					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P40					Titre du document : **Politique de tests de sécurité et de red teaming**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
RGPD (UE)	Art. 32(1)(d)	
NIS2 (UE)	Art. 21(2)(f)	
DORA (UE)	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Objet

1 Définir un programme structuré de tests de sécurité réguliers des réseaux, systèmes et applications de l'organisation, y compris des évaluations de vulnérabilités, des tests d'intrusion et des exercices de red teaming, afin de satisfaire aux exigences de l'article 21(2)(f) de NIS2 relatives à l'évaluation de l'efficacité des mesures de cybersécurité.

1.1 Veiller à ce que les faiblesses des mesures techniques et organisationnelles soient identifiées et corrigées de manière proactive au moyen de tests maîtrisés, afin d'améliorer en continu le niveau de sécurité de l'organisation.

2. Champ d’application

2 La présente politique couvre l'ensemble des systèmes d'information critiques, applications et infrastructures de soutien détenus ou exploités par l'organisation. Elle inclut également les tests de sécurité physique des sites lorsqu'ils sont pertinents au regard de la cybersécurité (par exemple, l'ingénierie sociale ou les tests d'intrusion physique, lorsqu'ils relèvent du périmètre du red teaming).

2.1 La présente politique s'applique aux équipes internes de sécurité, à toute société externe mandatée pour réaliser des tests de sécurité, ainsi qu'aux propriétaires de systèmes et d’applications concernés. Toutes les activités de test doivent être autorisées et suivre les procédures définies dans le présent document afin d'éviter toute perturbation non intentionnelle.

3. Objectifs

3 Vérifier l'efficacité des mesures de cybersécurité mises en œuvre (techniques, opérationnelles et organisationnelles) au moyen de tests périodiques et de simulations, conformément à l'exigence de NIS2 relative à la mesure de l'efficacité.

3.1 Détecter les vulnérabilités ou lacunes que les processus opérationnels habituels pourraient ne pas identifier, y compris les vulnérabilités zero-day ou les erreurs de configuration, dans des scénarios d'attaque réalistes (red teaming) avant qu'elles ne soient exploitées par des attaquants.

3.2 Fournir à la direction une assurance ainsi que des recommandations exploitables au moyen du signalement des constats de test, afin de permettre des décisions éclairées en matière de traitement des risques et une amélioration continue du programme de sécurité.

4. Rôles et responsabilités

4 Coordinateur des tests de sécurité (STC) : désigné par le RSSI, responsable de la planification et de la supervision de l'ensemble des activités de test de sécurité. Il veille à ce que les tests soient cadrés, autorisés, et à ce que les résultats soient communiqués et fassent l'objet d'un suivi.

4.1 Équipe de sécurité interne (Blue Team) : collabore aux tests (par exemple, fournit les informations nécessaires au cadrage et surveille les systèmes pendant les tests). Dans le cadre des exercices de red teaming, la Blue Team répond aux attaques simulées et ses capacités de détection et de réponse sont évaluées.

4.2 Red Team / testeurs d'intrusion : il peut s'agir d'une équipe interne de sécurité offensive ou de consultants externes. Ils exécutent les tests selon les règles d'engagement convenues, documentent l'ensemble des vulnérabilités découvertes et des chemins d'exploitation, et préservent la confidentialité.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Surveillance et audit

9 Le STC doit tenir un calendrier et un journal de l'ensemble des activités de test de sécurité réalisées. Ce journal doit inclure la date, le périmètre, l'auteur du test et une synthèse des résultats. Il doit être revu afin de vérifier le respect de la fréquence requise (par exemple, aucun système critique ne doit rester sans test au-delà du cycle annuel).

9.1 L'avancement de la remédiation des constats issus des tests doit être surveillé et communiqué chaque mois. Les problèmes en suspens de gravité élevée doivent être revus en réunion de direction jusqu'à leur clôture.

9.2 L'audit interne ou un auditeur indépendant procède chaque année à une revue du programme de tests de sécurité afin de vérifier que : les tests sont dûment autorisés, réalisés et documentés ; les constats critiques ont été traités ; et le programme répond aux attentes réglementaires (par exemple, les auditeurs peuvent vérifier qu'un test d'intrusion a été réalisé avant le lancement d'un nouveau service en ligne, si cela est requis). Tout écart donne lieu à des plans d'action corrective.

10. Revue et maintenance

10 La présente politique ainsi que le plan global de test font l'objet d'une revue au moins une fois par an. Cette revue prend en compte les évolutions du paysage des menaces (par exemple, l'émergence de nouvelles techniques d'attaque que nos tests actuels ne couvriraient pas) et adapte en conséquence les périmètres ou les fréquences.

10.1 Après tout incident majeur de cybersécurité ou toute violation, la présente politique doit être réexaminée afin de déterminer si des tests supplémentaires ou plus fréquents auraient pu prévenir ou détecter le problème. La politique est ensuite mise à jour pour intégrer ces ajustements (par exemple, l'ajout d'un nouveau scénario dans les exercices de red teaming sur la base des schémas d'attaque observés).

10.2 Les mises à jour de la présente politique doivent être approuvées par le RSSI et portées à la connaissance du conseil d’administration. L'ensemble du personnel concerné doit être informé des modifications, et les partenaires externes de test doivent être notifiés si un changement affecte les conditions de leur intervention.

11. Politiques associées et articulations

11.1 P06 – Politique de gestion des risques. Les résultats des tests alimentent l'évaluation des risques et le traitement des risques.

11.2 P22 – Politique de journalisation et de surveillance. Elle valide la couverture de détection pendant les exercices.

11.3 P24 – Politique de développement sécurisé. Elle intègre les constats des tests dans les contrôles du cycle de vie du développement logiciel (SDLC).

11.4 P25 – Politique relative aux exigences de sécurité des applications. Elle veille à ce que les exigences intègrent les enseignements issus des tests.

11.5 P30 – Politique de réponse aux incidents. Les scénarios de red teaming affinent les playbooks et la réponse.

11.6 P31 – Politique d'investigation numérique. Elle encadre la collecte sécurisée des artefacts pendant les tests.

11.7 P32 – Politique de continuité d'activité et de reprise après sinistre. Les exercices vérifient la résilience en situation d'attaque.

11.8 P33 – Politique d'audit et de surveillance de la conformité. Elle assure une supervision indépendante de l'efficacité du programme de tests.

12. Références

12.1 Directive NIS2 (UE 2022/2555), article 21(2), point (f) (politiques et procédures visant à évaluer l'efficacité des mesures de gestion des risques de cybersécurité)

12.2 Règlement d'exécution (UE) 2024/2690 de la Commission, annexe section 7 (exigences relatives à la surveillance, aux tests et à l'évaluation de l'efficacité des mesures de cybersécurité)

12.3 Guide technique de l'ENISA (2025) – annexe sur les tests de sécurité et l'audit (lignes directrices relatives à la conduite d'exercices de cybersécurité et de tests techniques)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Bonnes pratiques sectorielles : OWASP Testing Guide, NIST SP 800-115 (guide technique des tests de sécurité), CBEST/GREEN Team (cadres de red teaming du secteur financier, à titre de référence)