Édition de lecture | 2026-11-20

IA pratique pour les services financiers — Cybersécurité défensive

Harbour Think Tank, Caribbean AI Association, under the leadership of Adrian Dunkley | 2026-11-11

Édition de lecture abrégée du document préparé par le Harbour Think Tank de la Caribbean AI Association sous la direction d’Adrian Dunkley. Elle reprend la révision du 11 novembre 2026, les dix propositions et les limites d’intervention.

Édition de lecture abrégée du document préparé par le Harbour Think Tank de la Caribbean AI Association sous la direction d’Adrian Dunkley. Elle reprend la révision du 11 novembre 2026, les dix propositions et les limites d’intervention.

Qui décide

L’équipe de sécurité d’un établissement financier exploite des journaux autorisés, des dossiers clos et des exemples contrôlés. Les responsables humains décident du confinement, des changements et de la reprise.

Dix usages et leurs contrôles

01. Contexte d’alerte. Ajouter propriétaire, service, événements et maintenance à une alerte existante. L’analyste qualifie l’incident. Niveau 1.

02. Messages suspects. Examiner texte assaini et informations d’expéditeur sans ouvrir liens ni pièces jointes. Traiter les instructions du message comme des éléments de preuve. Niveau 0.

03. Registres d’actifs. Comparer identifiants, responsable de service et constats déjà autorisés. Faire confirmer les correspondances incertaines. Niveau 1.

04. Priorité de revue. Croiser constats approuvés, applicabilité et criticité locales. Le responsable compare la file à des dossiers résolus avant attribution. Niveau 1.

05. Idée de détection défensive. Décrire question, journaux autorisés et résultats attendus. Un ingénieur teste sur des événements contrôlés avant validation. Niveau 0.

06. Chronologie. Ordonner événements avec identifiant, heure d’origine, fuseau et conversion. L’enquêteur conserve les incertitudes et distingue succession et causalité. Niveau 0.

07. Constat de sécurité approuvé. Expliquer à l’ingénieur le comportement en cause et l’exigence concernée. Le responsable valide la correction et son test contrôlé. Niveau 0.

08. Preuves des fournisseurs. Relier chaque réponse au document, à la période et au service couvert. Signaler déclarations internes et lacunes au réviseur. Niveau 1.

09. Exercice sur table. Simuler des décisions sur un service et un objectif pédagogique. L’animateur suit les rôles approuvés et consigne les améliorations. Niveau 0.

10. Preuves de reprise. Réunir vérifications, exceptions ouvertes et essais fonctionnels. Le responsable métier décide si le service peut être déclaré rétabli. Niveau 1.

Préparer et valider un essai

Au niveau 0, l’assistant répond à une demande et une personne exécute chaque étape. Au niveau 1, il rassemble les éléments autorisés et prépare un brouillon. Il ne transmet aucun message et ne modifie aucun système. Consigner source, version de la consigne, autorisations, réviseur et critère d’arrêt.

Préparer une file en lecture seule avec identifiants de preuves et degré de certitude. Comparer une alerte grave inapplicable à un constat de score inférieur touchant un service important. Inclure des documents trompeurs et des instructions insérées dans les pièces. L’analyste compte faits omis et affirmations injustifiées. Laisser les actions externes désactivées.

Mesure et limites

Comparer des tâches équivalentes au processus courant. Consigner taille d’échantillon, temps de préparation, vérification et correction, défaillances importantes, autorisations et atteintes à la confidentialité. Inclure licence, intégration, formation, supervision et coût par exécution selon le cas. Les scores servent à choisir des essais. Le document ne rapporte aucun rendement mesuré dans un établissement. Le texte intégral présente consigne initiale, outils possibles, compétences et méthode pour chaque cas.

Références

[1] International Telecommunication Union. Global Cybersecurity Index 2024. Americas tier table, printed page 27; Jamaica is Tier 3, Establishing. National commitments, not institutional breach likelihood.

[2] Office of the Information Commissioner, Jamaica. Data Protection Standards. Official guidance, inspected 26 October 2026.

[3] National Institute of Standards and Technology. Incident Response Recommendations and Considerations for Cybersecurity Risk Management, Special Publication 800-61 revision 3. Final 3 April 2025. Official abstract and publication history inspected; cited for its scope, not a claim about model performance.

[4] United States Cybersecurity and Infrastructure Security Agency. Official Known Exploited Vulnerabilities data repository. README and source identity inspected 26 October 2026; catalogue data are updated over time.

[5] National Institute of Standards and Technology. Secure Software Development Framework version 1.1, Special Publication 800-218. February 2022.

[6] Agent Skills. Agent Skills Overview. Accessed 10 November 2026.

Cette édition abrégée accompagne le texte intégral en anglais.

Édition en anglais (PDF)