Cheat Sheet zur Vorbereitung auf KI-Agenten-Sicherheit

Unternehmen versuchen heute schnellstmöglich KI-Agenten in Systemen, Cloud-Umgebungen und Kundenanwendungen einzuführen. Doch die Vorbereitung auf die neue Situation kann nicht immer mit der großen Motivation Schritt halten: Während **91 % aller Unternehmen** bereits KI-Agenten einsetzen, fehlt **fast 50 % eine Möglichkeit, diese Agenten formell zu überwachen.** Dies führt zu neuen Herausforderungen bei Governance und Kontrolle.

Die nicht-menschlichen Identitäten von KI-Agenten bieten zwar leistungsstarke neue Möglichkeiten, bergen jedoch im gleichen Maße erhebliche Risiken. Ohne ein starkes Identity-Framework erweitern KI-Agenten die Angriffsfläche und schaffen Sicherheitslücken, die mit klassischen Kontrollen nicht bewältigt werden können.

Für die sichere Verwaltung von KI-Agenten im großen Maßstab benötigen Unternehmen eine **Identity-First-Sicherheitsbasis, die den gesamten Agentenlebenszyklus absichert – vom ersten Pilotprojekt bis zum vollständigen Einsatz in Produktionsumgebungen.**

Verwenden Sie dieses Cheat Sheet zur Vorbereitung auf die sichere KI-Nutzung als Kurzanleitung für Identity-Sicherheitspraktiken, die Ihnen helfen, für alle KI-Agenten-Ökosysteme **Transparenz zu gewährleisten, Kontrollen durchzusetzen und im großen Maßstab Compliance zu überprüfen**.

Die meisten Unternehmen setzen bereits KI-Agenten ein, aber fast 50 % fehlt eine Möglichkeit, diese Agenten formell zu überwachen.

Wichtige Identity-Sicherheitspraktiken für KI-Agenten-Ökosysteme

Governance für alle Agenten

Gewährleistung zentraler Transparenz und Kontrolle für KI-Agenten im gesamten Unternehmen

01.

Erkennung und Überwachung von KI-Agenten und nicht-menschlichen Identitäten

Erkennen und überwachen Sie kontinuierlich KI-Agenten und zugehörige Service-Accounts in allen Umgebungen. Dadurch wird verhindert, dass nicht verwaltete Identitäten außerhalb der etablierten Governance- oder Überwachungskontrollen agieren.

02.

Einrichtung einer zentralen Registrierungsstelle für Agenten

Registrieren Sie erkannte Agenten und weisen Sie einen Besitzer sowie Berechtigungen zu. Mit einer zentralen Registrierungsstelle wird die Verantwortlichkeit, die Auditierbarkeit und die Transparenz für alle KI-Systeme verbessert.

03.

Zentralisierte Governance für KI-Agenten-Identitäten

Verwalten Sie Provisionierung, Authentifizierung, Autorisierung und Deprovisionierung über ein zentrales Identity-System. Eine einheitliche Plattform beseitigt Fragmentierung, verbessert die Richtlinienkonsistenz und unterstützt die Skalierbarkeit.

04.

Kontinuierliche Überwachung von KI-Agenten-Aktivitäten in Echtzeit

Überwachen Sie Authentifizierungsaktivitäten, API-Aufrufe und Verhaltensmuster von KI-Agenten in Echtzeit. Mithilfe von Echtzeit-Transparenz können Sie Missbrauch, Anomalien oder kompromittierte Anmeldedaten schnell erkennen.

05.

Protokollierung und Überprüfung von KI-Agenten-Aktionen in allen Systemen

Erfassen und überprüfen Sie Authentifizierungs-ereignisse, Zugriffsversuche und von Agenten initiierte Aktionen. Eine starke Protokollierung unterstützt die Reaktion auf Vorfälle, die Validierung der Compliance und die Durchsetzung von Governance-Maßnahmen.

Absicherung aller Agenten

Bereitstellung von KI-Agenten, die sicher, vorhersehbar und entsprechend dem Unternehmensziel handeln

06. Bindung von Agenten-Sessions an eine verifizierte menschliche Identität

Bevor eine Agenten-Aktion stattfindet, legen Sie eine verifizierte menschliche Identität fest, damit alle Aktionen zurechenbar, verantwortlich und vertrauenswürdig sind.

07. Schutz von Token, Anmeldedaten und Secrets in einem dedizierten Vault

Speichern Sie langlebige Token, Anmeldedaten und Secrets in einem sicheren, isolierten Vault anstatt sie in Agenten einzubetten. Stellen Sie zur Laufzeit kurzlebige Token aus, um das Gefährdungspotenzial zu verringern und Datenlecks zu verhindern.

08. Durchsetzung von Autorisierungsprüfungen und Human-in-the-Loop-Kontrollen

Gewähren Sie Agenten nur dann Berechtigungen zum Handeln, wenn dies zulässig ist, und legen Sie fest, dass bei Aktionen mit höherem Risiko die Genehmigung durch einen Menschen erforderlich ist.

09. Durchsetzung von Zugriff für KI-Agenten nach dem Least-Privilege-Prinzip

Begrenzen Sie den Handlungsspielraum für Agenten auf autorisierte Ressourcen und Aktionen, die zum Zeitpunkt der Abfrage evaluiert werden. So wird sichergestellt, dass Berechtigungsbereiche eingehalten werden und das Verhalten vorhersehbar ist.

Verwandeln Sie Vorbereitung in Maßnahmen

Sind Sie bereit, die Kontrolle über Ihr KI-Agenten-Ökosystem zu übernehmen? Nutzen Sie unsere umfassende Checkliste für die Sicherheit und Compliance von KI-Identitäten, um Ihre nächsten Schritte für die Sicherheit und Compliance von KI-Identitäten zu planen.