Cloud Security 360°

Warum wir trotz aller Tools noch immer angreifbar sind…

Reffat Gharaibeh, Cloud Security Architect, Controlware GmbH

18.03.2026, Stuttgart

CNAPP
Cloud Native Application Protection Platform

Code + Build Security
- Prüfung von App Artefakten
- IaC Scanning
- Governance Policies
- CI/CD

CSPM
- Assetmanagement
- Fehlkonfigurationen erkennen
- Compliance sicherstellen

CWPP
- Runtime Protection
- Vulnerability Management
- Erkennung von Anomalien

CIEM
- „Overprivileged Identites“
- Anomalien
- Identitäts-basierte Angriffsflächen reduzieren

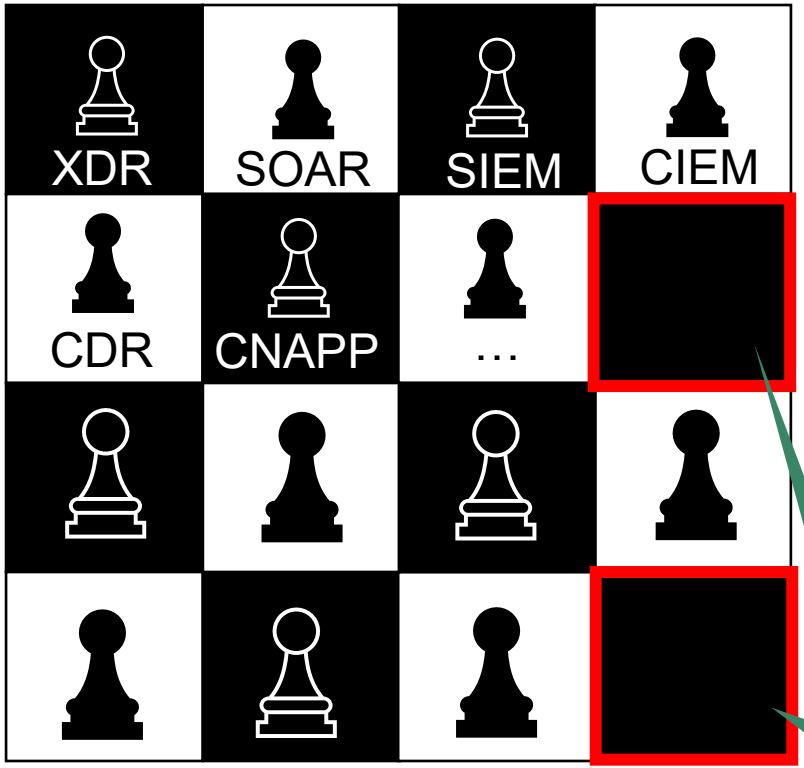
API Security
Überwachung von:
- Interne & Externe APIs
- API-Tokens

Data Security
- Sichtbarkeit & Compliance
- Klassifizierung
- Überwachung Cloud Storage

Cloud Detection and Response
Erkennung, Korrelation und automatisierte Reaktion auf Angriffe in der Cloud Umgebung

Die Vorstellung von Sicherheit

Security wird in Bereichen gedacht, die es „abzudecken gilt“…



Hier fehlt uns (nur) noch ein Tool!
Dann haben wir es geschafft!

