sure[secure]
your security operations center

secure mag

EVOLUTION DER SOC-ARCHITEKTUREN:

VON *ON-PREM* ZU *AI-NATIVEN* MODELLEN

Einordnung technologischer Entwicklungsstufen zwischen Kontrolle, Skalierung und Automatisierung

Einleitung

Security Operations Center (SOC) sind nicht im luftleeren Raum entstanden. Sie sind das Ergebnis konkreter technischer Zwänge, wachsender Bedrohungslagen und strategischer Entscheidungen von IT- und Security-Verantwortlichen.

Ein kurzer Blick zurück hilft, die heutige Diskussion einzuordnen: Die Ursprünge moderner SIEM-Systeme reichen in die frühen 2000er-Jahre zurück. Lösungen wie NetForensics oder später ArcSight kombinierten erstmals Log-Management mit Security Event Correlation. Ziel war es, aus isolierten Ereignissen ein Gesamtbild zu erzeugen, als Reaktion auf zunehmend verteilte Angriffe und steigende Compliance-Anforderungen.

Diese Entwicklung markiert einen Wendepunkt: Sicherheit wurde nicht mehr nur als Prävention verstanden, sondern als kontinuierliche Beobachtung und Bewertung von Ereignissen. In diesem Kontext haben sich SOC-Architekturen weiterentwickelt: von physisch kontrollierten On-Premise-Umgebungen über skalierbare Cloud-Modelle bis hin zu ersten AI-gestützten Betriebsansätzen.

Diese Entwicklung wird häufig als lineare Erfolgsgeschichte dargestellt: mehr Daten, mehr Automatisierung, mehr Effizienz. Eine solche Perspektive greift jedoch zu kurz. Jede Evolutionsstufe bringt neben Fortschritt auch neue Abhängigkeiten, Risiken und strukturelle Spannungsfelder mit sich.

Dieses Whitepaper analysiert die zentralen Architekturphasen kritisch und nimmt bewusst die Perspektive von Entscheidern ein: Warum wurden diese Modelle jeweils als „richtig“ angesehen, und wo liegen ihre Grenzen? Zudem stellt sich die Frage, ob „AI-native“ tatsächlich einen Paradigmenwechsel darstellt oder primär eine neue Abstraktionsschicht über bestehenden Herausforderungen.

On-Prem SOC:
Kontrolle als Ausgangspunkt

Die erste Generation moderner SOC-Architekturen war geprägt von maximaler Kontrolle. Sicherheitsinfrastruktur, Logdaten, Analysewerkzeuge und Prozesse befanden sich vollständig innerhalb der eigenen Rechenzentren, häufig physisch greifbar als „Blech im Keller“.

