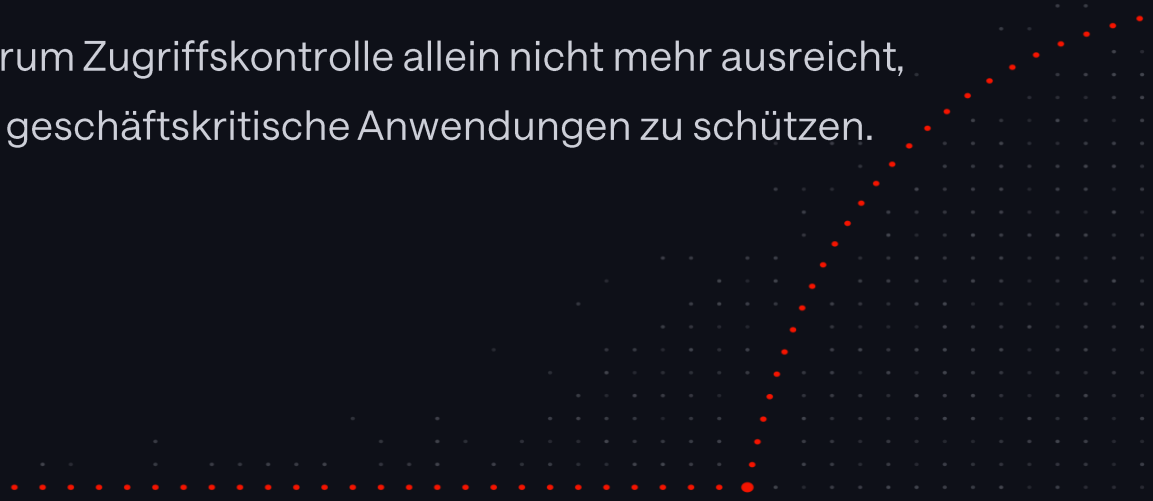
WHITE PAPER

Der Detection Gap

Warum Zugriffskontrolle allein nicht mehr ausreicht, um geschäftskritische Anwendungen zu schützen.



