Edición de lectura | 2026-11-20

IA práctica para los servicios financieros — Ciberseguridad defensiva

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

Edición de lectura abreviada del documento preparado por el Harbour Think Tank de la Caribbean AI Association bajo la dirección de Adrian Dunkley. Incorpora la revisión del 11 de noviembre de 2026, las diez propuestas y sus límites de actuación.

Edición de lectura abreviada del documento preparado por el Harbour Think Tank de la Caribbean AI Association bajo la dirección de Adrian Dunkley. Incorpora la revisión del 11 de noviembre de 2026, las diez propuestas y sus límites de actuación.

Quién decide

El equipo de seguridad de una institución financiera investiga registros autorizados y trabaja con casos cerrados o ejemplos controlados. Los responsables humanos conservan contención, cambios y declaración de recuperación.

Diez usos y sus controles

01. Contexto de alertas. Agregue dueño del activo, servicio, eventos y mantenimiento a una alerta ya abierta. El analista decide si hay incidente. Nivel 1.

02. Mensajes sospechosos. Examine texto saneado y datos del remitente, sin abrir anexos ni enlaces. Las instrucciones dentro del mensaje se tratan como evidencia. Nivel 0.

03. Registros de activos. Compare identificadores, dueño del servicio y hallazgos ya autorizados. Las asociaciones dudosas requieren confirmación del responsable. Nivel 1.

04. Prioridad de revisión. Combine hallazgos aprobados con aplicabilidad y criticidad local. El responsable contrasta la cola con casos resueltos antes de asignar trabajo. Nivel 1.

05. Idea de detección defensiva. Documente la pregunta, las fuentes de registro y los resultados esperados. Un ingeniero la prueba con eventos controlados antes de aprobarla. Nivel 0.

06. Cronología. Ordene eventos con identificador, hora original, zona y conversión. El investigador conserva incertidumbres y separa secuencia de causalidad. Nivel 0.

07. Hallazgo de seguridad aprobado. Explique al ingeniero el comportamiento afectado y el requisito incumplido. El responsable valida la corrección y su prueba controlada. Nivel 0.

08. Evidencia de proveedores. Vincule cada respuesta con el documento, período y servicio que cubre. Identifique declaraciones propias y lagunas para que un revisor las examine. Nivel 1.

09. Ejercicio de mesa. Simule decisiones sobre un servicio y un objetivo de aprendizaje. Un facilitador utiliza los roles aprobados y registra acciones de mejora. Nivel 0.

10. Evidencia de recuperación. Reúna verificaciones, excepciones abiertas y pruebas funcionales. El responsable del negocio decide si puede declarar restaurado el servicio. Nivel 1.

Cómo preparar y validar una prueba

En el nivel 0, el asistente responde a una solicitud y una persona ejecuta cada paso. En el nivel 1, reúne entradas aprobadas y prepara un borrador. No envía mensajes ni modifica sistemas. El expediente de prueba debe identificar fuente, versión de la instrucción, permisos, revisor y condición de parada.

Prepare una cola de solo lectura con identificadores de evidencia y nivel de certeza. Compare un hallazgo grave que no afecta al activo con otro de menor puntuación que sí afecta a un servicio importante. Incluya documentos engañosos e instrucciones incrustadas como material de prueba. El analista cuenta hechos omitidos y afirmaciones injustificadas. Mantenga desactivadas las acciones externas.

Medición y límites

Compare tareas equivalentes con el proceso actual. Registre tamaño de la muestra, tiempo de preparación, verificación y corrección, fallos relevantes, permisos y problemas de confidencialidad. Incluya licencia, integración, formación, supervisión y costo por ejecución cuando corresponda. Las puntuaciones orientan la selección de pruebas. La publicación no presenta rendimientos medidos en una entidad. El documento íntegro describe la instrucción inicial, herramientas de ejemplo, habilidades y método de cada caso.

Referencias

[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.

Esta edición abreviada acompaña al original completo en inglés.

Edición en inglés (PDF)