CyFun®

BASE

CyberFondamentaux 2023

Version 2023-03-01

TABLE DES MATIÈRES

INTRODUCTION

Le **cadre des cyberfondamentaux du CCB** est un ensemble de mesures concrètes pour :

- protéger les données,
- réduire considérablement le risque des cyberattaques les plus courantes,
- accroître la cyber-résilience d'une organisation.

Les exigences et les lignes directrices sont complétées par les idées pertinentes incluses dans le cadre NIST/CSF, l'ISO 27001/ISO 27002, la CEI 62443 et les contrôles de sécurité critiques CIS (ETSI TR 103 305-1).

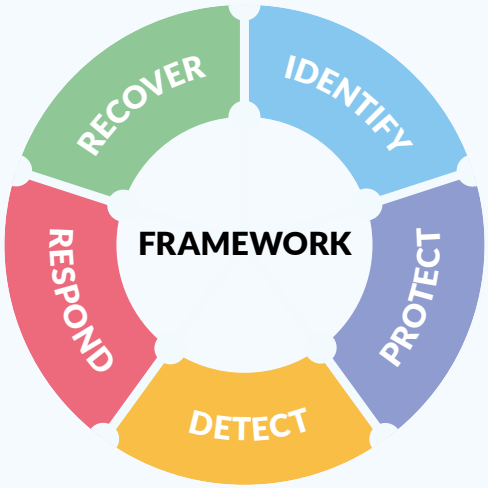
Le codage des exigences correspond aux codes utilisés dans le cadre NIST CSF. Comme toutes les exigences du NIST CSF ne sont pas applicables, certains codes qui existent dans le cadre NIST CSF peuvent manquer.

Le cadre et l'approche proportionnelle des niveaux d'assurance sont validés par des praticiens sur le terrain et à l'aide d'informations anonymes sur les cyberattaques du monde réel fournies par la Cyber Emergency Response Team fédérale (CERT.be - le service opérationnel du Centre pour la cybersécurité en Belgique).

Le **cadre des cyberfondamentaux du CCB** s'articule autour de cinq fonctions essentielles : identifier, protéger, détecter, répondre et rétablir. Ces fonctions permettent, quels que soient l'organisation et le secteur d'activité, de promouvoir la communication autour de la cybersécurité entre les praticiens techniques et les parties prenantes afin que les risques liés à la cybernétique puissent être intégrés dans la stratégie globale de gestion des risques de l'organisation.

Identifier (Identify)

Connaître les principales cybermenaces qui pèsent sur vos actifs les plus précieux. Essentiellement, vous ne pouvez pas protéger ce dont vous ignorez l'existence. Cette fonction aide à développer une compréhension organisationnelle de la manière de gérer les risques de cybersécurité liés aux systèmes, aux personnes, aux actifs, aux données et aux capacités.



Protéger (Protect)

La fonction de protection se concentre sur l'élaboration et la mise en œuvre des mesures de protection nécessaires pour atténuer ou contenir un cyberrisque.

Détecter (Detect)

L'objectif de la fonction Détecter est d'assurer la détection en temps utile des événements de cybersécurité.

Répondre (Respond)

La fonction de réponse concerne les contrôles qui permettent de répondre aux incidents de cybersécurité. La fonction de réponse soutient la capacité à contenir l'impact d'un incident de cybersécurité potentiel.

Rétablir (Recover)

La fonction de rétablissement se concentre sur les mesures de protection qui contribuent à maintenir la résilience et à restaurer les services qui ont été affectés par un incident de cybersécurité.

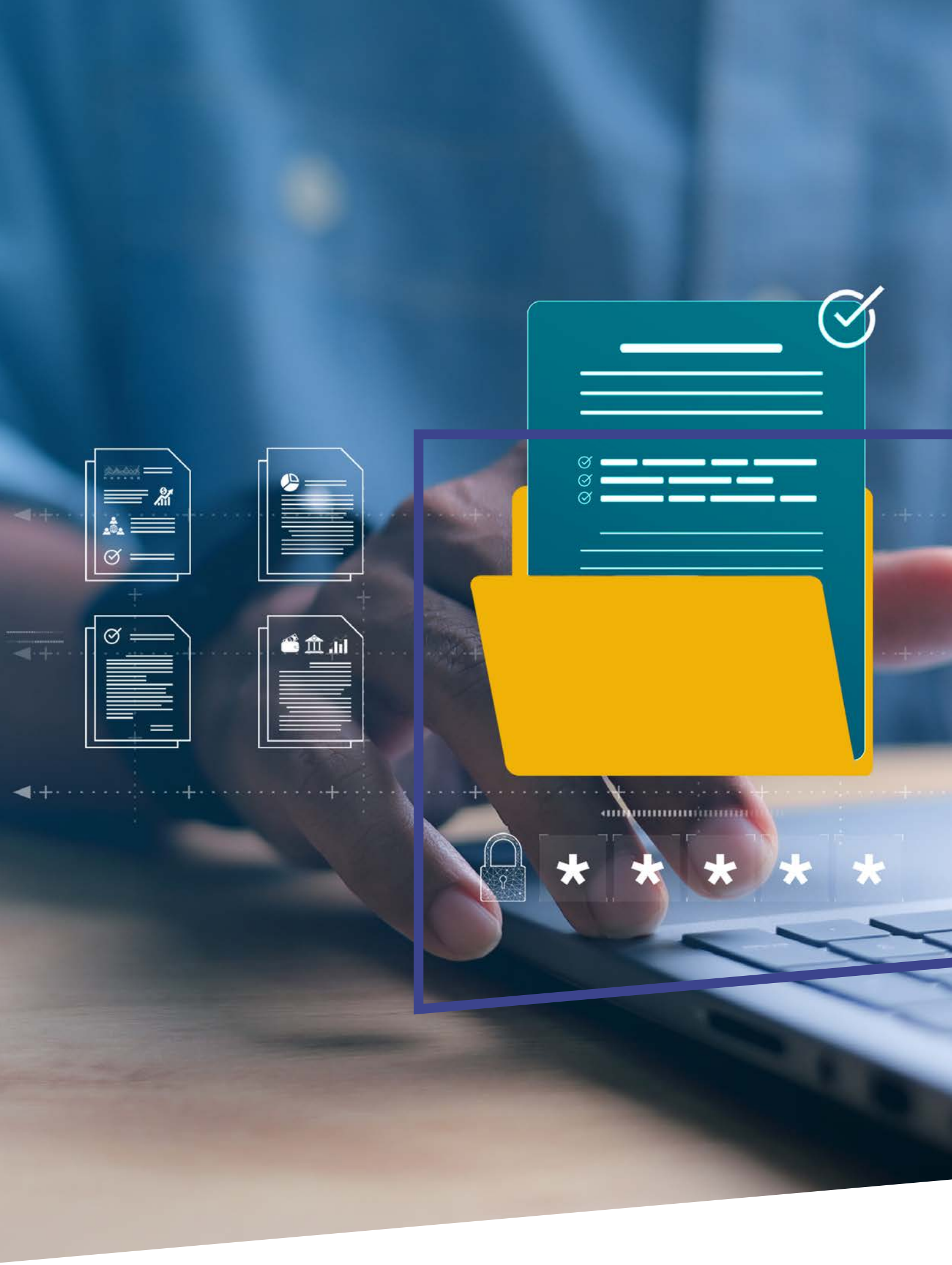
Pour répondre à la gravité de la menace à laquelle une organisation est exposée, en plus du niveau de départ ***Small***, 3 niveaux d'assurance sont proposés : ***Basique, Important et Essentiel***.