Die Illusion von Sicherheit

Warum Cloud Security trotz umfangreicher Tools und Compliance scheitert

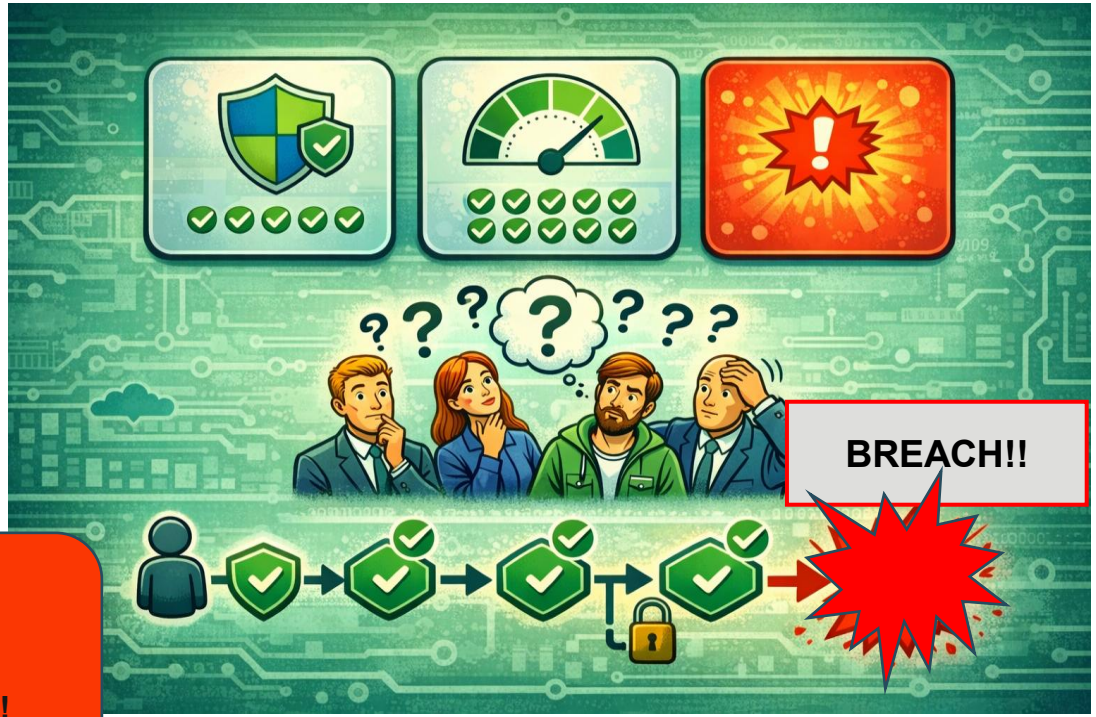
Tools Stacks implementiert!

Modernste Security Lösungen im Einsatz. Best Practices umgesetzt.

Dashboards zeigen: Compliant!

Alle Metriken im grünen Bereich. Keine kritischen Alerts / Schwachstellen.

Trotzdem:
Kritischer Sicherheitsvorfall!
aber nicht wegen fehlender Tools …



Wenn Best Practice + Best Practice = Worst Case

Das Emergenz-Problem

Config A: Best Practice!

Service Account mit S3-ReadOnly

Security Review: *„Appropriate for use case“*

Config B: Best Practice!

Lambda mit Assume-Role für Service Account.

Security Review: *"Standard integration pattern"*

Config C: Best Practice!

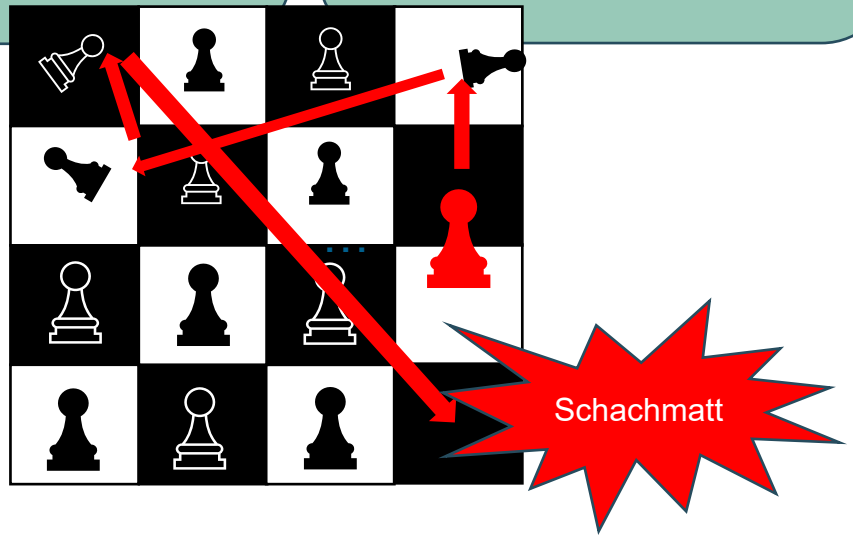
Cross-Account-Trust für Partner-Integration

