Cette traduction offerte par ISRI n'est pas une traduction officielle du référentiel

ID de la catégorie	Catégorie	ID mesure CIS	Type d'actifs	ID et titre de la mesure	Fonction de sécurité	Groupe d'implémentation		
						IG1 (essentiel)	IG2 (avancé)	IG3 (adptatif)
1	Inventaire et maîtrise des actifs d'entreprise	1.1	Équipements	1.1 - Dresser et maintenir l'inventaire détaillé des actifs d'entreprise	Identifier	X	X	X
1	Inventaire et maîtrise des actifs d'entreprise	1.2	Équipements	1.2 - Traiter le problème des actifs non autorisés	Réagir	X	X	X
1	Inventaire et maîtrise des actifs d'entreprise	1.3	Équipements	1.3 - Utiliser un outil de découverte d'actifs	Détecter		X	X
1	Inventaire et maîtrise des actifs d'entreprise	1.4	Équipements	1.4 - Utiliser la journalisation du protocole DHCP pour actualiser l'inventaire des actifs	Identifier		X	X
1	Inventaire et maîtrise des actifs d'entreprise	1.5	Équipements	1.5 - Utiliser un outil passif de découverte d'actifs	Détecter			X
2	Inventaire et maîtrise des actifs logiciels	2.1	Applications	2.1 - Établir et maintenir un inventaire des logiciels	Identifier	X	X	X
2	Inventaire et maîtrise des actifs logiciels	2.2	Applications	2.2 - S'assurer que les logiciels autorisés sont toujours supportés par les éditeurs	Identifier	X	X	X
2	Inventaire et maîtrise des actifs logiciels	2.3	Applications	2.3 - Traiter le problème des logiciels non autorisés	Réagir	X	X	X
2	Inventaire et maîtrise des actifs logiciels	2.4	Applications	2.4 - Utiliser des outils d'inventaire de logiciels automatisés	Détecter		X	X
2	Inventaire et maîtrise des actifs logiciels	2.5	Applications	2.5 - Dresser la liste des logiciels autorisés	Protéger		X	X
2	Inventaire et maîtrise des actifs logiciels	2.6	Applications	2.6 - Dresser la liste des bibliothèques logicielles autorisées	Protéger		X	X
2	Inventaire et maîtrise des actifs logiciels	2.7	Applications	2.7 - Dresser la liste des scripts autorisés	Protéger			X
3	Protection des données	3.1	Données	3.1 - Établir et maintenir un processus de gestion des données	Identifier	X	X	X
3	Protection des données	3.2	Données	3.2 - Établir et maintenir un inventaire des données	Identifier	X	X	X
3	Protection des données	3.3	Données	3.3 - Configurer les listes de contrôle d'accès aux données (permissions)	Protéger	X	X	X
3	Protection des données	3.4	Données	3.4 - Appliquer le délai de rétention des données	Protéger	X	X	X
3	Protection des données	3.5	Données	3.5 - Détruire les données de manière sécurisée	Protéger	X	X	X
3	Protection des données	3.6	Équipements	3.6 - Chiffrer les données sur les appareils des utilisateurs	Protéger	X	X	X
3	Protection des données	3.7	Données	3.7 - Établir et maintenir un système de classification des données	Identifier		X	X
3	Protection des données	3.8	Données	3.8 - Documenter les flux de données	Identifier		X	X
3	Protection des données	3.9	Données	3.9 - Chiffrer les données sur les supports amovibles	Protéger		X	X
3	Protection des données	3.1	Données	3.1 - Chiffrer les données sensibles en transit	Protéger		X	X
3	Protection des données	3.11	Données	3.11 - Chiffrer les données sensibles au repos	Protéger		X	X
3	Protection des données	3.12	Réseau	3.12 - Segmenter le traitement et le stockage des données en se basant sur leur sensibilité	Protéger		X	X
3	Protection des données	3.13	Données	3.13 - Déployer une solution de prévention des pertes de données (DLP)	Protéger			X