Charakteristika

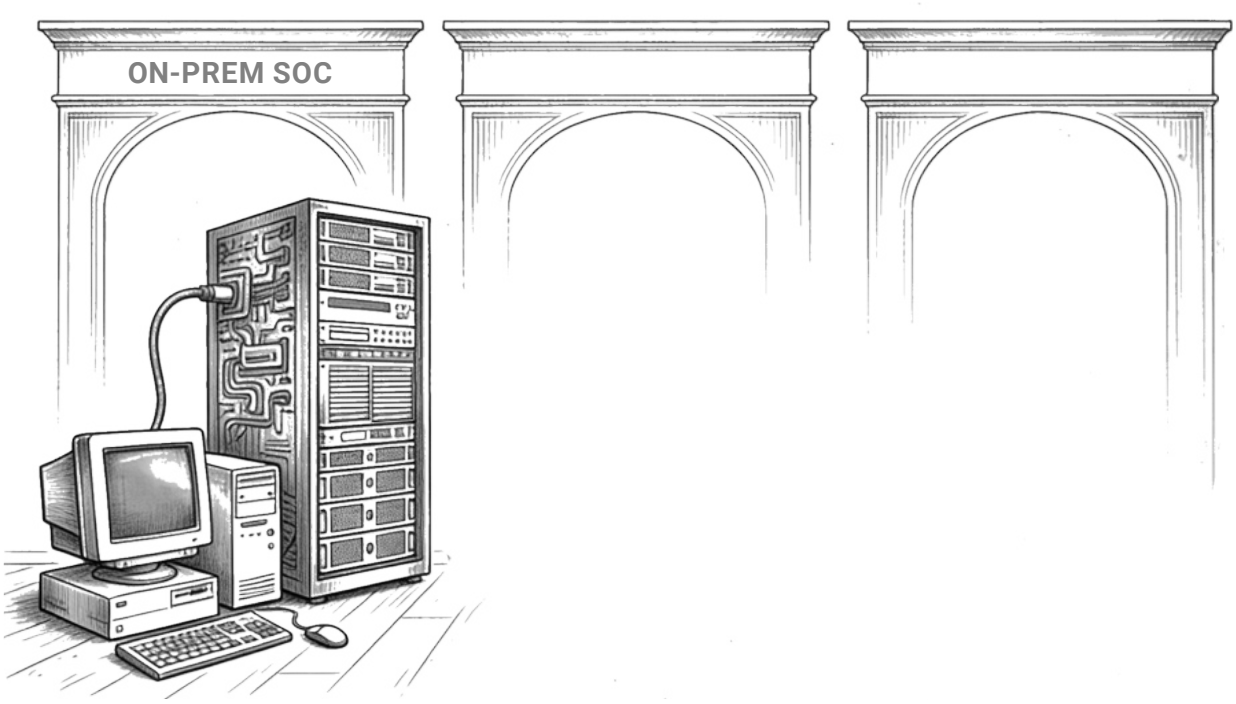
- Zentralisierte SIEM-Systeme
- Klare Netzwerkperimeter
- Statische Use Cases & Korrelationsregeln
- Hohe Investitionskosten (CapEx)
- Physische Infrastruktur im Eigenbetrieb

Technische Infrastruktur

Typischerweise bestand ein On-Prem SOC aus einer klar geschichteten Architektur:

- Logquellen (Firewalls, IDS/IPS, Server, Endpoints)
- Log Collector & Forwarder
- Zentrales SIEM (oft als dedizierter Cluster)
- Storage-Systeme (SAN/NAS) für Langzeitaufbewahrung
- Separates Netzwerksegment für Security-Systeme

Die Datenflüsse waren weitgehend linear: Erfassung > Aggregation > Korrelation > Alerting. Skalierung erfolgte vertikal oder durch zusätzliche Hardware-Knoten. Diese Architektur entsprach der damaligen IT-Realität: klar abgegrenzte Netzwerke, begrenzte Datenquellen und vergleichsweise stabile Bedrohungsszenarien.



Limitierender Faktor: Hardware

Das On-Prem SOC war untrennbar mit physischer Infrastruktur verbunden. Speicher, Rechenleistung und Netzwerkkomponenten mussten vorab dimensioniert und regelmäßig erweitert werden. Dieses Modell führte zu einem strukturellen Problem: Sicherheitsanforderungen wachsen nicht linear.

Neue Logquellen, höhere Retentionszeiten oder zusätzliche Analysefunktionen erforderten kontinuierliche Nachrüstung. Jede Erweiterung bedeutete neue Hardware: Beschaffung, Integration, Betrieb. Die Folge waren hohe und schwer planbare Investitionskosten. Insbesondere bei stark wachsenden Datenvolumina entwickelte sich das SOC zunehmend zu einem infrastrukturellen Kostenblock.

Sicht der Entscheider

Trotz dieser Einschränkungen galt das On-Prem SOC lange als alternativlos, vor allem aus Sicht von Entscheidern. Das zentrale Argument war Kontrolle gleich Sicherheit. Daten verließen das eigene Rechenzentrum nicht, Systeme waren physisch isoliert. Diese „Kellerlogik" prägte über Jahre die Sicherheitsstrategie vieler Organisationen.

Insbesondere in regulierten Branchen wurde diese Architektur als einziger gangbarer Weg betrachtet, um Compliance-Anforderungen zu erfüllen und Risiken zu minimieren.

