



Matrice d'Homologation Technique & Financière NIS2 (Article 21)

Dossier d'arbitrage budgétaire et de conformité juridictionnelle pour DSI, RSSI et Comités de Direction (Parcs de 20 à 500 postes)

1. CHECKLIST D'HOMOLOGATION RÉGLEMENTAIRE — ARTICLE 21.2 DIRECTIVE NIS2

ALINÉA NIS2	EXIGENCE RÉGLEMENTAIRE	SILO TECHNOLOGIQUE	PREUVE ATTENDUE EN AUDIT (ANSSI / CCB / NCSC)
Art. 21.2.a	Politiques d'analyse des risques et de sécurité des SI	GRC_NIS2	Registre des risques à jour (EBIOS RM / ISO 27001), PSSI validée par la direction et suivi des plans d'action.
Art. 21.2.b	Gestion et traitement des incidents de sécurité	EDR_XDR	Télémétrie EDR active sur 100 % des postes et serveurs, procédure de notification 24h/72h et isolation réseau.
Art. 21.2.c	Continuité d'activité, sauvegardes et PRA/PCA	BACKUP_DR	Sauvegardes immuables WORM / Object Lock (règle 3-2-1-1-0) et rapports de tests de restauration trimestriels.
Art. 21.2.d	Sécurité de la chaîne d'approvisionnement (Supply Chain)	IAM_PAM / GRC	Évaluation cyber des sous-traitants, immunité extraterritoriale (Cloud Act) et bastion PAM avec audit vidéo des tiers.
Art. 21.2.e	Gestion et divulgation des vulnérabilités	VULN_PENTEST	Scan continu de la surface d'attaque externe (EASM) et des VLANs internes, SLA de correction des CVE critiques.
Art. 21.2.f	Évaluation de l'efficacité des mesures de gestion des risques	GRC_NIS2 / VULN	Indicateurs de contrôle continu, tests d'intrusion périodiques et tableaux de bord de maturité COMEX.
Art. 21.2.g	Pratiques de base en cyber-hygiène et formation	IAM_PAM / EDR	Éradication des mots de passe réutilisés via coffre-fort d'entreprise (EPM) et durcissement des postes.
Art. 21.2.h	Procédures relatives à la cryptographie et au chiffrement	SASE_VPN / IAM	Tunnels réseau chiffrés de bout en bout (WireGuard / IPsec) et chiffrement Zero-Knowledge des secrets.
Art. 21.2.i	Sécurité des RH, contrôle d'accès et gestion des actifs	IAM_PAM / SASE	Moindre privilège réseau (ZTNA), révocation automatisée (SCIM) et rotation des comptes administrateurs AD.
Art. 21.2.j	Authentification multifacteur (MFA) et flux sécurisés	IAM_PAM / SASE	MFA systématique (TOTP / FIDO2 Passkeys) sur l'ensemble des accès distants, messageries et consoles critiques.

Note de responsabilité des dirigeants (Article 20 & 32 NIS2) : Les organes de direction des Entités Essentielles (EE) et Importantes (EI) sont tenus d'approuver les mesures de gestion des risques de cybersécurité et peuvent être tenus personnellement responsables en cas de négligence caractérisée. Plafond des sanctions administratives : jusqu'à 10 000 000 EUR ou 2 % du chiffre d'affaires mondial (EE) et 7 000 000 EUR ou 1,4 % du CA mondial (EI).



Référentiel Tarifaire (TCO) & Souveraineté Juridictionnelle

Simulation budgétaire comparative pour parcs de 50 postes et 200 postes (Montants HT vérifiés sous preuve officielle)

2. TABLEAU RÉCAPITULATIF DES SOLUTIONS TECHNOLOGIQUES AUDITÉES

LOGICIEL	SILO	JURIDICTION	STATUT CLOUD ACT	TARIF UNITAIRE HT	MIN.	TCO ANNUEL 50P	TCO ANNUEL 200P
Acronis Cyber Protect Cloud	BACKUP_DR	Suisse	Exempt Cloud Act (UE/CH)	5,90 EUR / m	5p	3 540 EUR / an	14 160 EUR / an
Bitdefender GravityZone	EDR_XDR	Roumanie	Exempt Cloud Act (UE/CH)	2,04 EUR / m	5p	1 224 EUR / an	4 896 EUR / an
Greenbone Enterprise (OpenVAS)	VULN_PENTEST	Allemagne	Exempt Cloud Act (UE/CH)	Sur devis	25p	Sur devis	Sur devis
HarfangLab EDR	EDR_XDR	France	Exempt Cloud Act (UE/CH)	Sur devis	50p	Sur devis	Sur devis
Intruder Vulnerability Scanner	VULN_PENTEST	Royaume-Uni (Adéquation RGPD UE)	Exempt Cloud Act (UE/CH)	9,50 EUR / m	10p	5 700 EUR / an	22 800 EUR / an
NordLayer	SASE_VPN	Lituanie / Pays-Bas (Groupe Nord Security)	Exempt Cloud Act (UE/CH)	8,00 EUR / m	5p	4 800 EUR / an	19 200 EUR / an
Proton Pass Business	IAM_PAM	Suisse	Exempt Cloud Act (UE/CH)	1,99 EUR / m	1p	1 194 EUR / an	4 776 EUR / an
SentinelOne Singularity	EDR_XDR	États-Unis	Soumis Cloud Act US	5,42 EUR / m	25p	3 252 EUR / an	13 008 EUR / an
Tailscale	SASE_VPN	Canada / États-Unis	Soumis Cloud Act US	5,50 EUR / m	1p	3 300 EUR / an	13 200 EUR / an
Tenacy	GRC_NIS2	France	Exempt Cloud Act (UE/CH)	Sur devis	1p	Sur devis	Sur devis
Vanta	GRC_NIS2	États-Unis	Soumis Cloud Act US	Sur devis	20p	Sur devis	Sur devis
Veeam Data Platform	BACKUP_DR	États-Unis	Soumis Cloud Act US	12,50 EUR / m	10p	7 500 EUR / an	30 000 EUR / an
Wallix PAM4ALL	IAM_PAM	France	Exempt Cloud Act (UE/CH)	Sur devis	10p	Sur devis	Sur devis

3. ARCHITECTURE CIBLE RECOMMANDÉE PAR PROFIL D'ENTITÉ

PROFIL D'ORGANISATION	PILE TECHNOLOGIQUE SOUVERAINE RECOMMANDÉE	BUDGET ANNUEL GLOBAL ESTIMÉ (HORS GRC)
PME / Entité Importante (50 postes) Sans équipe SOC dédiée	Bitdefender GravityZone (EDR) + NordLayer (ZTNA) + Proton Pass Business (EPM) + Acronis Cyber Protect (Backup) + Intruder (Scan)	~16 500 EUR à 22 000 EUR HT / an
ETI / Entité Essentielle (200 postes) Exigence ANSSI / Souveraineté stricte	HarfangLab EDR (Qualifié ANSSI) + Wallix PAM4ALL (Bastion CSPN) + Tenacy (GRC SecNumCloud) + Greenbone Enterprise + Veeam / Acronis	Sur devis intégrateur / MSSP (35 000 EUR+ / an)

Méthodologie d'Audit NIS2 // STACK HUB : Les prix indiqués correspondent aux tarifs publics d'entrée constatés hors taxes et hors options de stockage volumétrique ou prestations d'intégration sur site. Pour actualiser vos simulations de 10 à 500 postes en temps réel, rendez-vous sur le simulateur interactif en ligne.