Le **niveau de départ *Small*** permet à une organisation de faire une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées.

Le **niveau d'assurance *Basic*** contient les mesures de sécurité de l'information standard pour toutes les organisations. Celles-ci fournissent une valeur de sécurité efficace avec des technologies et des processus qui sont généralement déjà disponibles. Lorsque cela est justifié, les mesures sont adaptées et affinées.

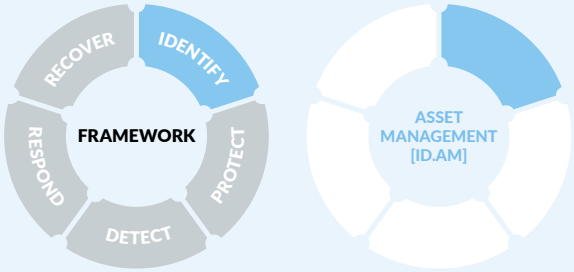
Plusieurs contrôles requièrent une attention particulière ; ces mesures sont étiquetées comme **mesure clé** .

Le cadre est un document vivant et continuera d'être mis à jour et amélioré en tenant compte des commentaires reçus des parties prenantes, de l'évolution du risque de menaces spécifiques de cybersécurité, de la disponibilité des solutions techniques et de la perspicacité progressive.



IDENTIFIER

Identify



Les données, le personnel, les dispositifs, les systèmes et les installations qui permettent à l'organisation d'atteindre ses objectifs opérationnels sont identifiés et gérés en fonction de leur importance relative par rapport aux objectifs de l'organisation et à sa stratégie en matière de risques.

ID.AM-1 Les dispositifs et systèmes physiques utilisés dans l'organisation sont inventoriés.

Un inventaire des actifs associés aux informations et aux installations de traitement de l'information au sein de l'organisation doit être documenté, examiné et mis à jour lorsque des changements surviennent.

Orientation

- Cet inventaire comprend des ordinateurs fixes et portables, des tablettes, des téléphones mobiles, des contrôleurs logiques programmables (PLC), des capteurs, des actionneurs, des robots, des machines-outils, des micrologiciels, des switchs, des routeurs, des alimentations et d'autres composants ou dispositifs en réseau.
- Cet inventaire doit inclure tous les actifs, qu'ils soient ou non connectés au réseau de l'organisation.
- L'utilisation d'un outil de gestion des actifs informatiques pourrait être envisagée.

ID.AM-2 Les plateformes et applications logicielles utilisées au sein de l'organisation sont inventoriées.

Un inventaire reflétant les plateformes et les applications logicielles utilisées dans l'organisation doit être documenté, révisé et mis à jour lorsque des changements surviennent.

Orientation

- Cet inventaire comprend les programmes logiciels, les plateformes logicielles et les bases de données, même s'ils sont externalisés (SaaS).
- Il convient que les accords d'externalisation fassent partie des accords contractuels avec le fournisseur.
- Il convient que les informations de l'inventaire comprennent par exemple : le nom, la description, la version, le nombre d'utilisateurs, les données traitées, etc.
- Il convient de faire la distinction entre les logiciels non pris en charge et les logiciels non autorisés.
- L'utilisation d'un outil de gestion des actifs informatiques pourrait être envisagée.

ID.AM-3 La communication organisationnelle et les flux de données sont schématisés.

Les informations que l'organisation stocke et utilise doivent être identifiées.

Orientation

- Commencez par énumérer tous les types d'informations que votre organisation stocke ou utilise. Définissez le "type d'information" de toute manière utile et logique pour votre organisation. Vous pouvez demander à vos employés de dresser une liste de toutes les informations qu'ils utilisent dans le cadre de leurs activités habituelles. Dressez une liste de tout ce à quoi vous pouvez penser, mais il n'est pas nécessaire d'être trop précis. Par exemple, vous pouvez conserver les noms et adresses électroniques de vos clients, les reçus de matières premières, vos informations bancaires ou d'autres informations exclusives.
- Envisagez de mettre en correspondance ces informations avec les actifs associés identifiés dans les inventaires des dispositifs physiques, des systèmes, des plateformes logicielles et des applications utilisés au sein de l'organisation (voir ID.AM-1 & ID.AM-2).

ID.AM-4 Les systèmes d'information externes sont catalogués.

Aucune exigence n'est identifiée pour le niveau d'assurance "Basic", mais des lignes directrices sont fournies pour renforcer la sécurité des informations.

Orientation

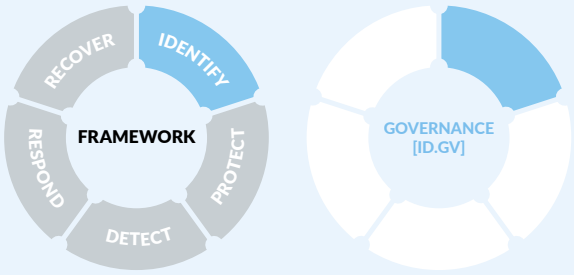
L'externalisation des systèmes, des plates-formes logicielles et des applications utilisés au sein de l'organisation est couverte par ID.AM-1 et ID.AM-2.

ID.AM-5 Les ressources sont organisées par ordre de priorité en fonction de leur classification, de leur criticité et de leur valeur opérationnelle.

Les ressources de l'organisation (matériel, dispositifs, données, temps, personnel, informations et logiciels) doivent être organisées par ordre de priorité en fonction de leur classification, de leur criticité et de leur valeur opérationnelle.

Orientation

- Déterminer les ressources de l'organisation (par exemple, le matériel, les dispositifs, les données, le temps, le personnel, les informations et les logiciels) :
  - Qu'arriverait-il à mon organisation si ces ressources étaient rendues publiques, endommagées, perdues... ?
  - Qu'arriverait-il à mon organisation lorsque l'intégrité des ressources ne serait plus garantie ?
  - Qu'arriverait-il à mon organisation si mes clients ou moi-même ne pouvions pas accéder à ces ressources ? Et organisez ces ressources en fonction de leur classification, de leur criticité et de leur valeur opérationnelle.
- Il convient que les ressources incluent les actifs de l'organisation.



Les politiques et procédures de gestion et de suivi des exigences réglementaires, juridiques, de risque, environnementales et opérationnelles de l'organisation sont comprises et éclairent la gestion du risque de cybersécurité.

ID.GV-1 La politique de cybersécurité de l'organisation est établie et communiquée.

Les politiques et procédures en matière de sécurité de l'information et de cybersécurité doivent être créées, documentées, examinées, approuvées et mises à jour lorsque des changements interviennent.