exeon

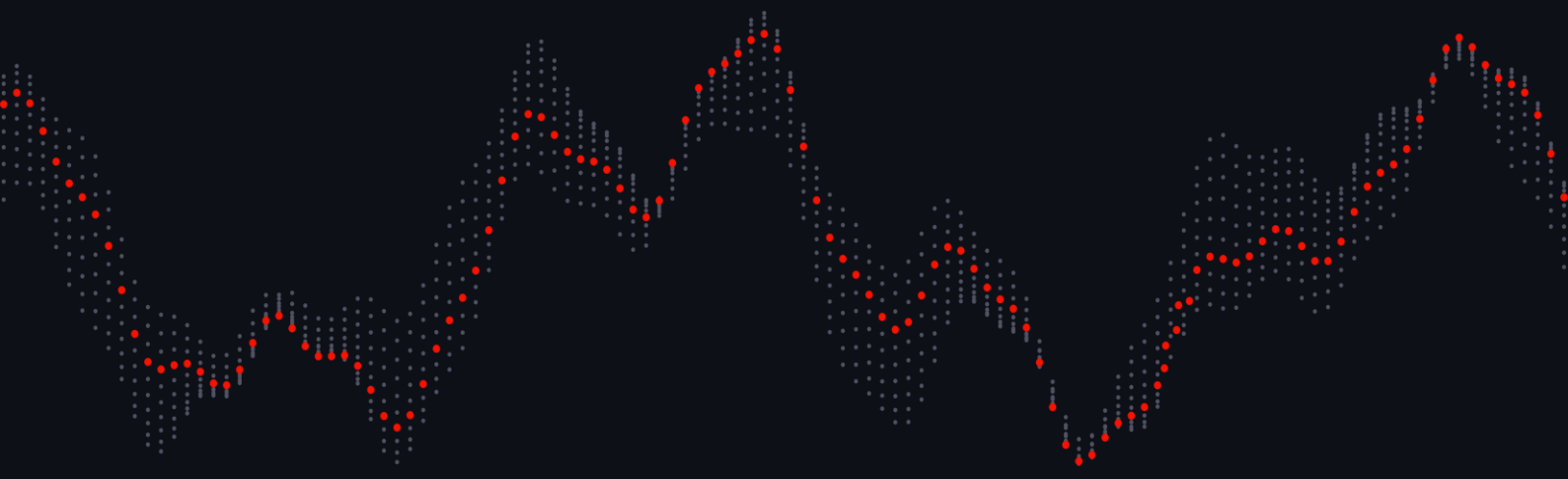
exeon.com

Inhaltsverzeichnis

01

ABSCHNITT 01

Executive Summary



Seit mehr als zwei Jahrzehnten investieren Organisationen erheblich in die Absicherung des Zugriffs auf ihre kritischsten Systeme.

Identity and Access Management (IAM), Segregation of Duties (SoD), Governance Risk & Compliance (GRC), Privileged Access Management (PAM), Multi-Faktor-Authentifizierung, Audit-Kontrollen und regulatorische Frameworks haben die Art und Weise, wie Zugriff geregelt wird, erheblich verbessert.

Diese Investitionen waren notwendig.
Sie bleiben notwendig.

Cybervorfälle und lange Dwell Times zeigen weiterhin, wie schwierig es ist, Aktivitäten nach der Zugriffsgewährung zu verstehen. Viele Organisationen können eine grundlegende operative Frage nicht beantworten:

> **Was tun unsere Benutzer, Administratoren, Partner und Dienstkonten gerade jetzt innerhalb unserer geschäftskritischen Systeme?**

Diese Frage steht im Zentrum dessen, was viele Sicherheitsverantwortliche zunehmend als wachsende Erkennungslücke erkennen.

Die Herausforderung ist besonders sichtbar in Systemen, die im operativen Herzen der Organisation angesiedelt sind:

- SAP-Landschaften
- Kernbanken- und Vermögensverwaltungsplattformen wie Avaloq
- Klinische Informationssysteme wie Epic
- Oracle-basierte Geschäftsplattformen
- Abacus-ERP-Umgebungen
- Manufacturing-Execution-Systeme (MES)
- Steuerungsplattformen für Energie und Versorgung
- Branchenspezifische operative Systeme

Diese “Kronjuwel”-Systeme unterscheiden sich nach Branche, Architektur und Anbieter.

Sie haben eine Gemeinsamkeit:

Sie enthalten die kritischsten Geschäftsprozesse, Daten und Entscheidungen einer Organisation.

Die traditionelle Frage lautete: Wer sollte Zugriff haben?

Die aufkommende Frage lautet: Wie schnell können wir erkennen, wenn legitimer Zugriff auf illegitime Weise genutzt wird?

Fünf Erkenntnisse, die den Detection Gap prägen

01 **Die Identität ist zur primären Angriffsfläche geworden**

Moderne Angreifer verschaffen sich Zugriff zunehmend über gültige Anmeldedaten statt über technische Exploits.

02 **Kritische Anwendungen verstärken die geschäftlichen Auswirkungen**

Die Kompromittierung operativer Plattformen wirkt sich direkt auf Umsatz, Betrieb, Kunden, Patienten, Bürger und Lieferketten aus.

03 **Traditionelle Kontrollen bleiben notwendig, sind aber unzureichend**

Access Governance erklärt Berechtigungen, jedoch nicht zwingend das tatsächliche Verhalten.

04 **Die Sicherheitssichtbarkeit bleibt fragmentiert**

Applikations-, IAM-, Compliance- und SOC-Teams beobachten oft unterschiedliche Teile derselben Geschichte.