Security Review: *"Business requirement, properly scoped"*

Emergentes Risiko: KRITISCH

Partner-Entwickler → Lambda ausführen → Service Account annehmen → Cross-Account-Trust nutzen → Unternehmensdaten exfiltrieren

Einzelbewertung: 3× LOW RISK ✓
CNAPP-Alert: KEINER
Pfad-Bewertung: CRITICAL 🔴



Configuration Compliance vs. Attack Surface Analysis

Der fundamentale Unterschied

Configuration Compliance

Was Tools beantworten

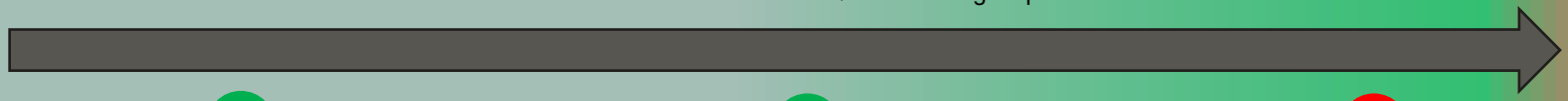
- Ist die Konfiguration konform mit Policies
- Folgt sie Best Practices?
- Ist sie dokumentiert und genehmigt
- Entspricht sie regulatorischen Anforderungen?

Ergebnis: „Ja/Nein“ für einzelne Konfiguration

Attack Surface Analysis

Wo Tools an Grenzen stoßen

- Welche **zusätzlichen** Pfade durch gültige Konfigurationen entstehen
- Wie sich erreichbare Ziele für Angreifer **in der Praxis** verändern
- Welche transitiven Berechtigungen sich im **Gesamtbild** ergeben?
- Neue / kreative Angriffspfade + Techniken



Configuration Compliance

Best Practice Validation, Policy Enforcement, Dokumentation

Attack Surface Reality

Well Known Path Combinations, Anomalies, automated Testing

Der blinde Fleck

Automated coverage ≠ vollständiges Bild der Angriffspfade

„Compliance prüft die Konfiguration. Attack Surface Analysis prüft die Konsequenz."

Warum diese Schieflage kritisch ist

Reaktive statt proaktive Sicherheit

Tools allein reagieren nur auf bekannte Bedrohungen. Unternehmen verpassen neue Angriffsvektoren und komplexe Bedrohungsszenarien.

Fehlende Priorisierung

Ohne strategischen Fokus werden alle Alerts gleich behandelt. Kritische Risiken gehen in der Masse unter, während Teams mit False Positives überfordert sind.

Mangelnder Business-Kontext

Security-Teams verstehen nicht, welche Assets wirklich geschäftskritisch sind. Ressourcen werden falsch allokiert und echte Risiken unterschätzt.

Security „Theater“ vs. Echte Sicherheit

Wenn Sicherheit gut aussieht – aber nichts bringt…

Das Phänomen

- Viele Kontrollen implementiert
- Viele Reports generiert
- Viel Gefühl von Sicherheit
- Fokus auf Tool, nicht auf Wirkung
- Checklisten & Compliance statt echte Angriffsmodelle