Orientation

- Les politiques et les procédures qui servent à identifier les pratiques et les attentes acceptables en matière d'opérations, peuvent être utilisées pour former les nouveaux employés à vos attentes en matière de sécurité de l'information et peuvent faciliter une enquête en cas d'incident. Il convient que ces politiques et procédures soient facilement accessibles aux employés.
- Il convient que les politiques et procédures en matière de sécurité de l'information et de cybersécurité décrivent clairement vos attentes en matière de protection des informations et des systèmes de l'organisation, ainsi que la manière dont la direction s'attend à ce que les ressources de l'organisation soient utilisées et protégées par tous les employés.

Il convient que les politiques et procédures soient revues et mises à jour au moins une fois par an et à chaque fois que des changements interviennent dans l'organisation ou la technologie. Chaque fois que les politiques sont modifiées, il convient d'informer les employés des changements.

ID.GV-3 Les exigences légales et réglementaires en matière de cybersécurité, y compris les obligations relatives à la vie privée et aux libertés civiles, sont comprises et gérées.

Les exigences légales et réglementaires en matière de sécurité de l'information/cybersécurité, y compris les obligations en matière de respect de la vie privée, doivent être comprises et appliquées.

Orientation

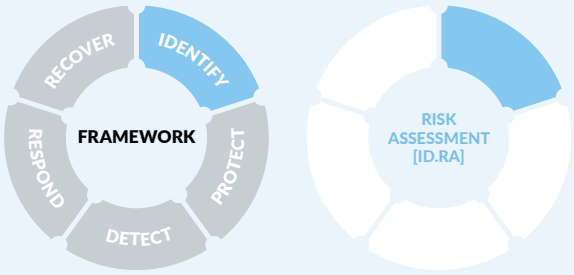
Il n'y a pas de directives supplémentaires.

ID.GV-4 Les processus de gouvernance et de gestion des risques traitent les risques liés à la cybersécurité.

Dans le cadre de la gestion globale des risques de l'organisation, une stratégie complète de gestion des risques liés à la sécurité de l'information et à la cybersécurité doit être élaborée et mise à jour lorsque des changements surviennent.

Orientation

Il convient que cette stratégie inclue la détermination et l'affectation des ressources nécessaires à la protection des actifs critiques de l'organisation.



L'organisation comprend le risque de cybersécurité pour les opérations de l'organisation (y compris la mission, les fonctions, l'image ou la réputation), ses actifs et les individus.

ID.RA-1 Les vulnérabilités des actifs sont identifiées et documentées.

Les menaces et les vulnérabilités doivent être identifiées.

Orientation

- Une vulnérabilité fait référence à une faiblesse dans le matériel, les logiciels ou les procédures de l'organisation. Il s'agit d'une faille par laquelle un acteur malveillant peut accéder aux actifs de l'organisation. Une vulnérabilité expose une organisation à des menaces.
- Une menace est un événement malveillant ou négatif qui tire parti d'une vulnérabilité.
- Le risque est le potentiel de perte et de dommage lorsque la menace se concrétise.

ID.RA-5 Les menaces, les vulnérabilités, les probabilités et les impacts sont utilisés pour déterminer les risques.

L'organisation doit effectuer des évaluations des risques dans lesquelles le risque est déterminé par les menaces, les vulnérabilités et l'impact sur les processus et les actifs de l'organisation.

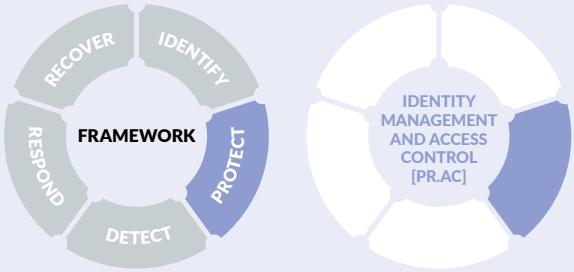
Orientation

- N'oubliez pas que les menaces exploitent les vulnérabilités.
- Identifier les conséquences que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs et les processus opérationnels connexes.


Username
Password
Remember me
Protected
Balance:
5.367.50 $

PROTÉGER

Protect



L'accès aux actifs physiques et logiques et aux installations associées est limité aux utilisateurs, processus et dispositifs autorisés, et est géré en fonction du risque évalué d'accès non autorisé aux activités et transactions autorisées.

PR.AC-1 Les identités et les identifiants sont émis, gérés, vérifiés, révoqués et audités pour les dispositifs, utilisateurs et processus autorisés.

Les identités et les identifiants des dispositifs et des utilisateurs autorisés doivent être gérés.

Orientation

Les identités et les identifiants des dispositifs et des utilisateurs autorisés peuvent être gérées par une politique de mot de passe. Une politique de mot de passe est un ensemble de règles destinées à renforcer la sécurité des TIC/OT en encourageant l'organisation à (liste non limitative et mesures à envisager le cas échéant) :

- Changez tous les mots de passe par défaut.
- Veillez à ce que personne ne travaille avec des privilèges d'administrateur pour les tâches quotidiennes.
- Conservez une liste limitée et mise à jour des comptes d'administrateur système.
- Appliquer les règles relatives aux mots de passe, par exemple, les mots de passe doivent être plus longs qu'un nombre de caractères adéquat avec une combinaison de types de caractères et être changés périodiquement ou lorsqu'il y a un soupçon de compromission.
- N'utilisez que des comptes individuels et ne partagez jamais vos mots de passe.
- Désactiver immédiatement les comptes inutilisés
- Les droits et les privilèges sont gérés par des groupes d'utilisateurs.

PR.AC-2 L'accès physique aux actifs est géré et protégé.

L'accès physique à l'installation, aux serveurs et aux composants du réseau doit être géré.

Orientation

- Envisagez de gérer strictement les clés d'accès aux locaux et les codes d'alarme. Il convient de prendre en compte les règles suivantes :
  - Récupérez toujours les clés ou les badges d'un employé lorsqu'il quitte définitivement l'organisation.
  - Changez fréquemment les codes d'alarme de l'organisation.
  - Ne jamais donner de clés ou de codes d'alarme à des prestataires extérieurs (agents de nettoyage, etc.), sauf s'il est possible de tracer ces accès et de les limiter techniquement à des plages horaires données.
- Envisagez de ne pas laisser les prises d'accès au réseau interne accessibles dans les lieux publics. Ces lieux publics peuvent être des salles d'attente, des couloirs...

PR.AC-3 L'accès à distance est géré.

Les points d'accès sans fil de l'organisation doivent être sécurisés.

Orientation

Tenez compte des éléments suivants lorsque vous utilisez un réseau sans fil :

- Changez le mot de passe administratif lors de l'installation d'un point d'accès sans fil.
- Configurez le point d'accès sans fil de manière à ce qu'il ne diffuse pas son identifiant (SSID).
- Configurez votre routeur pour qu'il utilise au moins le WiFi Protected Access (WPA-2 ou WPA-3 si possible), avec la norme de cryptage avancée (AES) pour le cryptage.
- Veillez à ce que l'accès Internet sans fil des clients soit séparé du réseau de votre organisation.
- Il convient d'éviter de se connecter à des points d'accès sans fil inconnus ou non sécurisés, et si cela est inévitable, il faut le faire par le biais d'un réseau privé virtuel (VPN) crypté.
- Gérer tous les dispositifs d'extrémité (fixes et mobiles) conformément aux politiques de sécurité de l'organisation.

Les réseaux de l'organisation auxquels on accède à distance doivent être sécurisés, notamment par une authentification multifactorielle (MFA).