Stärken

Der größte Vorteil lag in der vollständigen Datenhoheit. Sensible Sicherheitsdaten verließen zu keinem Zeitpunkt die eigene Infrastruktur. Dies erleichterte regulatorische Compliance erheblich. Zudem war die Systemkomplexität – gemessen an heutigen Maßstäben – überschaubar. Abhängigkeiten waren klar definiert, Integrationen begrenzt.

Schwächen

Mit zunehmender Digitalisierung stieß dieses Modell jedoch an strukturelle Grenzen. Die Skalierung von Speicher- und Rechenkapazitäten wurde teuer und unflexibel. Gleichzeitig nahm die Anzahl relevanter Datenquellen exponentiell zu. Laut einer Studie von IBM verursachten Datenvolumen und Komplexität bereits früh signifikante Verzögerungen bei der Angriffserkennung.[1]

Ein weiteres Problem war die starre Logik der Detektion. Regelbasierte Systeme konnten nur bekannte Muster erkennen. Unbekannte Angriffstechniken blieben häufig unentdeckt.

Kritische Einordnung

Das On-Prem SOC war kein ineffizientes Modell, es war ein Modell für eine andere Zeit. Und heute stößt es in vielen Umgebungen an seine Grenzen. Seine größte Stärke, die Kontrolle, wurde gleichzeitig zur größten Einschränkung, sobald IT-Umgebungen dynamischer wurden.

Gleichzeitig prägte es ein Sicherheitsverständnis, das bis heute nachwirkt: Sicherheit wird mit physischer Nähe und Isolation gleichgesetzt. Ein Paradigma, das in späteren Evolutionsstufen zunehmend infrage gestellt wird.

Cloud-native SOC: Skalierung als Versprechen

Mit der Verlagerung von Workloads in die Cloud veränderten sich auch die Anforderungen an Sicherheitsarchitekturen. SOCs mussten plötzlich hochdynamische, verteilte Umgebungen überwachen.

Charakteristika

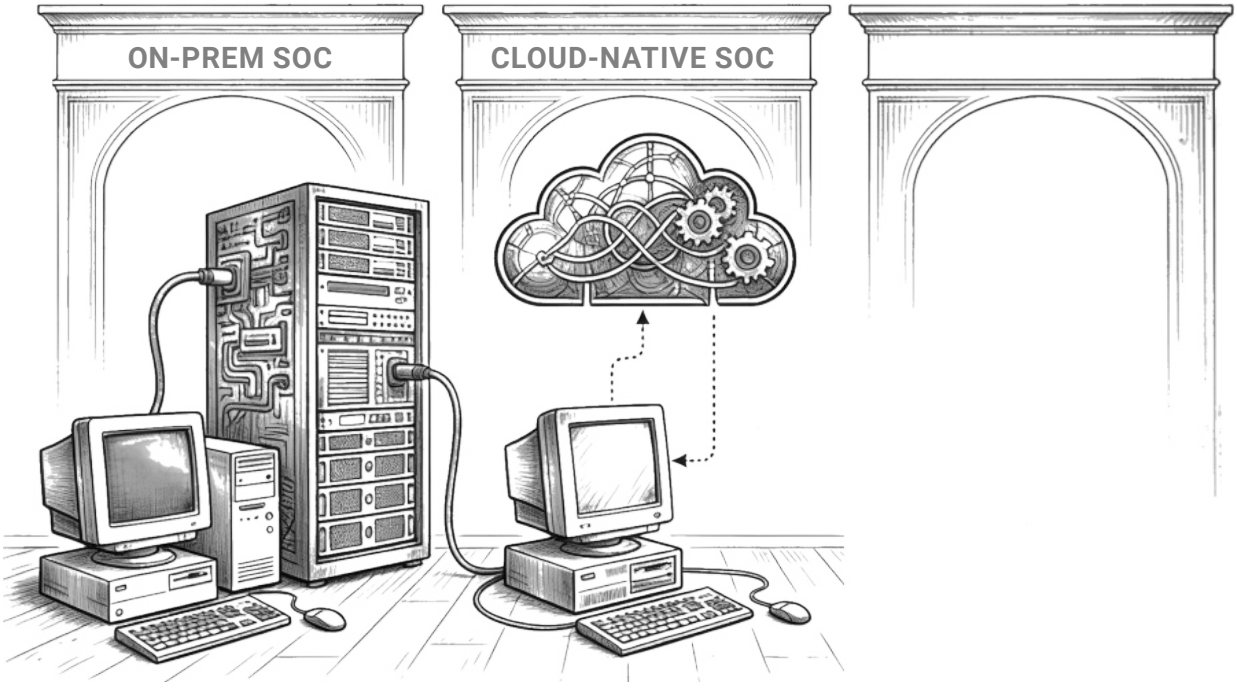
- Cloud-basierte SIEM- und XDR-Plattformen
- Elastische Skalierung von Speicher und Rechenleistung
- Integration heterogener Datenquellen (SaaS, IaaS, APIs)
- Opex-basierte Kostenmodelle