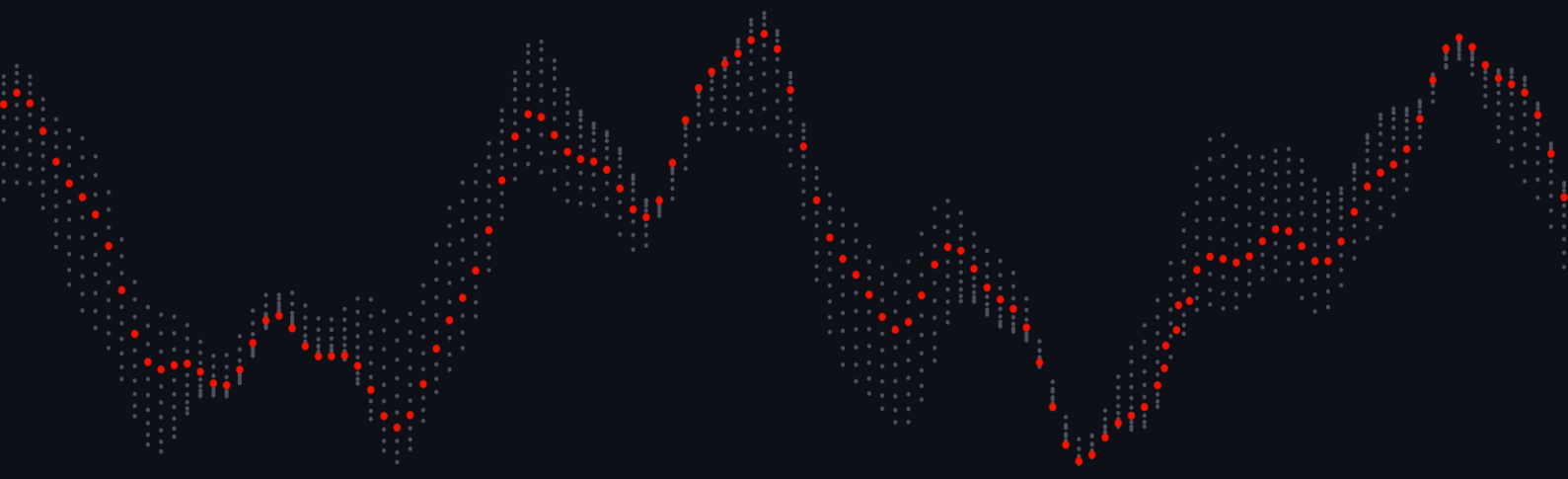
05 **Detection wird zur Resilienzanforderung**

Regulatoren erwarten von Organisationen zunehmend, dass sie Vorfälle nicht nur verhindern, sondern sie auch rasch erkennen.

02

ABSCHNITT 02

Das Bedrohungs-modell hat sich verändert



Sicherheitsstrategien konzentrierten sich lange darauf, unbefugte User ausserhalb des Perimeters zu halten. Moderne Angriffe umgehen dieses Modell zunehmend, weil gültige Anmeldedaten Angreifern bereits den benötigten Zugriff verschaffen können.

- Phishing
- Social Engineering
- Identitätsdiebstahl
- Kompromittierung von Drittparteien
- Session Hijacking
- Insider-Missbrauch
- Fehlkonfigurierte Integrationen

Moderne Angreifer brechen nicht ein. Sie loggen sich ein.

Einmal authentifiziert, sind sie oft nicht von legitimen Benutzern zu unterscheiden.

- Die Anmeldedaten sind gültig.
- Die Berechtigungen sind gültig.
- Die Transaktionen sind gültig.

Die Herausforderung besteht nicht mehr nur darin, sicheren Zugriff zu gewähren. Entscheidend ist, das Verhalten nach der Zugriffsgewährung zu verstehen.