Orientation

Appliquer le MFA (par exemple 2FA) sur les systèmes en contact avec l'Internet, tels que le courrier électronique, le bureau à distance et le réseau privé virtuel (VPN).

PR.AC-4 Les permissions et les autorisations d'accès sont gérées, en intégrant les principes du moindre privilège et de la séparation des tâches.

Les autorisations d'accès des utilisateurs aux systèmes de l'organisation doivent être définies et gérées.

Orientation

Il convient de considérer les éléments suivants :

- Établir et réviser régulièrement les listes d'accès par système (fichiers, serveurs, logiciels, bases de données, etc.), éventuellement par l'analyse de l'Active Directory dans les systèmes basés sur Windows, dans le but de déterminer qui a besoin de quel type d'accès (privilégié ou non), à quoi, pour exercer ses fonctions dans l'organisation.
- Créez un compte distinct pour chaque utilisateur (y compris pour les sous-traitants ayant besoin d'un accès) et exigez que des mots de passe forts et uniques soient utilisés pour chaque compte.
- Veillez à ce que tous les employés utilisent des comptes informatiques sans privilèges administratifs pour effectuer des fonctions de travail typiques. Cela inclut la séparation des comptes personnels et des comptes administratifs.
- Pour les comptes d'invités, envisagez d'utiliser les privilèges minimaux (par exemple, l'accès à l'Internet uniquement) requis pour vos besoins opérationnels.
- Il convient que la gestion des autorisations soit documentée dans une procédure et mise à jour le cas échéant.
- Utilisez l'authentification unique (SSO) si nécessaire.

L'organisation doit identifier qui devrait avoir accès aux informations et aux technologies critiques de l'organisation et les moyens d'y accéder.

Orientation

Les moyens d'accès peuvent inclure : une clé, un mot de passe, un code ou un privilège administratif.

L'accès des employés aux données et aux informations doit être limité aux systèmes et aux informations spécifiques dont ils ont besoin pour faire leur travail (principe du moindre privilège).

Orientation

Il convient que le principe du moindre privilège soit compris comme le principe selon lequel une architecture de sécurité doit être conçue de manière à ce que chaque employé se voie accorder les ressources système et d'autorisations minimales dont il a besoin pour exercer sa fonction.

À considérer :

- Ne pas permettre à un employé d'avoir accès à toutes les informations de l'organisation.
- Limiter le nombre d'accès Internet et d'interconnexions avec les réseaux partenaires au strict nécessaire pour pouvoir centraliser et homogénéiser plus facilement le suivi des échanges.
- Assurez-vous que lorsqu'un employé quitte l'organisation, tout accès aux informations ou aux systèmes de l'organisation est bloqué instantanément.

Personne ne doit avoir de privilèges d'administrateur pour les tâches quotidiennes.

Orientation

Considérez ce qui suit :

- Séparez les comptes d'administrateur des comptes d'utilisateur.
- Ne pas privilégier les comptes d'utilisateurs pour effectuer les tâches d'administration.
- Créez des mots de passe uniques pour les administrateurs locaux et désactivez les comptes inutilisés.
- Envisagez d'interdire la navigation sur Internet aux comptes administratifs.

PR.AC-5 L'intégrité du réseau (séparation du réseau, segmentation du réseau...) est protégée.

Des pare-feu doivent être installés et activés sur tous les réseaux de l'organisation.

Orientation

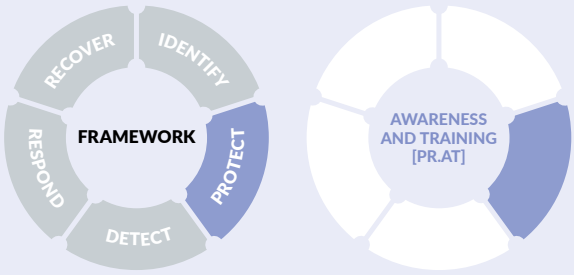
Considérez ce qui suit :

- Installez et faites fonctionner un pare-feu entre votre réseau interne et l'Internet. Il peut s'agir d'une fonction d'un point d'accès/routeur (sans fil) ou d'un routeur fourni par le fournisseur d'accès Internet (FAI).
- Assurez-vous qu'un logiciel antivirus est installé sur les solutions de pare-feu achetées et veillez à ce que le mot de passe de connexion et d'administration de l'administrateur soit modifié lors de l'installation et régulièrement par la suite.
- Installez, utilisez et mettez à jour un pare-feu logiciel sur chaque système informatique (y compris les téléphones intelligents et autres appareils en réseau).
- Installez des pare-feu sur chacun de vos ordinateurs et réseaux, même si vous utilisez un fournisseur de services en nuage ou un réseau privé virtuel (VPN). Assurez-vous que le réseau et les systèmes de votre domicile de télétravail sont équipés de pare-feu matériels et logiciels installés, opérationnels et régulièrement mis à jour.
- Envisagez d'installer un système de détection et de prévention des intrusions (IDPS). Ces dispositifs analysent le trafic réseau à un niveau plus détaillé et peuvent fournir un plus grand niveau de protection.

Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par l'intégration de la segmentation et de la ségrégation du réseau.

Orientation

- Envisagez de créer différentes zones de sécurité dans le réseau (par exemple, segmentation de base du réseau par des VLAN ou d'autres mécanismes de contrôle d'accès au réseau) et contrôlez/surveillez le trafic entre ces zones.
- Lorsque le réseau est "plat", la compromission d'un composant vital du réseau peut entraîner la compromission de l'ensemble du réseau.



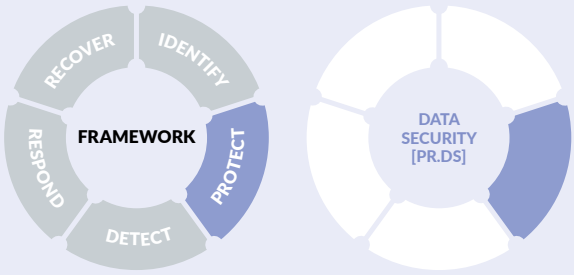
Le personnel et les partenaires de l'organisation reçoivent une formation de sensibilisation à la cybersécurité et sont formés à l'exécution de leurs tâches et responsabilités liées à la cybersécurité, conformément aux politiques, procédures et accords connexes.

PR.AT-1 Tous les utilisateurs sont informés et formés.

Les employés doivent être formés de manière appropriée.

Orientation

- Les employés comprennent tous les utilisateurs et les gestionnaires des systèmes TIC/OT, et il convient qu'ils soient formés dès leur embauche, puis régulièrement, aux politiques de sécurité de l'information de l'organisation et à ce qu'on attend d'eux pour protéger les informations et les technologies de l'organisation.
- Il convient que la formation doit être continuellement mise à jour et renforcée par des campagnes de sensibilisation.



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

PR.DS-1 Les données au repos sont protégées.

Ce contrôle est couvert par d'autres éléments du cadre ; aucune exigence supplémentaire n'est identifiée.