Technische Infrastruktur

Die Architektur verschiebt sich von physischer Infrastruktur hin zu servicebasierten Komponenten:

- Cloud-native Data Lakes für Logdaten
- Managed SIEM/XDR-Plattformen
- API-basierte Datenintegration
- Serverlose oder containerisierte Analysepipelines
- Globale Verteilung über mehrere Regionen

Datenflüsse sind nicht mehr strikt linear, sondern hochgradig verteilt. Events werden in Echtzeit ingestiert, normalisiert und korreliert, oft über mehrere Plattformen hinweg. Diese Entkopplung von physischer Infrastruktur ermöglicht Skalierung, erhöht jedoch gleichzeitig die Abhängigkeit von Plattformarchitekturen.



Stärken

Die Flexibilität ist der zentrale Vorteil. Neue Datenquellen lassen sich schneller integrieren, Analysekapazitäten bedarfsgerecht erweitern. Cloud-native SOCs haben sich deshalb in vielen Organisationen als De-facto-Standard etabliert. Sie ermöglichen eine Verarbeitung von Datenmengen, die On-Prem wirtschaftlich kaum darstellbar wäre.

Zudem erlauben moderne Plattformen eine deutlich tiefere Korrelation über System- und Organisationsgrenzen hinweg. Sicherheitsereignisse aus SaaS-Anwendungen, Cloud-Infrastrukturen und klassischen IT-Systemen lassen sich erstmals konsistent zusammenführen. Laut Bitkom sehen über 70 % der Unternehmen in der Cloud eine Voraussetzung für moderne Sicherheitsanalysen.[2]

Nicht zuletzt profitieren Organisationen von der Innovationsgeschwindigkeit der Anbieter. Neue Analyseverfahren, Detection-Logiken oder Integrationen stehen oft ohne eigene Implementierung zur Verfügung.

Schwächen

Die Verlagerung in die Cloud führt zu neuen Abhängigkeiten. Sicherheitsprozesse sind zunehmend an einzelne Plattformanbieter gebunden. Dies betrifft nicht nur Technologie, sondern auch Datenformate und Analysemodelle.

Ein weiteres Problem ist die Kostenstruktur. Während Cloud-Lösungen initial kosteneffizient erscheinen, können insbesondere ingest-basierte Preismodelle bei hohem Datenvolumen schnell eskalieren. Darüber hinaus entsteht eine neue Form von Intransparenz. Die tatsächliche Verarbeitung der Daten ist oft nicht vollständig nachvollziehbar, ein kritischer Punkt für forensische Analysen.

Kritische Einordnung

Das Cloud-native SOC löst viele Skalierungsprobleme des On-Prem-Modells. Gleichzeitig verschiebt es die Kontrolle von der Organisation hin zum Anbieter. Die Frage ist nicht mehr, ob Systeme skalieren, sondern wer die Kontrolle über diese Skalierung besitzt.

AI-native SOC: Automatisierung oder Abstraktion?