3	Protection des données	3.14	Données	3.14 - Journaliser les accès aux données sensibles	Détecter			X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.1	Applications	4.1 - Établir et maintenir un processus de configuration sécurisée	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.2	Réseau	4.2 - Établir et maintenir un processus de configuration sécurisée de l'infrastructure réseau	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.3	Utilisateurs	4.3 - Configurer le verrouillage automatique des sessions sur les actifs d'entreprise	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.4	Équipements	4.4 - Implémenter et gérer un pare-feu sur les serveurs	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.5	Équipements	4.5 - Implémenter et gérer un pare-feu sur les appareils des utilisateurs	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.6	Réseau	4.6 - Gérer de manière sécurisée les actifs d'entreprise et les logiciels	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.7	Utilisateurs	4.7 - Gérer les comptes par défaut sur les actifs d'entreprise et les logiciels	Protéger	X	X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.8	Équipements	4.8 - Désinstaller ou désactiver les services inutiles sur les actifs d'entreprise et les logiciels	Protéger		X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.9	Équipements	4.9 - Configurer les serveurs DNS de confiance dans les actifs d'entreprise	Protéger		X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.1	Équipements	4.1 - Mettre en œuvre la fonction de blocage automatique sur les appareils portables des utilisateurs	Réagir		X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.11	Équipements	4.11 - Mettre en œuvre la fonction d'effacement distant des appareils portables des utilisateurs	Protéger		X	X
4	Configuration sécurisée des actifs d'entreprise et des logiciels	4.12	Équipements	4.12 - Séparer les espaces de travail corporatifs sur les appareils mobiles des utilisateurs	Protéger			X
5	Gestion des comptes	5.1	Utilisateurs	5.1 - Établir et maintenir un inventaire des comptes	Identifier	X	X	X
5	Gestion des comptes	5.2	Utilisateurs	5.2 - Utiliser des mots de passe uniques	Protéger	X	X	X
5	Gestion des comptes	5.3	Utilisateurs	5.3 - Désactiver les comptes dormants	Réagir	X	X	X
5	Gestion des comptes	5.4	Utilisateurs	5.4 - Restreindre les privilèges administrateur des comptes administratifs dédiés	Protéger	X	X	X
5	Gestion des comptes	5.5	Utilisateurs	5.5 - Établir et maintenir un inventaire des comptes de service	Identifier		X	X
5	Gestion des comptes	5.6	Utilisateurs	5.6 - Centraliser la gestion des comptes	Protéger		X	X
6	Gestion du contrôle d'accès	6.1	Utilisateurs	6.1 - Établir un processus pour conférer des droits d'accès	Protéger	X	X	X
6	Gestion du contrôle d'accès	6.2	Utilisateurs	6.2 - Établir un processus de révocation des droits d'accès	Protéger	X	X	X

ID de la catégorie	Catégorie	ID mesure CIS	Type d'actifs	ID et titre de la mesure	Fonction de sécurité	Groupe d'implémentation		
						IG1 (essentiel)	IG2 (avancé)	IG3 (adptatif)
6	Gestion du contrôle d'accès	6.3	Utilisateurs	6.3 - Exiger l'authentification multi-factorielle pour toutes les applications exposées sur l'externe	Protéger	X	X	X
6	Gestion du contrôle d'accès	6.4	Utilisateurs	6.4 - Exiger l'authentification multi-factorielle pour tous les accès distants au réseau	Protéger	X	X	X
6	Gestion du contrôle d'accès	6.5	Utilisateurs	6.5 - Exiger l'authentification multi-factorielle pour tous les accès administratifs	Protéger	X	X	X
6	Gestion du contrôle d'accès	6.6	Utilisateurs	6.6 - Établir et maintenir un inventaire des systèmes d'authentification et d'autorisation	Identifier		X	X