Orientation

- Envisagez d'utiliser des techniques de cryptage pour le stockage des données, la transmission des données ou le transport des données (par exemple, ordinateur portable, USB).
- Envisagez de crypter les appareils des utilisateurs finaux et les supports amovibles contenant des données sensibles (disques durs, ordinateurs portables, appareils mobiles, périphériques de stockage USB, etc.) Cela peut être fait par exemple avec Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,...
- Envisagez de crypter les données sensibles stockées dans le nuage.

PR.DS-2 Les données en transit sont protégées.

Ce contrôle est couvert par d'autres éléments du cadre ; aucune exigence supplémentaire n'est identifiée.

Orientation

Lorsque l'organisation envoie souvent des documents ou des courriels sensibles, il est recommandé de chiffrer ces documents et/ou courriels à l'aide d'outils logiciels appropriés, pris en charge et autorisés.

PR.DS-3 Les actifs sont gérés de manière formelle tout au long de leur retrait, de leur transfert et de leur mise à disposition.

Les actifs et les supports doivent être éliminés de manière sûre.

Orientation

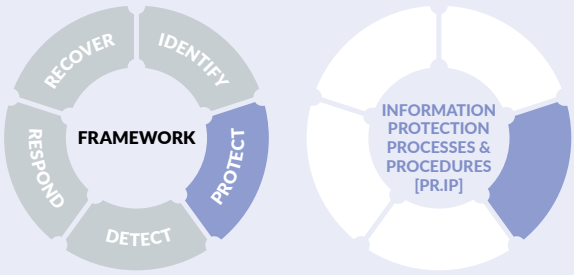
- Lors de l'élimination d'actifs tangibles tels que les ordinateurs professionnels/portables, les serveurs, le(s) disque(s) dur(s) et autres supports de stockage (clés USB, papier...), assurez-vous que toutes les données professionnelles ou personnelles sensibles sont supprimées de manière sécurisée (c'est-à-dire "effacées" électroniquement) avant d'être retirées et ensuite physiquement détruites (ou remises en service). Cette opération est également connue sous le nom de "assainissement" et est donc liée à l'exigence et aux conseils de PR.IP-6.
- Envisager d'installer une application d'effacement à distance sur les ordinateurs portables, les tablettes, les téléphones portables et autres appareils mobiles de l'organisation.

PR.DS-7 Les environnements de développement et de test sont séparés de l'environnement de production.

Aucune exigence n'est identifiée pour le niveau d'assurance "élémentaire", mais des lignes directrices sont fournies pour renforcer la sécurité des informations.

Orientation

- Il convient que tout changement que l'on souhaite apporter à l'environnement ICT/OT soit d'abord testé dans un environnement différent et distinct de l'environnement de production (environnement opérationnel) avant que ce changement ne soit effectivement mis en œuvre. De cette façon, l'effet de ces changements peut être analysé et des ajustements peuvent être effectués sans perturber les activités opérationnelles.
- Envisagez d'ajouter et de tester des fonctions de cybersécurité dès le début du développement (principes du cycle de développement sécurisé).



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

PR.IP-4 Des sauvegardes des informations sont effectuées, maintenues et testées.

Les sauvegardes des données critiques de l'organisation doivent être effectuées et stockées sur un système différent du dispositif sur lequel se trouvent les données originales.

Orientation

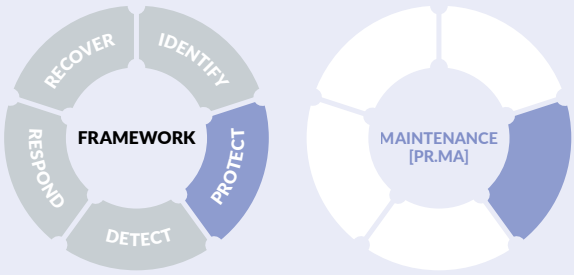
- Les données des systèmes critiques de l'organisation comprennent par exemple les logiciels, les configurations et les paramètres, la documentation, les données de configuration du système, y compris les sauvegardes de la configuration de l'ordinateur, les sauvegardes de la configuration des applications, etc.
- Envisagez une sauvegarde régulière et mettez-la hors ligne périodiquement.
- Il convient que les objectifs de temps et de point de rétablissement doivent être pris en compte.
- Envisagez de ne pas stocker la sauvegarde des données de l'organisation sur le même réseau que le système sur lequel résident les données originales et fournissez une copie hors ligne. Cela permet notamment d'éviter le cryptage des fichiers par les pirates (risque de ransomware).

PR.IP-11 La cybersécurité est incluse dans les pratiques de ressources humaines (déprovisionnement, sélection du personnel...).

Le personnel ayant accès aux informations ou aux technologies les plus critiques de l'organisation doit être vérifié.

Orientation

- Il convient que l'accès aux informations ou aux technologies critiques soit pris en compte lors du recrutement, pendant l'emploi et lors de la cessation d'activité.
- Il convient que les vérifications des antécédents tiennent compte des lois, des règlements et de l'éthique applicables, proportionnellement aux besoins de l'organisation, à la classification des informations auxquelles il faut accéder et aux risques perçus.



La maintenance et la réparation des composants des systèmes de contrôle et d'information industriels sont effectuées conformément aux politiques et procédures.

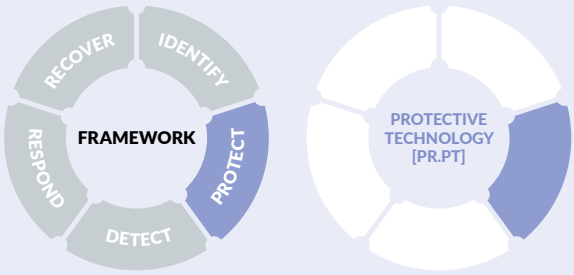
PR.MA-1 L'entretien et la réparation des actifs organisationnels sont effectués et consignés, avec des outils approuvés et contrôlés.

Les correctifs et les mises à jour de sécurité pour les systèmes d'exploitation et les composants critiques du système doivent être installés.

Orientation

Il convient de considérer les éléments suivants :

- Limitez-vous à l'installation des applications (systèmes d'exploitation, microprogrammes ou plugins) dont vous avez besoin pour gérer votre organisation et mettez-les à jour régulièrement.
- Il convient de n'installer que la version actuelle et prise en charge par le fournisseur du logiciel que vous choisissez d'utiliser. Il peut être utile d'attribuer un jour par mois à la vérification des correctifs.
- Il existe des produits qui peuvent analyser votre système et vous avertir lorsqu'il existe une mise à jour pour une application que vous avez installée. Si vous utilisez l'un de ces produits, assurez-vous qu'il vérifie les mises à jour pour chaque application que vous utilisez.
- Installer les correctifs et les mises à jour de sécurité en temps voulu.



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

PR.PT-1 Les enregistrements d'audit/logs sont déterminés, documentés, mis en œuvre et révisés conformément à la politique.

Les logs doivent être maintenus, documentés et examinés.

Orientation

- Assurez-vous que la fonctionnalité d'enregistrement des activités du matériel ou du logiciel de protection/détection (par exemple, les pare-feu, les antivirus) est activée.
- Il convient que les logs soient sauvegardés et conservés pendant une période prédéfinie.
- Il convient que les logs soient examinés pour déceler toute tendance inhabituelle ou indésirable, telle qu'une utilisation importante des sites Web de médias sociaux ou un nombre inhabituel de virus trouvés régulièrement sur un ordinateur particulier. Ces tendances peuvent indiquer un problème plus grave ou signaler la nécessité de renforcer les protections dans un domaine particulier.