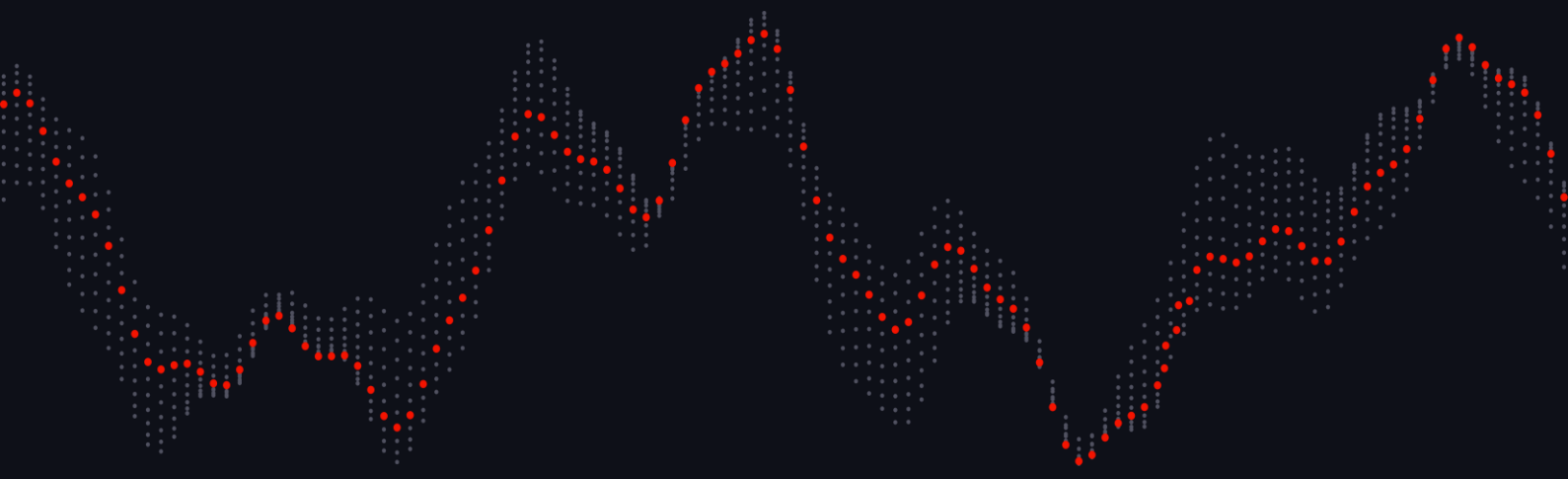
Angreifer agieren zunehmend als legitime Benutzer.

Bei den schädlichsten Cybervorfällen werden zunehmend legitime Identitäten für unrechtmässige Handlungen missbraucht.

03

ABSCHNITT 03

Die drei Typen von Insidern verstehen



Insider-Risiken beschränken sich nicht mehr auf böswillige Mitarbeitende. Viele identitätsbasierte Vorfälle betreffen Personen, die bereits legitimen Zugriff auf Systeme, Anwendungen und Geschäftsprozesse haben. Entscheidend sind ihre Absicht, ihr Verhalten und ihre jeweiligen Umstände. Dabei treten drei Kategorien besonders häufig auf.

Der böswillige Insider

Der böswillige Insider missbraucht seinen Zugriff absichtlich zum persönlichen, finanziellen, ideologischen oder wettbewerblichen Vorteil.

- Diebstahl sensibler Informationen
- Betrügerische Finanztransaktionen
- Sabotage von Systemen oder Prozessen
- Vorsätzliche Offenlegung vertraulicher Informationen

Obwohl solche Vorfälle oft erhebliche Aufmerksamkeit erregen, stellen sie nur eine Dimension des Insider-Risikos dar.

Der böswillige Insider kennt die Umgebung, weiss, wo kritische Informationen liegen, und versteht häufig, wie sich traditionelle Kontrollen umgehen lassen.

Der fahrlässige Insider

Der fahrlässige Insider hat keine böswillige Absicht. Das Risiko entsteht durch Fehler, Nachlässigkeit oder unsichere Praktiken.

Beispiele hierfür sind:

- Opfer von Phishing-Angriffen werden
- Weitergabe von Anmeldedaten
- Fehlkonfiguration von Systemen
- Versand sensibler Informationen an unbeabsichtigte Empfänger
- Umgehung von Kontrollen aus Bequemlichkeit, etwa das Vergessen, den Bildschirm zu sperren
- Nutzung nicht autorisierter Anwendungen oder Cloud-Dienste

In vielen Organisationen stellt diese Kategorie die grösste Quelle von Sicherheitsvorfällen dar. Die Herausforderung ist nicht böswillige Absicht. Die Herausforderung besteht darin, zu erkennen, wann routinemässige, fahrlässige oder aus Bequemlichkeit getriebene Handlungen ein wesentliches Risiko schaffen.