6	Gestion du contrôle d'accès	6.7	Utilisateurs	6.7 - Centraliser le contrôle d'accès	Protéger		X	X
6	Gestion du contrôle d'accès	6.8	Données	6.8 - Définir et maintenir un contrôle d'accès basé sur les rôles	Protéger			X
7	Gestion continue des vulnérabilités	7.1	Applications	7.1 - Établir et maintenir un processus de gestion des vulnérabilités	Protéger	X	X	X
7	Gestion continue des vulnérabilités	7.2	Applications	7.2 - Établir et maintenir un processus de remédiation	Réagir	X	X	X
7	Gestion continue des vulnérabilités	7.3	Applications	7.3 - Réaliser une gestion automatisée des correctifs des systèmes d'exploitation	Protéger	X	X	X
7	Gestion continue des vulnérabilités	7.4	Applications	7.4 - Réaliser une gestion automatisée des correctifs des applications	Protéger	X	X	X
7	Gestion continue des vulnérabilités	7.5	Applications	7.5 - Réaliser des balayages de vulnérabilités automatisés sur les actifs d'entreprise internes	Identifier		X	X
7	Gestion continue des vulnérabilités	7.6	Applications	7.6 - Réaliser des balayages de vulnérabilités automatisés sur les actifs d'entreprise externes	Identifier		X	X
7	Gestion continue des vulnérabilités	7.7	Applications	7.7 - Corriger les vulnérabilités détectées	Réagir		X	X
8	Gestion des journaux d'audit	8.1	Réseau	8.1 - Établir et maintenir un processus d'audit des journaux	Protéger	X	X	X
8	Gestion des journaux d'audit	8.2	Réseau	8.2 - Collecter les journaux d'audit	Détecter	X	X	X
8	Gestion des journaux d'audit	8.3	Réseau	8.3 - S'assurer de disposer d'un espace de stockage suffisant pour la journalisation	Protéger	X	X	X
8	Gestion des journaux d'audit	8.4	Réseau	8.4 - Normaliser la synchronisation temporelle	Protéger		X	X
8	Gestion des journaux d'audit	8.5	Réseau	8.5 - Collecter les journaux d'audit détaillés	Détecter		X	X
8	Gestion des journaux d'audit	8.6	Réseau	8.6 - Collecter les journaux d'audit relatifs aux requêtes DNS	Détecter		X	X
8	Gestion des journaux d'audit	8.7	Réseau	8.7 - Collecter les journaux d'audit relatifs aux requêtes URL	Détecter		X	X
8	Gestion des journaux d'audit	8.8	Équipements	8.8 - Collecter les journaux d'audit relatifs aux commandes en ligne saisies	Détecter		X	X
8	Gestion des journaux d'audit	8.9	Réseau	8.9 - Centraliser les journaux d'audit	Détecter		X	X
8	Gestion des journaux d'audit	8.1	Réseau	8.1 - Conserver les journaux d'audit	Protéger		X	X
8	Gestion des journaux d'audit	8.11	Réseau	8.11 - Réaliser des revues des journaux d'audit	Détecter		X	X
8	Gestion des journaux d'audit	8.12	Données	8.12 - Collecter les journaux des fournisseurs de service	Détecter			X
9	Protections des courriels et de la navigation web	9.1	Applications	9.1 - S'assurer de n'utiliser que des navigateurs et des clients de messagerie pleinement supportés	Protéger	X	X	X
9	Protections des courriels et de la navigation web	9.2	Réseau	9.2 - Utiliser des services de filtrage DNS	Protéger	X	X	X
9	Protections des courriels et de la navigation web	9.3	Réseau	9.3 - Maintenir et appliquer le filtrage des URL au niveau réseau	Protéger		X	X
9	Protections des courriels et de la navigation web	9.4	Applications	9.4 - Restreindre les extensions inutiles ou interdites des navigateurs et des clients de messagerie	Protéger		X	X
9	Protections des courriels et de la navigation web	9.5	Réseau	9.5 - Implémenter DMARC (Domain-based Message Authentication, Reporting, and Conformance)	Protéger		X	X
9	Protections des courriels et de la navigation web	9.6	Réseau	9.6 - Bloquer les types de fichiers inutiles	Protéger		X	X
9	Protections des courriels et de la navigation web	9.7	Réseau	9.7 - Déployer et maintenir les protections anti-malicielles sur les serveurs de messagerie	Protéger			X