PR.PT-4 Les réseaux de communication et de contrôle sont protégés.

Des filtres web et e-mail doivent être installés et utilisés.

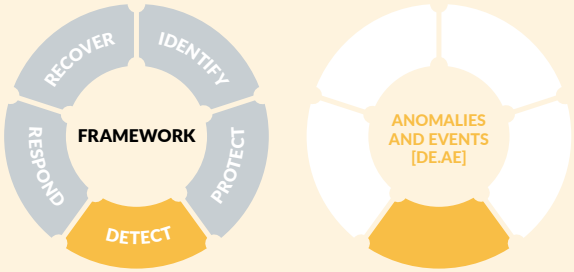
Orientation

- Il convient que les filtres de messagerie détectent les courriers électroniques malveillants et que le filtrage soit configuré en fonction du type de pièces jointes des messages afin que les fichiers des types spécifiés soient automatiquement traités (par exemple, supprimés).
- Il convient que les filtres Web avertissent l'utilisateur si un site Web est susceptible de contenir des logiciels malveillants et empêcher potentiellement les utilisateurs d'accéder à ce site.


WARNING!
SYSTEM WARNING

DÉTECTER

Detect



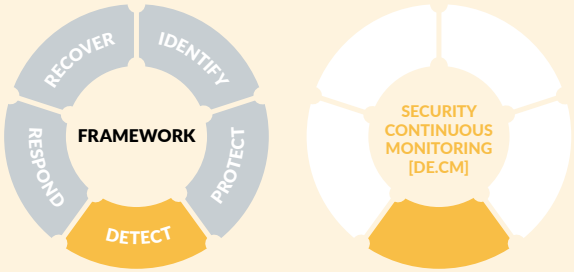
Les activités anormales sont détectées et l'impact potentiel des événements est compris.

DE.AE-3 Les données d'événements sont collectées et corrélées à partir de sources et de capteurs multiples.

La fonctionnalité d'enregistrement de l'activité du matériel ou du logiciel de protection/détection (par exemple, les pare-feu, les anti-virus) doit être activée, sauvegardée et examinée.

Orientation

- Il convient que les logs soient sauvegardés et conservés pendant une période prédéfinie.
- Il convient que les logs soient examinés pour déceler toute tendance inhabituelle ou indésirable, telle qu'une utilisation importante des sites Web de médias sociaux ou un nombre inhabituel de virus trouvés régulièrement sur un ordinateur particulier. Ces tendances peuvent indiquer un problème plus grave ou signaler la nécessité de renforcer les protections dans un domaine particulier.



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

DE.CM-1 Le réseau est surveillé pour détecter les événements potentiels de cybersécurité.

Des pare-feu doivent être installés et exploités aux limites du réseau et complétés par une protection pare-feu sur les terminaux.

Orientation

- Les terminaux comprennent les ordinateurs de bureau, les ordinateurs portables, les serveurs...
- Envisagez, dans la mesure du possible, d'inclure les téléphones intelligents et autres appareils en réseau dans l'installation et l'exploitation des pare-feu.
- Envisagez de limiter le nombre de gateways vers internet.

DE.CM-3 L'activité du personnel est surveillée pour détecter les événements potentiels de cybersécurité.

Des outils de protection des terminaux et des réseaux permettant de surveiller le comportement de l'utilisateur final pour détecter toute activité dangereuse doivent être mis en œuvre.

Orientation

Envisagez le déploiement d'un système de détection/prévention des intrusions (IDS/IPS).

DE.CM-4 Le code malveillant est détecté.

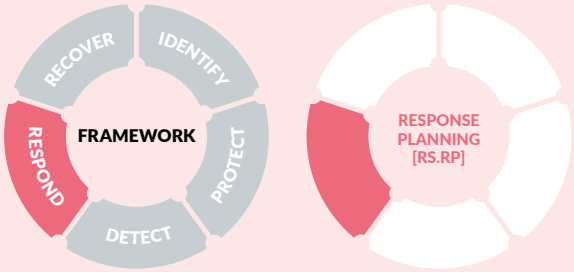
Les programmes anti-virus, anti-spyware et autres programmes malveillants doivent être installés et mis à jour.

Orientation

- Les logiciels malveillants comprennent les virus, les logiciels espions et les ransomwares et il convient qu'ils soient combattus par l'installation, l'utilisation et la mise à jour régulière de logiciels antivirus et anti logiciels espions sur chaque appareil utilisé dans le cadre des activités de l'organisation (y compris les ordinateurs, les smartphones, les tablettes et les serveurs).
- Il convient que les logiciels antivirus et anti logiciels espions recherchent automatiquement les mises à jour en "temps réel" ou au moins quotidiennement, puis procédent à une analyse du système, le cas échéant.
- Il convient de fournir les mêmes mécanismes de protection contre les codes malveillants pour les ordinateurs à domicile (télétravail, par exemple) ou les appareils personnels utilisés pour le travail professionnel (BYOD).

RÉPONDRE

Respond



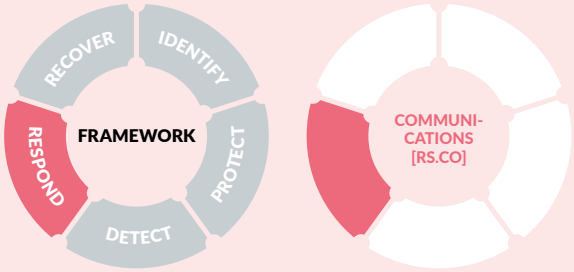
Les processus et procédures de réponse sont exécutés et maintenus, afin de garantir une réponse aux incidents de cybersécurité détectés.

RS.RP-1 Le plan de réponse est exécuté pendant ou après un incident.

Un processus de réponse aux incidents, comprenant les rôles, les responsabilités et les pouvoirs, doit être exécuté pendant ou après un événement lié à l'information ou à la cybersécurité sur les systèmes critiques de l'organisation.

Orientation

- Il convient que le processus de réponse aux incidents inclue un ensemble prédéterminé d'instructions ou de procédures pour détecter, répondre et limiter les conséquences d'une cyber-attaque malveillante.
- Il convient que les rôles, les responsabilités et les pouvoirs prévus dans le plan de réponse aux incidents soient précis quant aux personnes impliquées, leurs coordonnées, leurs différents rôles et responsabilités, à la personne qui prend la décision de lancer les procédures de rétablissement et à celle qui sera le contact avec les parties prenantes externes appropriées.



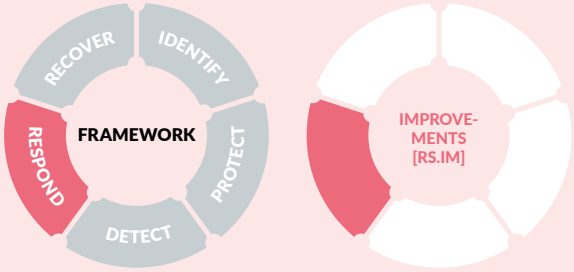
Les activités de réponse sont coordonnées avec les parties prenantes internes et externes (par exemple, le soutien externe des forces de l'ordre).