Der kompromittierte Insider

Der kompromittierte Insider ist zu einer der wichtigsten Risikokategorien in der modernen Cybersicherheit geworden.

In diesem Szenario ist der Benutzer weder böswillig noch fahrlässig. Stattdessen erlangt ein externer Akteur die Kontrolle über dessen Identität - durch:

- Diebstahl von Anmeldedaten
- Malware
- Session Hijacking
- Social Engineering
- Kompromittierung von Drittparteien oder der Lieferkette

Der Angreifer agiert dann mit einer legitimen Identität.

Aus Sicht vieler Systeme erscheint die Aktivität gültig:

- Korrekter Benutzername
- Valide Authentifizierung
- Genehmigte Berechtigungen
- Autorisierte Transaktionen

Der einzige bedeutsame Unterschied ist das Verhalten selbst.

Abbildung 1. *Obwohl sich die Motive erheblich unterscheiden, treten alle drei Kategorien häufig als legitime Benutzer auf, die innerhalb genehmigter Systeme agieren.*

Die entscheidende Beobachtung

Ein böswilliger Insider, ein fahrlässiger Insider und ein kompromittierter Insider können alle:

- **Sich erfolgreich anmelden**
- **Auf genehmigte Systeme zugreifen**
- **Autorisierte Anwendungen nutzen**
- **Innerhalb zugewiesener Berechtigungen agieren**

Zugriffskontrollen erkennen sehr zuverlässig, ob ein Zugriff bestehen sollte.

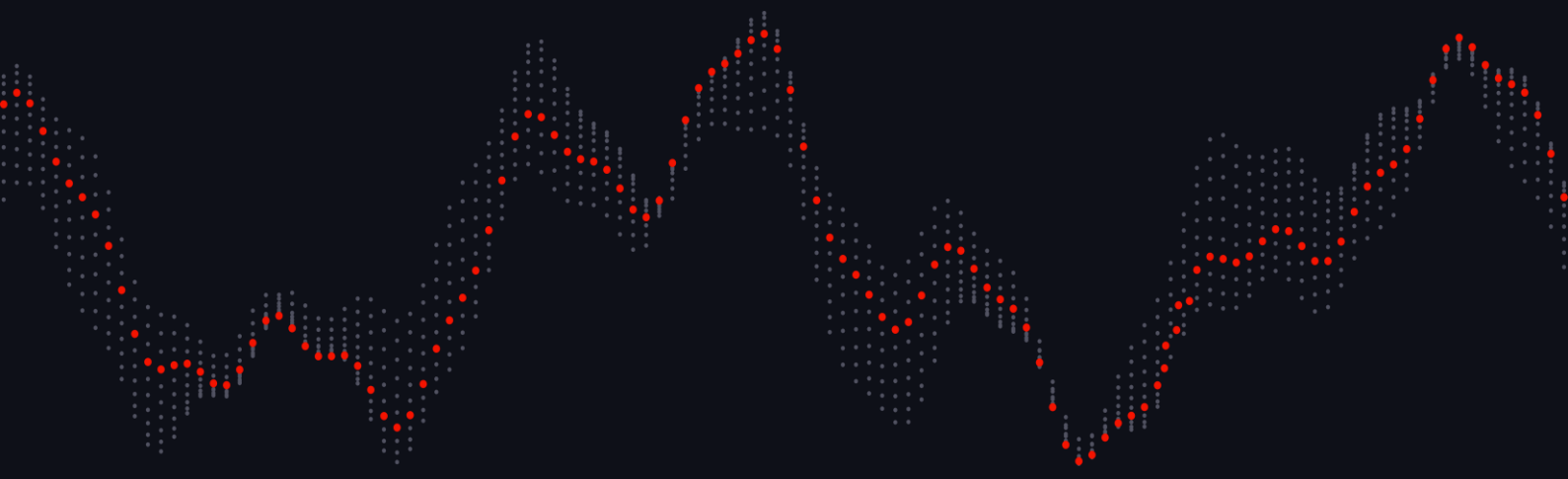
Sie zeigen jedoch nicht immer, ob das daraus resultierende Verhalten sinnvoll ist.

