VORTEILE VON KI-GESTÜTZTEM IAM, PAM UND IGA IN VERSCHIEDENEN BRANCHEN

VON PATECCO

KI IN IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

- Der Einsatz künstlicher Intelligenz (KI) in den Bereichen Identitäts- und Zugriffsmanagement (IAM), Privileged Access Management (PAM) sowie Identitäts-Governance und -Verwaltung (IGA) verändert die Cybersicherheitsstrategien in einer Vielzahl von Branchen.
- Durch die Nutzung der Fähigkeit von KI, große Datensätze zu analysieren, potenzielle Bedrohungen vorherzusagen und eine Echtzeit-Erkennung bereitzustellen, können Organisationen ihr Sicherheitsframework erheblich stärken, ihre Abläufe optimieren und die Einhaltung gesetzlicher Vorschriften sicherstellen.

FINANZBRANCHE

- **Echtzeit-Betrugserkennung:**
  Das KI-gesteuerte IAM überwacht Transaktionen kontinuierlich, um Anomalien wie ungewöhnliches Verhalten zu erkennen, und markiert verdächtige Aktivitäten in Echtzeit, um potenziellen Betrug zu verhindern.
- **Dynamische privilegierte Zugriffskontrolle:**
  Schützt den Zugriff auf Finanzsysteme, Kundenkonten, Transaktionsdaten und Handelsplattformen. Minimiert das Risiko eines unbefugten Zugriffs auf wichtige Finanzdaten.
- **Automatisiertes Compliance- und Risikomanagement:**
  Die KI-gestützte IGA automatisiert Zugriffszertifizierungen, Prüfpfade und Compliance-Berichte und identifiziert schnell übermäßige Berechtigungen oder Rollenkonflikte. Dies reduziert den manuellen Arbeitsaufwand und hilft Institutionen dabei, die Einhaltung gesetzlicher Vorschriften zu gewährleisten.
- **Ergebnis:** Höhere Sicherheit, geringeres Risiko und kontinuierliche Einhaltung gesetzlicher Vorschriften.

VERSICHERUNGEN

- **Betrugserkennung und –Prävention:**
  IAM analysiert kontinuierlich das Nutzerverhalten und Transaktionsmuster, um Anomalien im Zusammenhang mit betrügerischen Forderungen oder unbefugten Aktivitäten zu identifizieren, und ermöglicht so Echtzeit-Warnmeldungen und schnelle Reaktionen.
- **Kontextbewusstes privilegiertes Zugriffsmanagement:**
  Schützt den Zugriff auf sensible Informationen wie Versicherungsnehmerdaten, Finanzunterlagen und Schadensdatenbanken.
- **Automatisierte Governance und Compliance:**
  IGA optimiert Audits und die Einhaltung von Vorschriften wie DORA und DSGVO durch die Automatisierung von Zugriffsüberprüfungen, die Pflege von Prüfpfaden und die Identifizierung von Richtlinienverstößen.
- **Ergebnis:** Verbesserte Betrugserkennung, sicherer Zugriff auf sensible Daten und optimierte Einhaltung von Vorschriften.