→ **Wenig tatsächliche Risikoreduktion**

„Maximum Coverage“

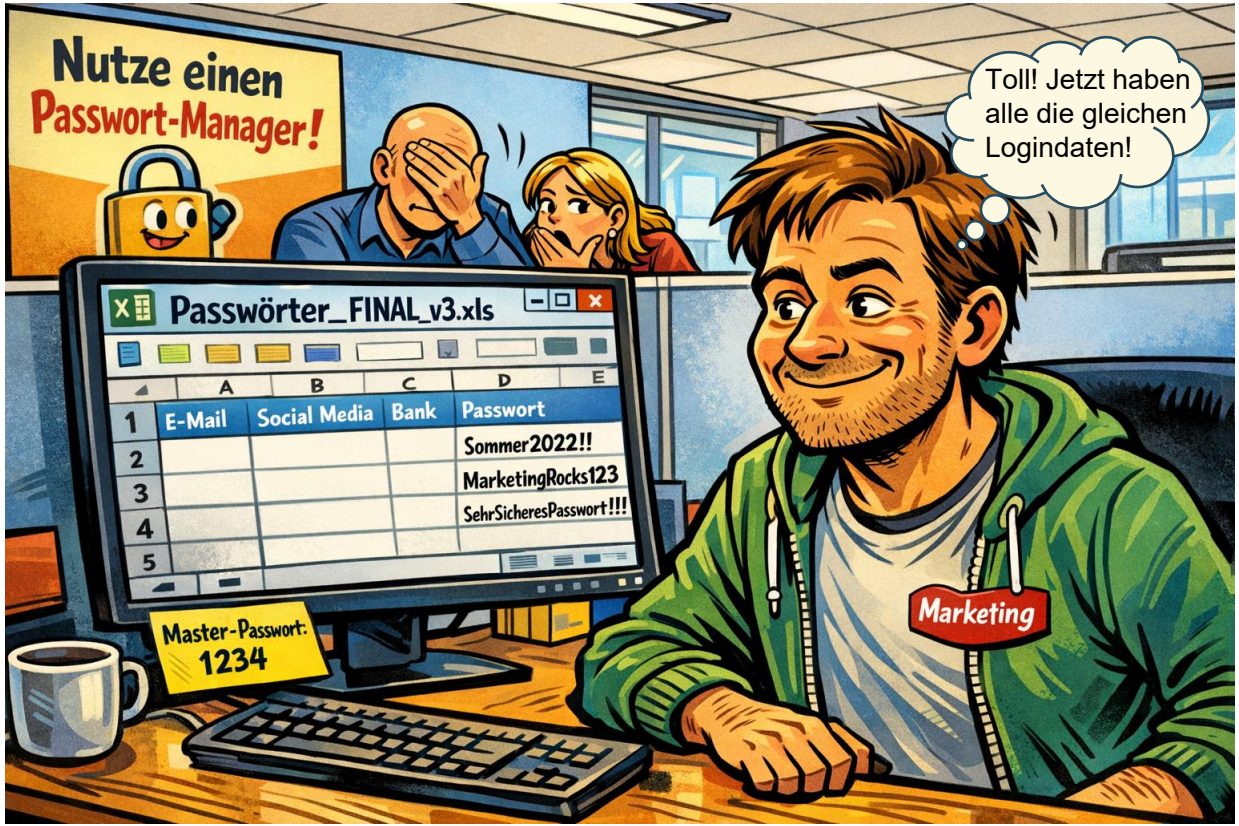
„Security Theater“	Risk-Driven Security
100 Findings behoben	3 kritische Angriffspfade geschlossen
Dashboard grün	Attack-Surface reduziert
Checkboxen erfüllt	Business-kritische Assets geschützt

Echte Sicherheit

- Fokus auf **Risikoreduktion** statt Tool-Coverage
- **Top-Angriffspfade** und deren Schließung
- Schutz von **Business-kritischen Assets** im Zentrum
- Kombination aus Technik + Prozess + Mensch
- Kontrollen werden nach Business-Kontext ausgerichtet