10	Défenses contre les maliciels	10.1	Équipements	10.1 - Déployer et maintenir les logiciels anti-maliciels	Protéger	X	X	X
10	Défenses contre les maliciels	10.2	Équipements	10.2 - Configurer les mises à jour automatiques des signatures des anti-maliciels	Protéger	X	X	X
10	Défenses contre les maliciels	10.3	Équipements	10.3 - Désactiver les fonctions d'exécution automatique des supports amovibles	Protéger	X	X	X
10	Défenses contre les maliciels	10.4	Équipements	10.4 - Configurer la vérification automatique par un anti-maliciel des supports amobibles	Détecter		X	X
10	Défenses contre les maliciels	10.5	Équipements	10.5 - Activer les fonctionnalités anti-exploitation	Protéger		X	X
10	Défenses contre les maliciels	10.6	Équipements	10.6 - Gérer de manière centralisée les logiciels anti-maliciels	Protéger		X	X
10	Défenses contre les maliciels	10.7	Équipements	10.7 - Utiliser des logiciels anti-maliciels avec analyse comportementale	Détecter		X	X
11	Récupération des données	11.1	Données	11.1 - Établir et maintenir un processus de restauration des données	Reprendre	X	X	X
11	Récupération des données	11.2	Données	11.2 - Réaliser des sauvegardes automatiques	Reprendre	X	X	X
11	Récupération des données	11.3	Données	11.3 - Protéger les données de restauration	Protéger	X	X	X
11	Récupération des données	11.4	Données	11.4 - Établir et maintenir une instance isolée des données de restauration	Reprendre	X	X	X
11	Récupération des données	11.5	Données	11.5 - Tester la restauration des données	Reprendre		X	X
12	Gestion de l'infrastructure réseau	12.1	Réseau	12.1 - S'assurer que l'infrastructure réseau est à jour	Protéger	X	X	X
12	Gestion de l'infrastructure réseau	12.2	Réseau	12.2 - Établir et maintenir une architecture sécurisée des réseaux	Protéger		X	X
12	Gestion de l'infrastructure réseau	12.3	Réseau	12.3 - Gérer de manière sécurisée l'infrastructure réseau	Protéger		X	X
12	Gestion de l'infrastructure réseau	12.4	Réseau	12.4 - Établir et maintenir des diagrammes d'architecture	Identifier		X	X
12	Gestion de l'infrastructure réseau	12.5	Réseau	12.5 - Centraliser les fonctions d'authentification, autorisation et audit réseau (AAA)	Protéger		X	X

ID de la catégorie	Catégorie	ID mesure CIS	Type d'actifs	ID et titre de la mesure	Fonction de sécurité	Groupe d'implémentation		
						IG1 (essentiel)	IG2 (avancé)	IG3 (adptatif)
12	Gestion de l'infrastructure réseau	12.6	Réseau	12.6 - Utiliser des protocoles de gestion réseau et de communication sécurisés	Protéger		X	X
12	Gestion de l'infrastructure réseau	12.7	Équipements	12.7 - S'assurer que les appareils distants utilisent un VPN et se connectent à l'infrastructure AAA de l'entreprise	Protéger		X	X
12	Gestion de l'infrastructure réseau	12.8	Équipements	12.8 - Établir et maintenir des ressources dédiées pour toutes les tâches d'administration (PAW)	Protéger			X
13	Surveillance et défense du réseau	13.1	Réseau	13.1 - Centraliser l'alertage relatif aux événements de sécurité	Détecter		X	X
13	Surveillance et défense du réseau	13.2	Équipements	13.2 - Déployer une solution de détection d'intrusions système (HIDS)	Détecter		X	X
13	Surveillance et défense du réseau	13.3	Réseau	13.3 - Déployer une solution de détection d'intrusions réseau (NIDS)	Détecter		X	X
13	Surveillance et défense du réseau	13.4	Réseau	13.4 - Réaliser un filtrage de trafic entre les segments réseau (FW)	Protéger		X	X
13	Surveillance et défense du réseau	13.5	Équipements	13.5 - Gérer le contrôle d'accès pour les actifs distants	Protéger		X	X
