# Catégories de contrôles

## Catégories de contrôles

Les contrôles relatifs à la cybersécurité sont regroupés en trois catégories principales :

* Contrôles administratifs et de gestion
* Contrôles techniques
* Contrôles physiques

**Les contrôles administratifs et de gestion** portent sur la composante humaine de la cybersécurité. Ces contrôles comprennent des politiques et des procédures qui définissent la manière dont une entreprise gère les données et qui détaillent clairement les responsabilités des employés, notamment leur rôle dans la protection de l'entreprise. Alors que les contrôles administratifs sont généralement basés sur des politiques, l'application de ces politiques peut nécessiter l'utilisation de contrôles techniques ou physiques.

Les **contrôles techniques** consistent en des solutions telles que les pare-feux, les systèmes de détection d'intrusion (IDS), les systèmes de prévention d'intrusion (IPS), les produits audiovisuels, le chiffrement, etc. Les contrôles techniques peuvent être utilisés de différentes manières pour atteindre les buts et objectifs de l'entreprise.

**Les contrôles physiques** comprennent les serrures de porte, les serrures d'armoire, les caméras de surveillance, les lecteurs de badges, etc. Ils sont utilisés pour limiter l'accès physique aux ressources matérielles par du personnel non autorisé.

## Types de contrôle

Il existe cinq types de contrôles :

1. Préventif
2. Correctif
3. Détectif
4. Dissuasif
5. Compensatoire

Ces contrôles fonctionnent ensemble pour fournir une défense en profondeur et protéger les ressources. **Les contrôles préventifs** sont conçus pour éviter qu'un incident ne se produise. **Les contrôles correctifs** sont utilisés pour restaurer une ressource après un incident. **Les contrôles détectifs** sont mis en œuvre pour déterminer si un incident s'est produit ou est en cours. **Les contrôles dissuasifs** sont conçus pour décourager les attaques. Enfin, **les contrôles compensatoires** sont utilisés pour renforcer la sécurité d'une ressource lorsque les contrôles actuels ne suffisent pas à la protéger de manière adéquate.

Reportez-vous aux tableaux suivants pour obtenir des détails spécifiques sur chaque type de contrôle et son objectif.

| Contrôles administratifs | | |
| --- | --- | --- |
| Nom du contrôle | Type de contrôle | Objectif du contrôle |
| Moindre privilège | Préventif | Réduire le risque et l'impact global d'un acteur malveillant ou de comptes compromis |
| Plans de reprise après sinistre | Correctif | Assurer la continuité des activités |
| Politiques de mots de passe | Préventif | Réduire la probabilité de compromettre un compte par des techniques d'attaque par force brute ou par dictionnaire |
| Politiques de contrôle d'accès | Préventif | Renforcer la confidentialité et l'intégrité en définissant les groupes autorisés à accéder aux données ou à les modifier |
| Politiques de gestion des comptes | Préventif | Gérer le cycle de vie des comptes, réduire la surface d'attaque et limiter l'impact global des anciens employés mécontents et de l'utilisation par défaut des comptes |
| Séparation des tâches | Préventif | Réduire le risque et l'impact global d'un acteur malveillant ou de comptes compromis |

| Contrôles techniques | | |
| --- | --- | --- |
| Nom du contrôle | Type de contrôle | Objectif du contrôle |
| Pare-feu | Préventif | Filtrer le trafic indésirable ou malveillant pour l'empêcher de pénétrer dans le réseau |
| IDS/IPS | Détectif | Détecter et empêcher le trafic anormal qui correspond à une signature ou à une règle |
| Chiffrement | Dissuasif | Assurer la confidentialité des informations sensibles |
| Sauvegardes | Correctif | Restaurer/récupérer à la suite d'un événement |
| Gestion des mots de passe | Préventif | Réduire la fatigue liée aux mots de passe |
| Logiciel antivirus (AV) | Correctif | Détecter et mettre en quarantaine les menaces connues |
| Surveillance, maintenance et intervention manuelles | Préventif | Nécessaire pour identifier et gérer les menaces, les risques ou les vulnérabilités des systèmes obsolètes |

| Contrôles physiques | | |
| --- | --- | --- |
| Nom du contrôle | Type de contrôle | Objectif du contrôle |
| Coffre-fort temporisé | Dissuasif | Réduire la surface d'attaque et l'impact global des menaces physiques |
| Éclairage adéquat | Dissuasif | Dissuader les menaces en limitant les cachettes |
| Système de télévision en circuit fermé (CCTV) | Préventif/détectif | La télévision en circuit fermé est à la fois un contrôle préventif et un contrôle détectif, car sa présence peut réduire le risque que certains types d'événements se produisent, et elle peut être utilisée après un événement pour informer sur ses conditions |
| Armoires verrouillables (pour les équipements de réseau) | Préventif | Renforcer l'intégrité en empêchant le personnel non autorisé et d'autres personnes d'accéder physiquement à l'équipement de l'infrastructure du réseau ou de le modifier |
| Panneau indiquant le fournisseur de services d'alarme | Dissuasif | Dissuader certains types de menaces en donnant l'impression que la probabilité de réussite d'une attaque est faible |
| Verrous | Dissuasif/préventif | Renforcer l'intégrité en dissuadant et en empêchant le personnel et les individus non autorisés d'accéder physiquement aux ressources |
| Détection et prévention des incendies (alarme incendie, système de gicleurs, etc.) | Détectif/préventif | Détecter un incendie dans un lieu physique et prévenir les dommages aux ressources physiques tels que les stocks, les serveurs, etc. |