Der Faktor Mensch – „Bob“ aus der Marketingabteilung

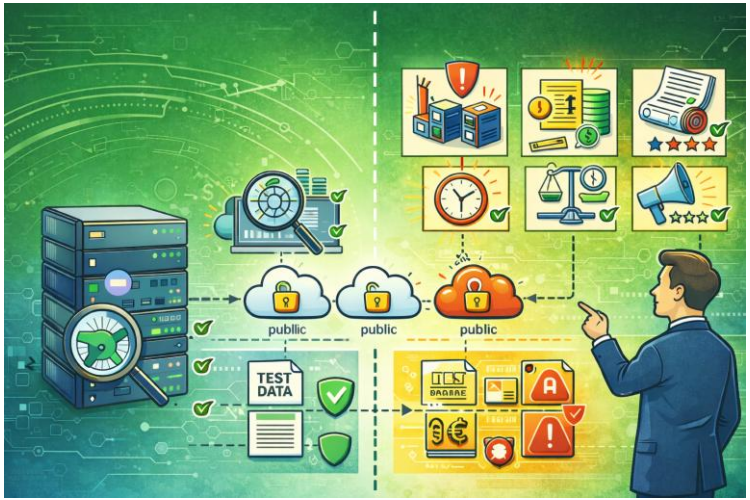
- Bob nutzt moderne **SaaS-Tools, Social Media** und Kampagnenplattformen
- Arbeitet unter **Zeitdruck**
- **Passwörter speichert er in einer Excel-Datei** → So kann er bequem darauf zugreifen und auch seinen Teamkollegen **Zugriff** darauf **gewähren**



Der Faktor Mensch – Kausalitätsbringer!

Risiko braucht Kontext – und Kontext braucht Menschen

Was Tools sehen
- Konfigurationen
- Berechtigungen
- Netzwerk Topologie
- Ressourcen Status
- Schwachstellen / CVEs
- Bekannte Angriffspfade



Was Menschen verstehen
- Business-Kritikalität
- Datenwert
- Zeitliche Dringlichkeit
- Regulatorische Implikationen
- Reputationsrisiko

Technische Sicht	Business-Kontext	Reales Risiko
S3-Bucket mit Read-Public	Test-Dummy-Daten	LOW ✓
S3-Bucket mit Read-Public	Kundenzahlungsdaten	CRITICAL 🔴

→ *Technisch identisch. Risiko fundamental unterschiedlich.*

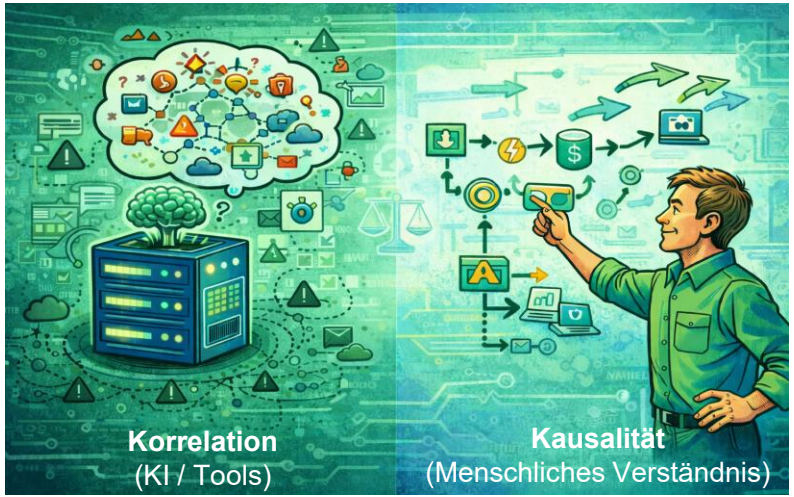
Die Formel: Risiko = Technische Schwäche × Business-Impact. Ohne Business-Kontext ist jede Risikoeinschätzung unvollständig.

Kausalität schlägt Korrelation

Warum Muster erkennen, nicht bedeutet Zusammenhänge zu verstehen!

Korrelationsbasierte Tools

- Lernen aus historischen Breaches
- Erkennen bekannte Muster
- "Das war schon mal gefährlich"
- **Problem: Neue Attack Chains haben keine Historie**



Korrelation
(KI / Tools)

Kausalität
(Menschliches Verständnis)

Kausales Verständnis

- Verstehen von Wirkmechanismen
- Simulieren neue Szenarien
- "Deshalb ist es gefährlich„
- **Vorteil: "What-if"-Analysen möglich**

Was KI sieht (Korrelation)

"Service Account + S3 Access + Lambda" korreliert mit 73% der Data Breaches in unserer Trainingsdaten

Was Menschen verstehen (Kausalität)

"Lambda kann Service Account annehmen → dieser hat S3-Read → wenn Cross-Account-Trust existiert → dann kann externes Konto Daten lesen"

