

#3 Week: Shadow AI

 Schatten-KI ist die Nutzung von KI-Tools, die nicht für die Arbeit genehmigt wurden.

⚠ Meistens beginnt sie mit einer Abkürzung, die zunächst vernünftig erscheint. Die genehmigte Methode ist langsamer, und ein kostenloses Tool kann die Aufgabe in Sekunden erledigen. Das Problem ist, dass diese Tools erst nützlich werden, wenn man ihnen reale Informationen aus dem Arbeitskontext liefert.

⚠ Beispiel: Sie fügen ein Kundendokument in ein öffentliches KI-Tool ein, um eine schnelle Zusammenfassung zu erhalten. Sobald diese Informationen ein genehmigtes System verlassen, wissen Sie möglicherweise nicht, wo sie gespeichert sind oder wer darauf zugreifen kann.

👉 Ihre Aktion: Bevor Sie Arbeitsinformationen in ein KI-Tool einfügen, prüfen Sie, ob das Tool genehmigt ist und die Informationen sicher geteilt werden können. Wenn Sie unsicher sind, hören Sie auf und verwenden Sie die genehmigte Option oder fragen Sie das Sicherheitsteam.

 Die Herausforderung dieser Woche ist **Der sensible Prompt**. Sie werden ein realistisches KI-Tool-Szenario betrachten und entscheiden, was sicher geteilt werden kann.

👉 Nehmen Sie sich 3 Minuten Zeit, um das Szenario dieser Woche zu prüfen und Ihre **Red-Flag-Karte** zu sammeln.

[An der Challenge teilnehmen]

 Hören Sie sich **Episode 3: „Der sensible Prompt“** an, um zu erfahren, was mit Daten passieren kann, die in öffentliche KI-Tools eingefügt werden, und wie man KI bei der Arbeit sicher einsetzt.

[Jetzt anhören]

Schnell ist nützlich. Genehmigt ist sicherer.