13	Surveillance et défense du réseau	13.6	Réseau	13.6 - Collecter les journaux des flux réseau	Détecter		X	X
13	Surveillance et défense du réseau	13.7	Équipements	13.7 - Déployer une solution de prévention d'intrusions système (HIPS)	Protéger			X
13	Surveillance et défense du réseau	13.8	Réseau	13.8 - Déployer une solution de prévention d'intrusions réseau (NIPS)	Protéger			X
13	Surveillance et défense du réseau	13.9	Équipements	13.9 - Déployer un contrôle d'accès au niveau du port (802.1x)	Protéger			X
13	Surveillance et défense du réseau	13.1	Réseau	13.1 - Réaliser un filtrage au niveau applicatif (WAF, Proxy filtrant)	Protéger			X
13	Surveillance et défense du réseau	13.11	Réseau	13.11 - Régler les seuils d'alertage sur événements de sécurité	Détecter			X
14	Formation de sensibilisation et des compétences sécurité	14.1	N/A	14.1 - Établir et maintenir un programme de sensibilisation à la sécurité	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.2	N/A	14.2 - Former les employés à reconnaître l'ingénierie sociale	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.3	N/A	14.3 - Former les employés aux bonnes pratiques relatives à l'authentification	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.4	N/A	14.4 - Former les employés aux bonnes pratiques relatives à la manipulation des données	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.5	N/A	14.5 - Former les employés aux causes d'exposition de données accidentelles	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.6	N/A	14.6 - Former les employés à reconnaître et à signaler les incidents de sécurité	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.7	N/A	14.7 - Former les employés à identifier et à signaler si des mises à jour manquent sur les actifs d'entreprise	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.8	N/A	14.8 - Former les employés aux dangers de se connecter à et à transmettre les données de l'entreprise sur des réseaux non fiables (non sécurisés)	Protéger	X	X	X
14	Formation de sensibilisation et des compétences sécurité	14.9	N/A	14.9 - Organiser des formations de sensibilisation à la sécurité basées sur les rôles, avec une dimension pratique	Protéger		X	X
15	Gestion des fournisseurs de service	15.1	N/A	15.1 - Établir et maintenir un inventaire des fournisseurs de service	Identifier	X	X	X
15	Gestion des fournisseurs de service	15.2	N/A	15.2 - Établir et maintenir une politique de gestion des fournisseurs d'accès	Identifier		X	X
15	Gestion des fournisseurs de service	15.3	N/A	15.3 - Classifier les fournisseurs de service	Identifier		X	X
15	Gestion des fournisseurs de service	15.4	N/A	15.4 - S'assurer que les contrats avec les fournisseurs de service incluent des exigences de sécurité	Protéger		X	X
15	Gestion des fournisseurs de service	15.5	N/A	15.5 - Évaluer les fournisseurs de service	Identifier			X
15	Gestion des fournisseurs de service	15.6	Données	15.6 - Surveiller les fournisseurs de service	Détecter			X
15	Gestion des fournisseurs de service	15.7	Données	15.7 - Résilier de manière sécurisée les fournisseurs de service	Protéger			X
16	Sécurité des logiciels d'application	16.1	Applications	16.1 - Établir et maintenir un processus de développement applicatif sécurisé	Protéger		X	X
16	Sécurité des logiciels d'application	16.2	Applications	16.2 - Établir et maintenir un processus pour valider et traiter les vulnérabilités logicielles	Protéger		X	X
16	Sécurité des logiciels d'application	16.3	Applications	16.3 - Réaliser une analyse des causes profondes des vulnérabilités de sécurité	Protéger		X	X