"Ein Tool zeigt uns das 'Was'. Menschen verstehen das 'Warum' und können das 'Was wäre wenn' durchspielen."
*Security-Tools (inklusive KI) zeigen **"Diese Dinge treten gemeinsam auf"** (Korrelation). Was fehlt: **"Deshalb führt A über B zu C"** (Kausalität).*

CSPM vs. Security Checkups

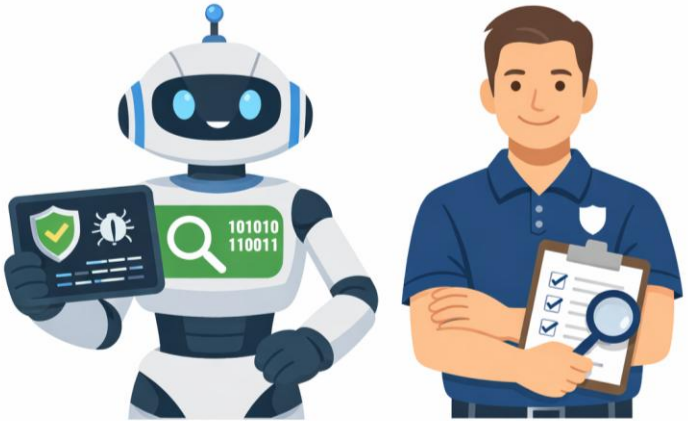
Vom Scannen zur echten Sicherheitsbewertung

CSPM – Automatisierung

Autopilot-Modus
Automatisierte Fehlkonfigurations-Scans

Compliance Bewertung
Regelbasierte Standard-Benchmarks

Skalierbar
Multi-Cloud-Abdeckung, versch. Benchmarks/Frameworks



CSPM zeigt Symptome.

“Security Checkups” zeigen die Ursachen.

Security Checkups – Menschen

Erfahrener Pilot
Architekturanalyse mit Kontext

Tiefenprüfung
Hinterfragen von Trust-Modellen

Reale Risiken
Identifikation echter Angriffswege

Individuelle Bewertung
Kontextbasierte Risikoanalyse

CNAPP vs. Cloud Penetration Testing

CNAPP

Continious Scanning
CSPM, CWPP, CIEM, IaC, CDR, Attack Path

Misconfiguration & Compliance Monitoring
Benchmarking & Controls

Vulnerability Scanning
Multi-Layer CVEs

Policy Enforcement & Risk Scoring

Cloud Penetration Testing

Angriffsimulation
Angriffsketten über mehrere Services

Privilege Escalation
Übernahme/Erweiterung von Identitäten/Rechten

Business Logic Exploits
Ausnutzen von “Regelkonformen” Konfigurationen & Architekturen

Realisitisch Impact- Bewertung
“Das ist möglich!”

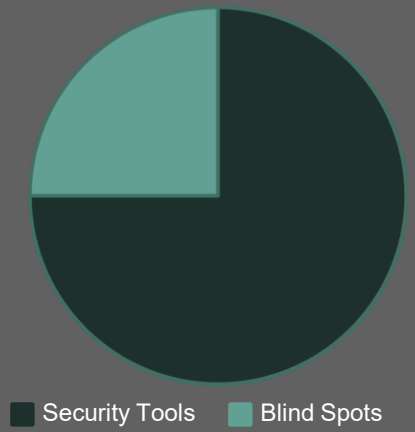
Kreative Abuse-Szenarien
Erschließung neuer Angriffstechniken on the fly

“Ein CNAPP zeigt Ihnen, wo Türen offen stehen.”
“Ein Cloud Penetration Test zeigt, ob ein Angreifer dadurch ins Gebäude gelangt – und was er dort erreichen kann.”

Cloud Security 360° – Die vollständige Risiko-Abdeckung

HEUTE

Realität: Tool-fokussierter Ansatz



Security Tools & Controls (CSPM, CIEM, EDR, etc.)