Mit dem Aufkommen leistungsfähiger KI-Modelle wird zunehmend von einer neuen Evolutionsstufe gesprochen: dem AI-native SOC. Gemeint ist ein Sicherheitsbetrieb, der maßgeblich durch maschinelles Lernen, Automatisierung und zunehmend autonome Systeme geprägt ist.

Der Begriff klingt nach einem klaren Zielbild. In der Praxis ist dieses Bild jedoch noch unscharf, und genau darin liegt seine Spannung.

Charakteristika

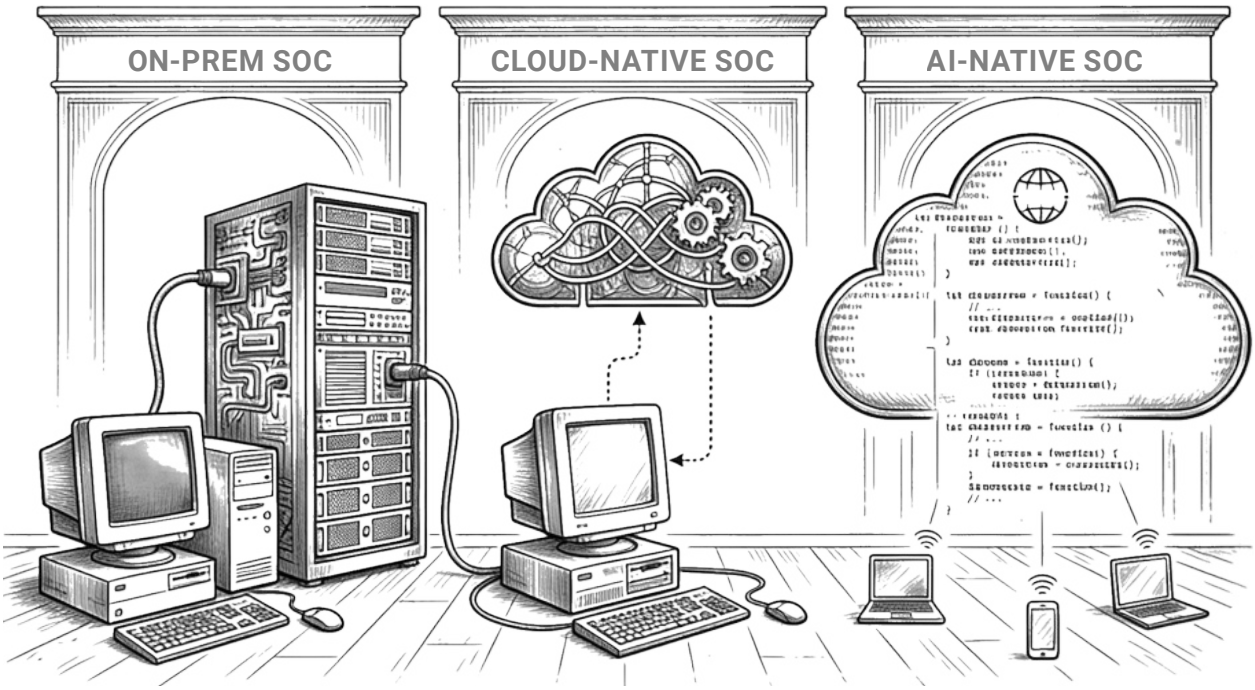
- Einsatz von Machine Learning zur Anomalieerkennung
- Automatisierte Incident Response (SOAR)
- AI-gestützte Analyse von Alerts und Kontextdaten
- Erste Ansätze von AI Agents in Security-Prozessen

Technische Infrastruktur

Im AI-nativen Kontext erweitert sich die Architektur um daten- und modellzentrierte Komponenten:

- Feature Stores & Trainingsdaten-Pipelines
- ML-Modelle für Detection & Priorisierung
- SOAR-Plattformen mit automatisierten Playbooks
- LLM-basierte Assistenzsysteme für Analysten
- Erste agentenbasierte Systeme zur teilautomatisierten Entscheidungsfindung

Die Datenverarbeitung erfolgt zunehmend in Feedback-Schleifen: Modelle generieren Hypothesen, bewerten Ereignisse und werden durch neue Daten kontinuierlich angepasst. Damit verschiebt sich der Fokus weg von Infrastruktur, hin zu Datenqualität, Modellgüte und Prozessintegration.



