Microsoft 365 Copilot

Shadow AI 위험 스프린트 키트

보안 및 IT 리더가 비인가 AI 사용, 과도한 정보 공유 위험, 데이터 보호 및 거버넌스에 대해 적절한 내부 이해관계자와 논의할 수 있도록 지원하는 일반 정보용 체크리스트와 실행 계획 도구입니다.



개요

Shadow AI 위험 스프린트 키트는 잠재적인 비인가 AI 사용, 데이터 처리 고려 사항 및 거버넌스 접근 방식에 대해 구조적인 논의를 진행할 수 있도록 설계된 일반적인 정보 제공용 프레임워크입니다. 이 자산은 관련 이해관계자 전반에 걸쳐 AI 관련 의사결정의 가시성, 우선순위 지정 및 조정을 팀이 논의하는 데 도움이 되도록 설계되었습니다.

본 자산은 조직의 환경에 맞게 조정되어야 하며, 사용 전에 최신 Microsoft 문서, 라이선스, 가용성, 그리고 해당되는 법률, 개인정보, 준수, 보안, IT, 조달, 비즈니스 요구사항과 비교하여 검토되어야 합니다.

내용

3
Shadow AI 위험 퀴즈

4
5일 스프린트 지도

5
실행 플래너

6
자세히 알아보기

이 스프린트 활용 시기

AI 애플리케이션, Copilot, 에이전트 및 확장이 내부 검토 프로세스와 다른 속도로 도입될 수 있는 경우, 이 스프린트는 퍼실리테이션 도구로 활용될 수 있습니다. 이 도구는 논의와 우선순위 설정을 지원하며, 필수 조치를 명시하지 않습니다.

제안된 스프린트 업무 중심 성과

- AI 도구와 데이터 접점에 대해 논의할 수 있는 작업용 목록을 작성하세요.
- 추가 검토가 필요한 영역을 파악하고 우선순위를 지정하세요.
- 잠재적인 데이터 보호 및 액세스 관련 고려 사항을 이해 관계자 검토를 위해 살펴보세요.
- 소유권 및 운영 주기를 포함한 잠재적인 거버넌스 접근 방안을 논의하세요.

면책 조항

이 콘텐츠는 정보 제공 목적으로만 제공됩니다. 이는 법률, 규제, 규정 준수 또는 기술적 조언을 구성하지 않으며, 탐지, 보호, 위험 감소 또는 규정 준수 결과를 보장하지 않습니다. 조직은 제품 기능, 가용성, 라이선스를 포함하여 의무, 위험 허용 범위 및 기술 환경 설정을 독립적으로 평가할 책임이 있습니다.

여기서 시작하기: 빠른 Shadow AI 위험 퀴즈

응답은 논의를 위한 방향성 있는 입력으로만 사용하세요. 우려 수준이 높은 응답이 여러 번 나타날 경우, 추가적인 가시성 확보, 이해관계자 검토 또는 우선순위 지정을 위한 주제를 제시할 수 있습니다. 여러 중간 수준 우려 반응은 책임, 정책 명확성 또는 증거 처리 절차의 필요성이 제기될 수 있는 영역을 제시할 수 있습니다. 대부분의 응답에서 우려 수준이 낮게 나타난다면, 해당 스프린트를 준비 상태 점검 및 최적화 활동으로 활용할 수 있음을 시사합니다.

이 퀴즈는 공식 평가, 채점 기준, 감사 또는 규정 준수 판단이 아니며, 다음 단계는 각 조직의 법적, 규제, 계약, 기술 및 운영 환경을 고려해야 합니다.

토론 질문	낮은 우려	중간 우려	높은 우려
현재 사용 중인 AI 앱, 확장 기능, Copilot, 플러그인 및 에이전트에 대한 최신 현황을 파악하고 계신가요?	□ 재고가 최신 상태인 것으로 보입니다.	□ 부분적인 가시성.	□ 신뢰할 수 있는 가시성이 없음.
AI 도구가 어떤 민감한 데이터에 접근할 수 있는지 확인할 수 있나요?	□ 액세스가 매핑된 것으로 보입니다.	□ 핵심 도구만.	□ 알 수 없거나 일관되지 않음.
승인된 AI 도구와 활용 경로가 명확한가요?	□ 경로가 분명해 보입니다.	□ 지침이 일관되지 않습니다.	□ 팀이 각각 독립적으로 도구를 선택합니다.
통제 조치가 AI 관련 데이터 경로에 매핑되어 있나요?	□ 제어가 매핑된 것으로 보입니다.	□ 일부 워크플로에 적용되었습니다.	□ AI 활용에 매핑되지 않음.
AI 거버넌스 결정에 대한 근거가 있나요?	□ 소유자와 일정이 정의된 것으로 보입니다.	□ 증거가 비정형적입니다.	□ 일관된 입증 경로가 없습니다.

