestion centralisé d'identification et d'authentification 	<ul style="list-style-type: none"> Je réalise des tests d'intrusion de mes SI exposés sur Internet 	<ul style="list-style-type: none"> Je mets en œuvre annuellement des plans de contrôle et d'audit Je réalise des scans de vulnérabilité en continu Je réalise un audit red team
 <p>8. Je sais détecter les événements de sécurité et y réagir</p>	<ul style="list-style-type: none"> Je dispose d'une fiche réflexe en cas d'incident 	<ul style="list-style-type: none"> J'ai activé les principaux journaux d'évènements de mes équipements de sécurité et de mon système de gestion centralisée d'identification et d'authentification et les ai centralisés dans un espace dédié indépendant de ces SI J'ai une procédure formelle de gestion des incidents de sécurité J'ai défini et testé une procédure d'arrêt d'urgence de mon SI en cas de sinistre 	<ul style="list-style-type: none"> J'ai activé les principaux journaux d'évènements pour les applications et infrastructures les plus sensibles, et les ai centralisés dans un espace dédié indépendant de ces SI J'utilise les moyens de détection natifs des équipements de sécurité déjà déployés afin de générer des alertes pour les principaux incidents redoutés J'ai défini un processus de gestion de crise cyber, testé annuellement 	<ul style="list-style-type: none"> J'ai systématiquement activé les principaux journaux d'évènements de la majorité de mes composants, et les ai centralisés dans un espace dédié indépendant de ces SI J'ai mis en place une solution d'analyse de mes journaux d'évènements (p. ex. SIEM) afin de générer des alertes en accord avec une stratégie de détection J'ai mis en place une équipe pour analyser en permanence les évènements de sécurité et réagir si nécessaire (SOC) J'ai mis en place une équipe d'experts en cybersécurité disponible 24/7 en cas de sinistre

*Référentiel susceptible d'évoluer dans le cadre de l'amélioration continue du dispositif