Hier verläuft die Grenze zwischen Access Governance und Threat Detection.

04

ABSCHNITT 04

Warum Krohnjuwel-Anwendungen wichtig sind



WIESO KRONJUWEL-ANWENDUNGEN WICHTIG SIND

Nicht alle Systeme sind gleich wichtig. Die meisten Organisationen verfügen über eine kleine Zahl von Systemen, deren Kompromittierung unmittelbare operative Konsequenzen hätte.

Die konkreten Anwendungen variieren je nach Branche.

BRANCE	KRONJUWEL-SYSTEME
Fertigung	SAP, MES, Supply-Chain-Plattformen
Finanzdienstleistungen	Kernbankensysteme, Avaloq, Zahlungsplattformen
Gesundheitswesen	EPIC, Klinische Informationssysteme
Handel	ERP, Logistikplattformen
Energie & Versorgung	OT-Plattformen, Asset-Management-Systeme
Öffentlicher Sektor	Bürgerdienst-Plattformen, Finanzsysteme

Die Kompromittierung dieser Systeme kann zu Folgendem führen:

- Finanzbetrug
- Betriebsunterbrechung
- Regulatorischen Verstössen
- Risiken für die Patientensicherheit
- Unterbrechungen der Lieferkette
- Datenexfiltration
- Verlust öffentlichen Vertrauens

Diese Systeme enthalten oft eine einzigartige Kombination aus:

- Sensiblen Informationen
- Umfangreichen Privilegien
- Autorität über einen Geschäftsprozess
- Systemübergreifenden Integrationen

Infolgedessen betrachten Angreifer sie zunehmend als hochwertige Ziele.

KERNAUSSAGE

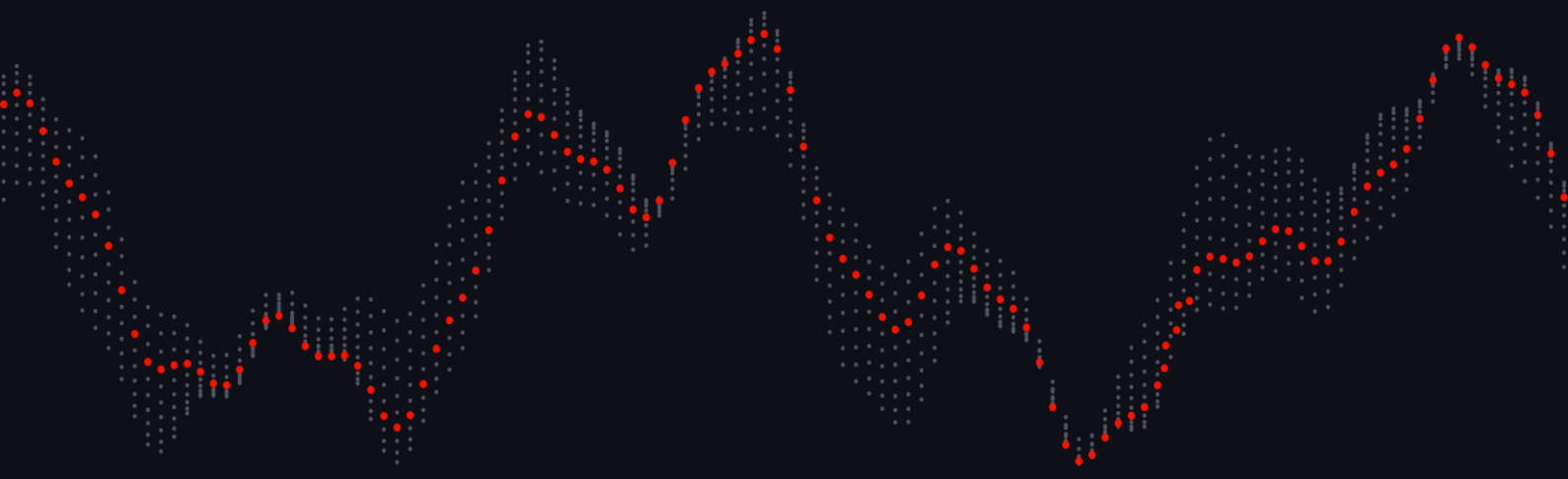
Das Ziel ist selten die Anwendung selbst.