16	Sécurité des logiciels d'application	16.4	Applications	16.4 - Établir et gérer un inventaire des composants logiciels tiers	Protéger		X	X
16	Sécurité des logiciels d'application	16.5	Applications	16.5 - Utiliser des composants logiciels tiers tenus à jour et de confiance	Protéger		X	X
16	Sécurité des logiciels d'application	16.6	Applications	16.6 - Établir et maintenir un système et un processus d'évaluation de la sévérité des vulnérabilités applicatives	Protéger		X	X
16	Sécurité des logiciels d'application	16.7	Applications	16.7 - Utiliser des gabarits standards de configuration sécurisée pour l'infrastructure applicative	Protéger		X	X
16	Sécurité des logiciels d'application	16.8	Applications	16.8 - Séparation des systèmes de production et de non-production	Protéger		X	X
16	Sécurité des logiciels d'application	16.9	Applications	16.9 - Former les développeurs dans les concepts de la sécurité applicative et le codage sécurisé	Protéger		X	X
16	Sécurité des logiciels d'application	16.1	Applications	16.1 - Appliquer les principes de conception sécurisée dans les architectures applicatives	Protéger		X	X
16	Sécurité des logiciels d'application	16.11	Applications	16.11 - Utiliser des modules et des services réputés pour la sécurité applicative des composants	Protéger		X	X
16	Sécurité des logiciels d'application	16.12	Applications	16.12 - Implémenter des vérifications de sécurité au niveau du code	Protéger			X
16	Sécurité des logiciels d'application	16.13	Applications	16.13 - Réaliser des tests d'intrusion applicatifs	Protéger			X
16	Sécurité des logiciels d'application	16.14	Applications	16.14 - Réaliser des modélisations des menaces	Protéger			X
17	Gestion de la réaction aux incidents	17.1	N/A	17.1 - Désigner le personnel en charge du traitement des incidents	Réagir	X	X	X
17	Gestion de la réaction aux incidents	17.2	N/A	17.2 - Établir et maintenir des informations de contact afin de signaler les incidents	Réagir	X	X	X
17	Gestion de la réaction aux incidents	17.3	N/A	17.3 - Établir et maintenir un processus d'entreprise pour les réactions aux incidents	Réagir	X	X	X
17	Gestion de la réaction aux incidents	17.4	N/A	17.4 - Établir et maintenir un processus de réaction aux incidents	Réagir		X	X
17	Gestion de la réaction aux incidents	17.5	N/A	17.5 - Attribuer des rôles et les responsabilités clé	Réagir		X	X

ID de la catégorie	Catégorie	ID mesure CIS	Type d'actifs	ID et titre de la mesure	Fonction de sécurité	Groupe d'implémentation		
						IG1 (essentiel)	IG2 (avancé)	IG3 (adptatif)
17	Gestion de la réaction aux incidents	17.6	N/A	17.6 - Définir les mécanismes pour communiquer durant les réactions aux incidents	Réagir		X	X
17	Gestion de la réaction aux incidents	17.7	N/A	17.7 - Réaliser des exercices de réaction aux incidents routiniers	Reprendre		X	X
17	Gestion de la réaction aux incidents	17.8	N/A	17.8 - Mener des revues post-incident	Reprendre		X	X
17	Gestion de la réaction aux incidents	17.9	N/A	17.9 - Établir et maintenir des seuils d'incidents de sécurité	Reprendre			X
18	Tests d'intrusion	18.1	N/A	18.1 - Établir et maintenir un programme de tests d'intrusion	Identifier		X	X
18	Tests d'intrusion	18.2	Réseau	18.2 - Réaliser des tests d'intrusion externes périodiques	Identifier		X	X
18	Tests d'intrusion	18.3	Réseau	18.3 - Corriger les constats des tests d'intrusion	Protéger		X	X
18	Tests d'intrusion	18.4	Réseau	18.4 - Valider les mesures de sécurité	Protéger			X
18	Tests d'intrusion	18.5	N/A	18.5 - Réaliser des tests d'intrusion internes périodiques	Identifier			X