RS.CO-3 Les informations sont partagées conformément aux plans de réponse.

Les informations relatives aux incidents de cybersécurité doivent être communiquées et partagées avec les employés de l'organisation dans un format qu'ils peuvent comprendre.

Orientation

Il n'y a pas de directives supplémentaires.



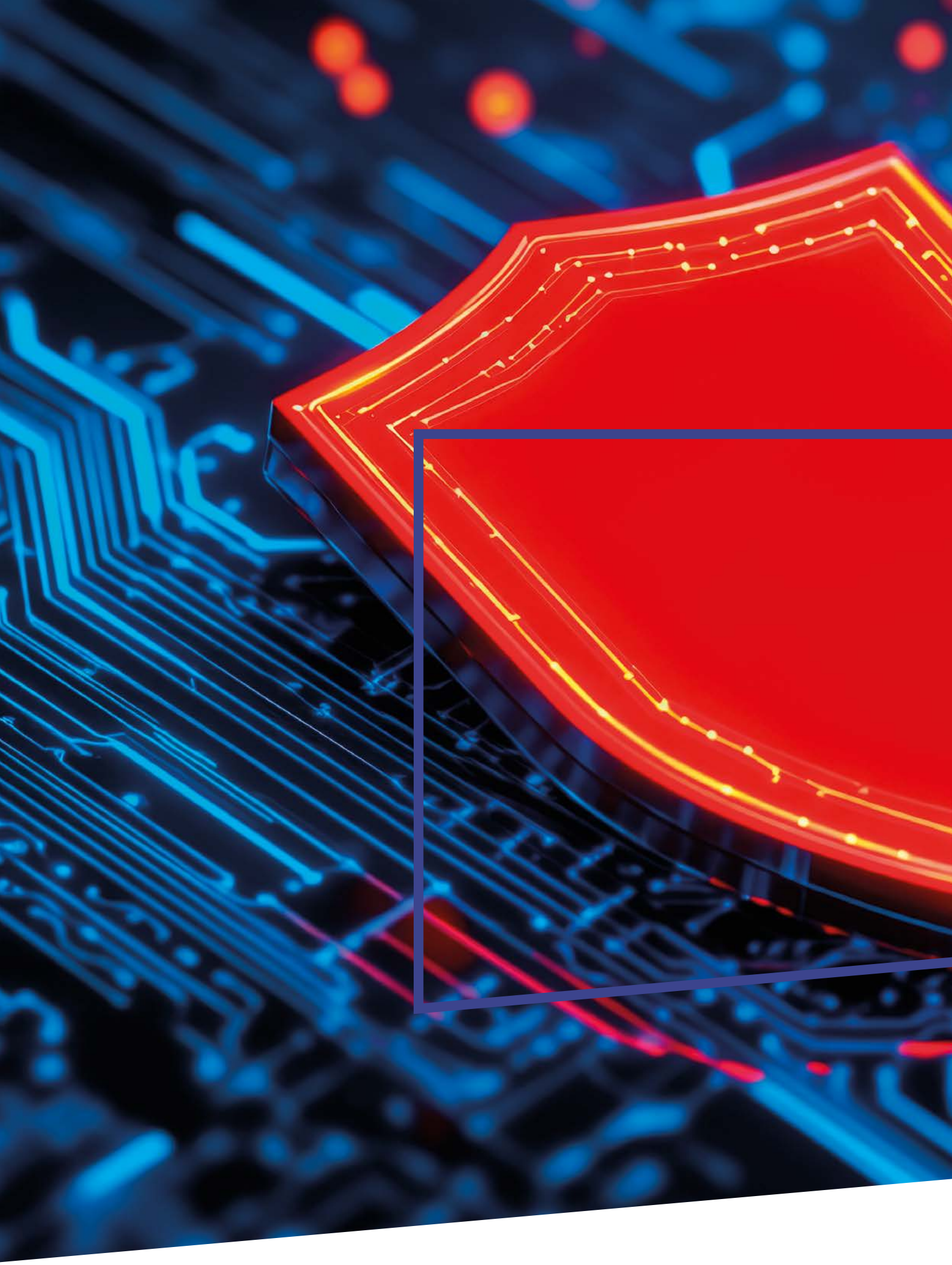
Les activités de réponse de l'organisation sont améliorées par l'intégration des enseignements tirés des activités de détection/réponse actuelles et précédentes.

RS.IM-1 Les plans de réponse intègrent les enseignements tirés.

L'organisation doit effectuer des évaluations post-incident afin d'analyser les enseignements tirés de la réponse à l'incident et du rétablissement, et par conséquent améliorer les processus / procédures / technologies pour renforcer sa cyber-résilience.

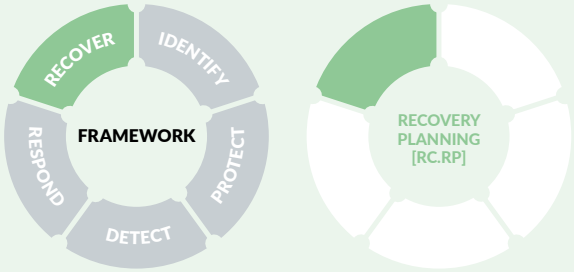
Orientation

Envisagez de réunir les personnes concernées après chaque incident et réfléchissez ensemble aux moyens d'améliorer ce qui s'est passé, comment cela s'est passé, comment nous avons réagi, comment cela aurait pu mieux se passer, ce qui devrait être fait pour éviter que cela ne se reproduise, etc.



RÉTABLIR

Recover



Des processus et des procédures de rétablissement sont exécutés et maintenus pour assurer la restauration des systèmes ou des actifs touchés par des incidents de cybersécurité.

RC.RP-1 Le plan de rétablissement est exécuté pendant ou après un incident de cybersécurité.

Un processus de rétablissement en cas de catastrophes et d'incidents liés à l'information et à la cybersécurité est élaboré et exécuté selon les besoins.

Orientation

Il convient qu'un processus soit élaboré pour déterminer les mesures immédiates à prendre en cas d'incendie, d'urgence médicale, de cambriolage, de catastrophe naturelle ou d'incident de sécurité informatique.

Il convient que ce processus prenne en compte :

- Rôles et responsabilités, y compris qui prend la décision de lancer les procédures de rétablissement et qui sera le contact avec les parties prenantes externes appropriées.
- Ce qu'il faut faire avec les informations et les systèmes d'information de l'organisation en cas d'incident. Cela comprend l'arrêt ou le verrouillage des ordinateurs, le déplacement vers un site de secours, le retrait physique des documents importants, etc.
- Qui appeler en cas d'incident.

ANNEXE

ANNEXE A : LISTE DES MESURES CLÉS POUR LE NIVEAU D'ASSURANCE "BASIC".

PROTÉGER

PR.AC-1 Les identités et les identifiants sont émis, gérés, vérifiés, révoqués et audités pour les dispositifs, les utilisateurs et les processus autorisés.

(1) Les identités et les identifiants des dispositifs et des utilisateurs autorisés doivent être gérés.

PR.AC-3 L'accès à distance est géré.

(2) Les réseaux de l'organisation auxquels on accède à distance doivent être sécurisés, notamment par une authentification multifactorielle (MFA).