Keine Abdeckung: 'Blind Spots' und kritische Lücken

NOTWENDIG

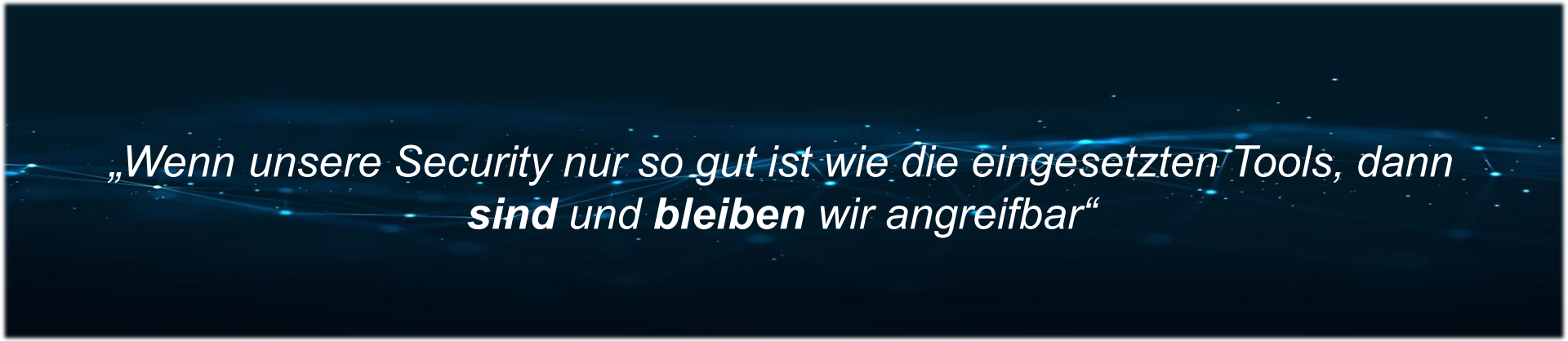
360°-Ansatz: **Balanced Security**

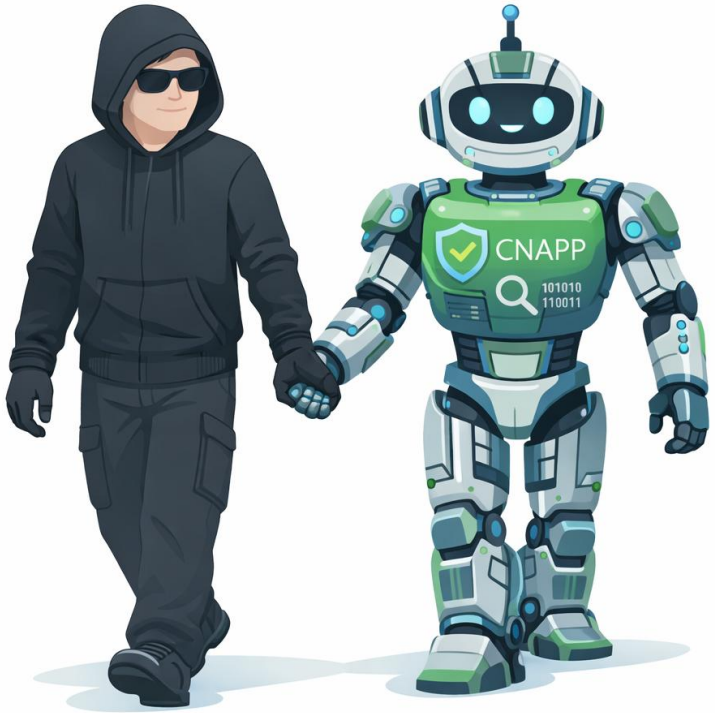
Security Tools
Kausales Verständnis
Fokus & Faktor Mensch
Angriffspfad
Business-Kontext

Ziel:

Gleichmäßige Abdeckung über fünf kritische Sicherheitsdimensionen hinweg.

Zum Abschluss





„Bereit für einen 360˚-Blick auf Ihre Cloud-Sicherheit? Kontaktieren Sie uns für ein individuelles Assessment.“

IT-Security
Roadshow 2026

controlware

Danke für Ihre Aufmerksamkeit.