5일 스프린트 지도

응답은 논의를 위한 방향성 있는 입력으로만 사용하세요. 우려 수준이 높은 응답이 여러 번 나타날 경우, 추가적인 가시성 확보, 이해관계자 검토 또는 우선순위 지정을 위한 주제를 제시할 수 있습니다. 여러 중간 수준 우려 반응은 책임, 정책 명확성 또는 증거 처리 절차의 필요성이 제기될 수 있는 영역을 제시할 수 있습니다. 대부분의 응답에서 우려 수준이 낮게 나타난다면, 해당 스프린트를 준비 상태 점검 및 최적화 활동으로 활용할 수 있음을 시사합니다.

이 퀴즈는 공식 평가, 채점 기준, 감사 또는 규정 준수 판단이 아니며, 다음 단계는 각 조직의 법적, 규제, 계약, 기술 및 운영 환경을 고려해야 합니다.

일	초점	행동	결과	체크리스트
1	잠재적인 비인가 AI 활용에 대해 논의합니다.	신호를 검토하고, 알려진 도구와 미지의 도구를 구분하며, 비즈니스 컨텍스트를 파악합니다.	재고 목록, 도구 목록 및 담당자 지정 초안.	□ 식별된 소스 □ 알 수 없는 도구 기록됨 □ 파악된 격차
2	잠재적 검토 영역 논의합니다.	사용 사례를 민감도, 액세스, 공유, 자동화 및 규정 준수 기준에 따라 그룹화합니다.	우선 순위가 지정된 논의 항목 및 이해관계자 검토 목록.	□ 데이터 경로 파악 완료 □ 우려가 높은 도구 확인됨 □ 제안된 소유자
3	데이터와 액세스를 보호하세요.	기본 통제, 데이터 보호 시나리오, 그리고 접근 또는 엔드포인트 관련 고려 사항을 논의하세요.	통제 고려 사항, 정책 항목 및 모니터링 영역.	□ 논의된 통제 □ DLP 또는 라벨 기록됨 □ 모니터링 공백 포착됨
4	AI 앱 및 에이전트 거버넌스 수립	소유권, 도입 프로세스, 예외 경로 및 증거 요구 사항 초안 작성.	역할, 검토 절차 및 증거 등록부 개념.	□ 소유자 식별됨 □ 예외 기록됨 □ 등록 시작됨
5	스프린트를 정례화하세요.	우선순위를 확인하고 지침 초안을 작성하며 30일 주기를 제안합니다.	계획 우선순위, 지침 개요, 발표 주제 및 주기.	□ 우선순위 문서화 □ 지침 초안 작성 □ 주기 제안

30일 실행 플래너 맵

추천 리더십 보고. 예시 주제로는 AI 사용 패턴, 데이터 관련 고려 사항, 실행 우선순위, 이해관계자 조율 및 단기 계획 수립이 포함됩니다.

우선순위	소유자	작업	증거/성공 지표	기한
1				
2				
3				
4				
5				
6				

Microsoft에서 자세히 알아보기

Microsoft Security 리소스에서 AI 사용의 보호 및 관리와 관련된 내용을 살펴보세요. 여기에는 데이터 보호, 신원 및 접근, 엔드포인트 보안, 책임 있는 AI 도입을 위한 가이드가 포함되어 있습니다.

미리 대비하여 Microsoft Security를 통해 안전하게 나아가세요.
인텔리전스와 신뢰가 공존하는 프론티어 혁신을 Microsoft AI를 통해 경험하세요.
Microsoft 365를 통해 AI 및 데이터 보안을 확보하여 생산성을 높이세요.