PR.AC-4 Les permissions et les autorisations d'accès sont gérées en intégrant les principes du moindre privilège et de la séparation des tâches.

(3) Les autorisations d'accès des utilisateurs aux systèmes de l'organisation doivent être définies et gérées.

(4) Il convient d'identifier qui doit avoir accès aux informations et aux technologies critiques de l'organisation de l'organisation et les moyens d'y accéder.

(5) L'accès des employés aux données et aux informations est limité aux systèmes et aux informations spécifiques dont ils ont besoin pour faire leur travail.

(6) Personne ne doit avoir de privilèges d'administrateur pour les tâches quotidiennes.

PR.AC-5 L'intégrité du réseau est protégée (par exemple, séparation du réseau, segmentation du réseau).

(7) Des pare-feu doivent être installés et activés sur tous les réseaux de l'organisation.

(8) Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par l'intégration de la segmentation et de la ségrégation du réseau.

PR.IP-4 Des sauvegardes des informations sont effectuées, maintenues et testées.

(9) Les sauvegardes des données critiques de l'organisation doivent être effectuées et stockées sur un système différent du dispositif sur lequel résident les données originales.

PR.MA-1 L'entretien et la réparation des actifs de l'organisation sont effectués et consignés, avec des outils approuvés et contrôlés.

(10) Les correctifs et les mises à jour de sécurité pour les systèmes d'exploitation et les composants critiques du système doivent être installés.

PR.PT-1 Les enregistrements d'audit/logs sont déterminés, documentés, mis en œuvre et revus conformément à la politique.

(11) Les logs doivent être tenus, documentés et examinés.

DÉTECTER

DE.AE-3 Les données d'événements sont collectées et corrélées à partir de sources et de capteurs multiples.

(12) La fonctionnalité d'enregistrement des activités du matériel ou du logiciel de protection/détection (par exemple, les pare-feu, les antivirus) doit être activée, sauvegardée et examinée.

DE.CM-4 Un code malveillant est détecté.

(13) Les programmes anti-virus, anti-spyware et autres programmes malveillants doivent être installés et mis à jour.

Avis de non-responsabilité

Le présent document et ses annexes ont été élaborés par le Centre pour la cybersécurité en Belgique (CCB), une administration fédérale créée par l'arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre.

Tous les textes, mises en page, dessins et autres éléments de toute nature figurant dans ce document sont soumis à la **législation sur le droit d'auteur**. La reproduction d'extraits de ce document est autorisée uniquement à des fins non commerciales et à condition que la source soit mentionnée.

Ce document contient des informations techniques rédigées principalement en français. Ces informations concernent la sécurité des réseaux et des systèmes d'information s'adresse aux services informatiques et peuvent utiliser des termes anglais du langage informatique. Une traduction en anglais, néerlandais et allemand de ces informations techniques sont également rendu accessible par le CCB.

Le CCB n'accepte **aucune responsabilité quant au contenu** de ce document.
Les informations fournies :

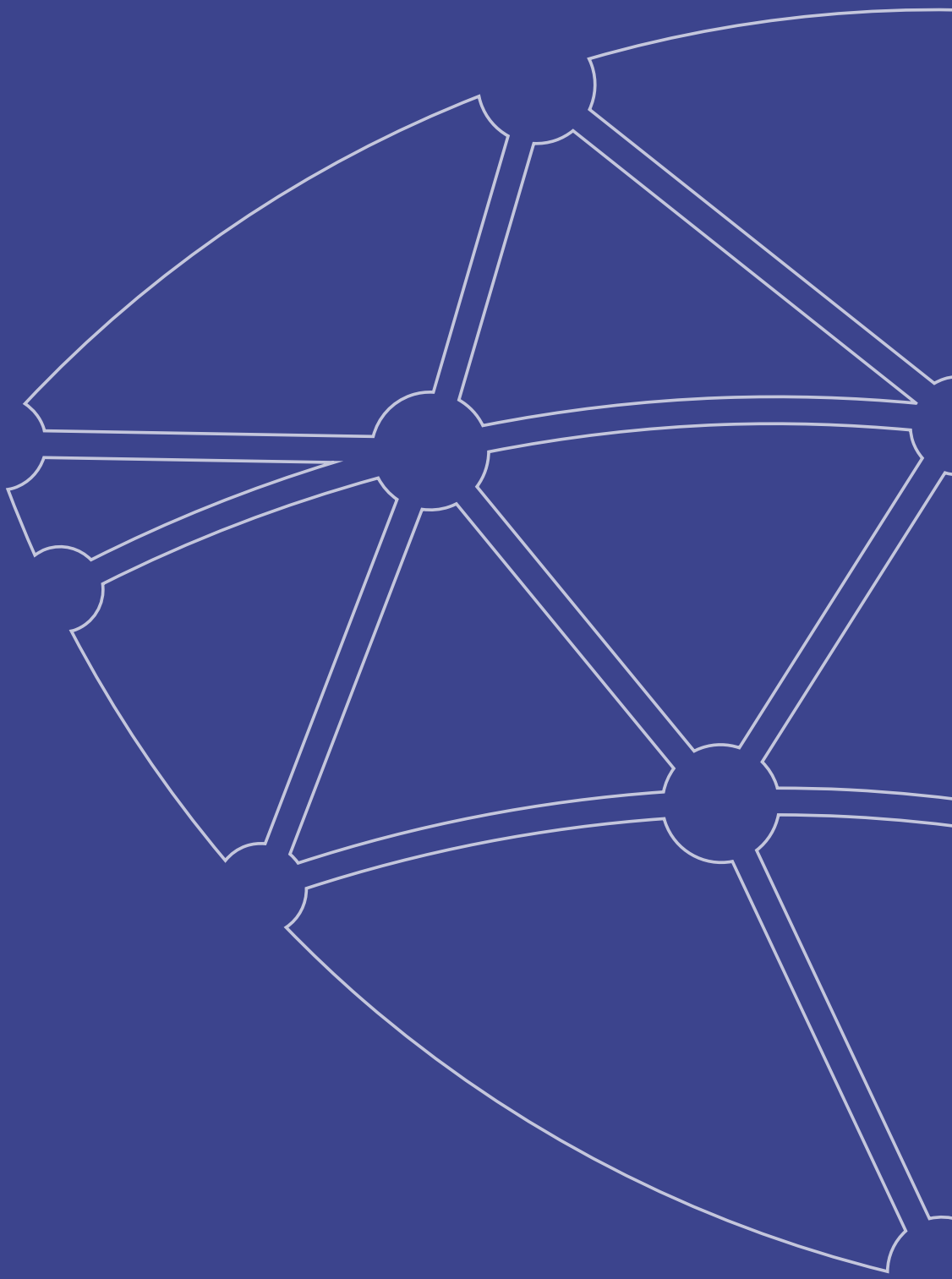
- sont exclusivement de nature générale et ne visent pas à prendre en considération toutes les situations particulières.
- ne sont pas nécessairement exhaustives, précises ou à jour sur tous les points.

Rédacteur responsable

Centre pour la Cybersécurité de Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 18
1000 Bruxelles

Dépôt légal

D/2023/14828/001



Centre pour la Cybersécurité Belgique

Rue de la Loi, 18

1000, Bruxelles