PODCAST

CYBER SECURITY Basement

In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.

Jetzt reinhören

Spotify

Apple Podcast

YouTube Music

amazon music

und noch mehr...

Aktueller Stand

In der Praxis beschränkt sich „AI-native“ derzeit weitgehend auf unterstützende Funktionen. Systeme priorisieren Alerts, schlagen Korrelationen vor oder automatisieren Standardprozesse. Vollständig autonome Sicherheitsentscheidungen sind selten und in vielen Organisationen bewusst nicht gewünscht.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, dass KI-Systeme in der Cyberabwehr derzeit primär als Assistenzsysteme eingesetzt werden.[3]

Chancen

Die größte Chance liegt in der Reduktion operativer Last. Analysten werden von repetitiven Aufgaben entlastet und können sich auf komplexe Fälle konzentrieren. Zudem eröffnen KI-Modelle neue Möglichkeiten in der Erkennung bislang unbekannter Angriffsmuster, insbesondere durch Verhaltensanalysen.

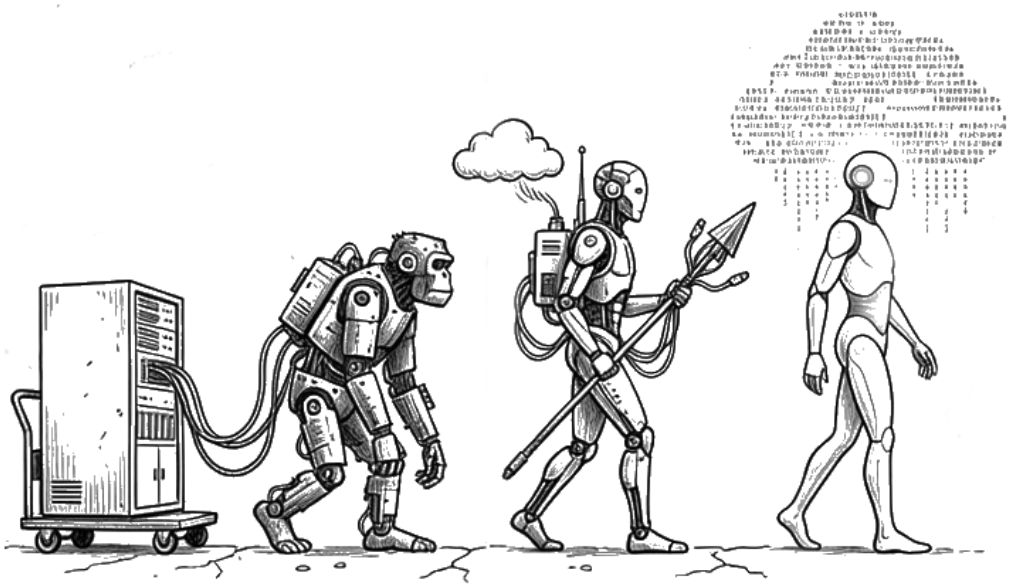
Risiken

Gleichzeitig entstehen neue Unsicherheiten. KI-Modelle sind nicht deterministisch. Entscheidungen sind oft schwer nachvollziehbar. Hinzu kommt das Risiko von Fehlklassifikationen sowie die Abhängigkeit von Trainingsdaten.

Autonome Prozesse & AI Agents

Ein besonders diskutierter Aspekt ist der Einsatz von AI Agents. Derzeit bewegen sich diese Ansätze überwiegend im experimentellen Bereich. In produktiven SOC-Umgebungen werden sie meist als unterstützende Komponenten eingesetzt: etwa zur Vorbereitung von Entscheidungen oder zur Teilautomatisierung von Playbooks.

Die Vision eines vollständig autonomen SOC bleibt damit offen. Ob sie technisch erreichbar, organisatorisch gewünscht oder regulatorisch zulässig ist, steht derzeit noch nicht fest.