PHARMA

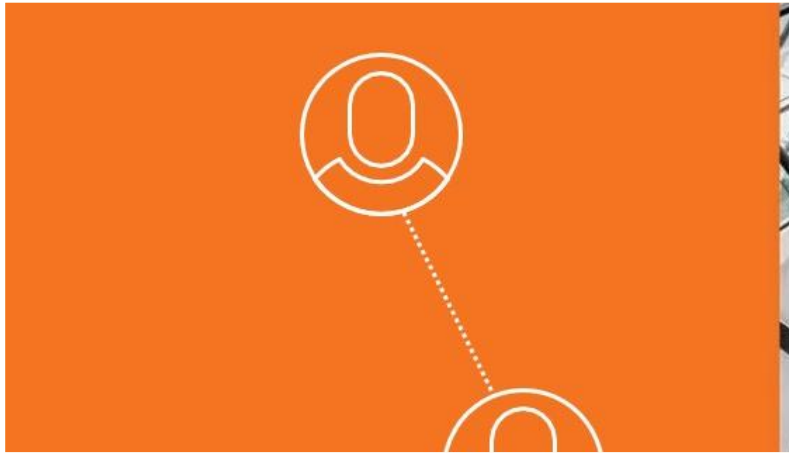
- **Sicherer Zugriff auf Forschungsdaten:** IAM-Systeme überwachen den Zugriff auf proprietäre Forschungs- und klinische Studiendaten, erkennen ungewöhnliche Zugriffsmuster und verhindern die unbefugte Nutzung sensibler Informationen.
- **Privileged Access Management:** Schützt sensible Daten: Patientenakten, Daten aus klinischen Studien, geistiges Eigentum (Formeln, Forschungsergebnisse). Erkennt den Missbrauch von Anmeldedaten oder die Ausweitung von Berechtigungen, bevor es zu einer Sicherheitsverletzung kommt.
- **Automated Compliance and Audit Readiness:** IGA vereinfacht die Einhaltung von Vorschriften wie NIS2, HIPAA und DSGVO, indem es Zugriffsüberprüfungen automatisiert, Prüfpfade generiert und Verstöße gegen Richtlinien aufzeigt, bevor sie eskalieren.
- **Ergebnis:** Verbesserter Datenschutz, geringeres Risiko unbefugter Zugriffe und effizientes Compliance-Management.

ENERGIE

- **Schutz kritischer Infrastrukturen:**
  IAM überwacht den Zugriff auf Steuerungssysteme und Betriebsplattformen und erkennt dabei ungewöhnliches Verhalten, das auf Insider-Bedrohungen oder Cyberangriffe auf kritische Infrastrukturen hindeuten könnte.
- **Privilegiertes Zugriffsmanagement für OT- und IT-Systeme:**
  Schützt den Zugang zu kritischen Infrastruktursystemen wie Stromnetzen, Raffinerien, Pipelines und SCADA/ICS-Systemen. Schützt vor Cyberangriffen, die kritische Energiesysteme gefährden könnten, und minimiert Betriebsausfälle und finanzielle Auswirkungen.
- **Automatisierte Compliance- und Risikoüberwachung:**
  IGA unterstützt die Compliance, indem Zugriffsrechte automatisch geprüft und unautorisierte Berechtigungen erkannt werden.
- **Ergebnis:** Verbesserter Schutz kritischer Infrastrukturen, sicherer OT/IT-Zugang und optimierte Compliance.

INGENIEURWESEN

- **Schutz des geistigen Eigentums:**
  IAM überwacht den Zugriff auf Konstruktionsdateien, Quellcode und proprietäre Engineering-Daten, erkennt ungewöhnliche Zugriffsmuster und verhindert die unbefugte Offenlegung von Daten.
- **Kontrollierter privilegierter Zugriff auf kritische Systeme:**
  Schützt sensible technische Daten wie Entwürfe, Blaupausen, geistiges Eigentum und proprietäre Software. Minimiert die Wahrscheinlichkeit eines unbefugten Zugriffs auf kritische Systeme, darunter CAD-, PLM- und Projektmanagement-Plattformen.
- **Automatisierte Governance und Compliance:**
  IGA automatisiert Zugriffsüberprüfungen, setzt rollenbasierte Kontrollen durch und führt Prüfprotokolle, wodurch Ingenieurbüros dabei unterstützt werden, vertragliche, gesetzliche und interne Compliance-Anforderungen zu erfüllen.
- **Ergebnis:** Gesichertes geistiges Eigentum, kontrollierter Systemzugriff und vereinfachte Compliance für effiziente Abläufe.



ZUSAMMENFASSUNG

- KI-gestützte IAM-, PAM- und IGA-Lösungen ermöglichen proaktive und adaptive Identitätssicherheit.
- Echtzeitanalysen und Verhaltensdaten helfen dabei, Betrug und Insider-Bedrohungen zu verhindern.
- Automatisierte Governance verbessert die Compliance-Genauigkeit und die Audit-Bereitschaft.
- Kontextbezogene und zeitnahe Zugriffsrechte reduzieren das Risiko des Missbrauchs von Privilegien.
- KI-gestützte Identitätslösungen unterstützen Skalierbarkeit und langfristige digitale Resilienz.

Kontaktieren Sie uns. Wir unterstützen Sie gerne!

- PATECCO GmbH
- +49(0) 23 23 - 987 97 96
- info@patecco.com
- www.patecco.com