Kritische Einordnung

„AI-native“ ist weniger ein abgeschlossener Zustand als vielmehr ein Suchprozess. Viele grundlegende Herausforderungen bleiben bestehen: Datenqualität, Integrationskomplexität und Abhängigkeiten verschwinden nicht, sie verschieben sich lediglich.

Gleichzeitig eröffnet sich ein neues Spannungsfeld: zwischen Effizienzgewinnen durch Automatisierung und dem Bedarf nach Kontrolle und Nachvollziehbarkeit. Wie sich dieses Spannungsfeld auflöst, ist offen. Denkbar sind hochautomatisierte SOCs mit minimaler menschlicher Intervention, ebenso wie bewusst hybride Modelle, in denen KI gezielt unterstützt, aber nicht entscheidet.

Gerade diese Offenheit macht den aktuellen Diskurs aus und unterscheidet ihn fundamental von den vorherigen Evolutionsstufen. Der Begriff „AI-native“ suggeriert einen fundamentalen Wandel. Tatsächlich handelt es sich derzeit eher um eine zusätzliche Schicht innerhalb bestehender Architekturen.

Viele der zugrunde liegenden Probleme bleiben bestehen:

- Datenqualität
- Integrationskomplexität
- Abhängigkeit von Plattformen

KI verschiebt diese Probleme nicht zwingend, sie maskiert sie teilweise. Gleichzeitig ist nicht auszuschließen, dass sich mit zunehmender Reife ein echter Paradigmenwechsel ergibt. Ob dieser jedoch in Richtung vollständiger Autonomie oder hybrider Modelle führt, ist derzeit offen.

SOC-Evolution im Überblick

- On-Prem: maximale Kontrolle, geringe Skalierbarkeit
- Cloud-native: hohe Skalierung, reduzierte Kontrolle
- AI-native: steigende Automatisierung, unklare Entscheidungslogik

Fazit:

Die Evolution der SOC-Architekturen ist keine lineare Erfolgsgeschichte. Jede Phase löst spezifische Probleme und erzeugt gleichzeitig neue. On-Prem bietet Kontrolle, skaliert jedoch schlecht. Cloud-native skaliert, reduziert jedoch die Kontrolle. AI-native verspricht Entlastung, bringt jedoch neue Unsicherheiten in Entscheidungsprozesse.

Die zentrale Herausforderung besteht darin, diese Spannungsfelder bewusst zu managen, statt sich von technologischen Narrativen leiten zu lassen.

CISO-Takeaways

- Architekturentscheidungen sind immer auch Entscheidungen über Kontrolle
- Skalierbarkeit darf nicht isoliert bewertet werden
- KI ersetzt keine sauberen Daten- und Prozessstrukturen
- Vendor-Abhängigkeiten nehmen mit jeder Evolutionsstufe zu
- Der organisatorische Reifegrad bestimmt den Nutzen von KI maßgeblich

Schlusswort:

Die Diskussion um AI-native SOCs steht erst am Anfang. Vieles, was heute als Innovation gilt, ist in der Praxis noch experimentell. Es ist daher zu früh, von einem klar definierten Zielbild zu sprechen. Wahrscheinlicher ist eine Phase hybrider Modelle, in denen menschliche Expertise und algorithmische Unterstützung eng verzahnt sind.

Ob sich daraus ein vollständig autonomes SOC entwickelt oder ob der Mensch dauerhaft im Zentrum bleibt, ist keine rein technologische Frage, sondern eine Frage von Vertrauen, Verantwortung und Risikobereitschaft.

Weitere Informationen zum Thema:

Podcast-Folge:

In dieser Folge geht es um die Zukunft von Threat Intelligence, den realen Mehrwert von KI im SOC und die Grenzen autonomer Security.

Quellen

[1] IBM Security: Cost of a Data Breach Report
[2] Bitkom: Cloud Report
[3] BSI: Künstliche Intelligenz in der Cyber-Sicherheit

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de