Das Ziel ist der Geschäftsprozess, die Daten oder der operative Hebel, den die Anwendung kontrolliert.

05

ABSCHNITT 05

Wie Unternehmens-IT heute tatsächlich funktioniert



Die Realität moderner Unternehmensarchitekturen unterscheidet sich erheblich von den Umgebungen, für die viele Sicherheitsmodelle ursprünglich konzipiert wurden.

Organisationen operieren heute über:

- Legacy/On-Premises-Systeme
- Private Cloud-Umgebungen
- Public Cloud-Plattformen
- OT- und IoT-Umgebungen
- SaaS-Anwendungen
- Ökosysteme von Drittanbietern
- Remote-Belegschaften

> **Doch ein Faktor verbindet sie zunehmend alle: die Identität.**

Eine einzelne menschliche oder maschinelle Identität kann mit Dutzenden von Systemen über mehrere Umgebungen hinweg interagieren.

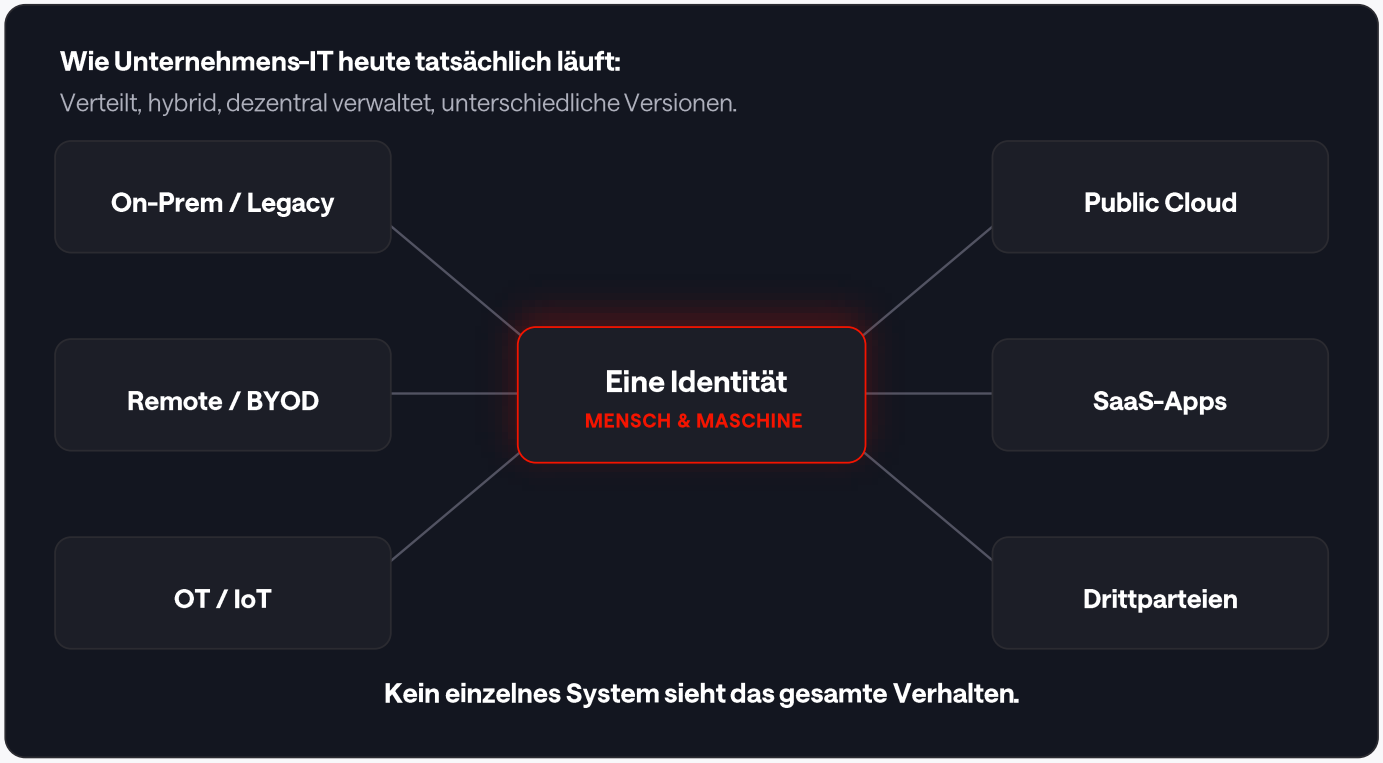


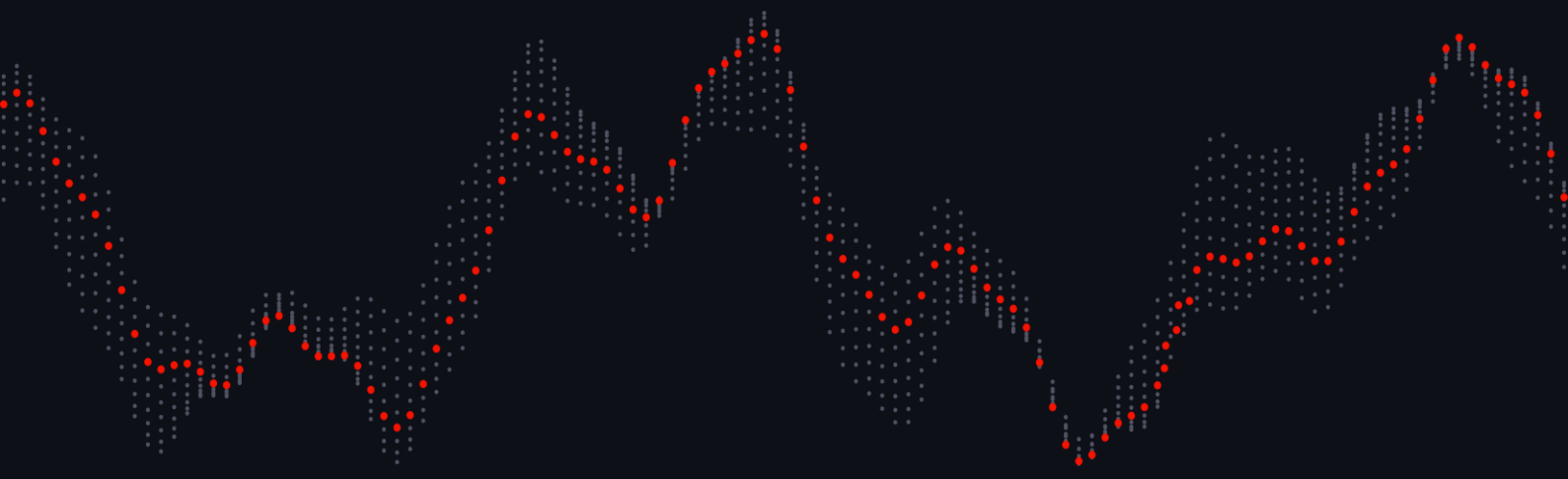
Abbildung 2. *Eine Identität erstreckt sich zunehmend über mehrere Technologiedomänen. Kein einzelnes System sieht das vollständige Verhaltensbild.*

Wenn sich Identitäten über Umgebungen hinweg bewegen, wird es zunehmend schwierig, Aktivitäten zu verstehen. Was in einem System normal erscheint, kann im Kontext des breiteren Geschäftsumfelds ganz anders aussehen.

06

ABSCHNITT 06

Die Reife moderner Zugriffskontrolle



Organisationen haben enorme Fortschritte bei der Steuerung des Zugriffs gemacht.

Branchenübergreifend umfassen Sicherheitsprogramme heute:

- Identity and Access Management (IAM)
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Segregation of Duties (SoD)
- Privileged Access Management (PAM)
- Multi-Faktor-Authentifizierung (MFA)

Zusammen beantworten diese Fähigkeiten eine entscheidende Frage: Wer darf welche Handlung ausführen?

Eine starke Governance bleibt die Grundlage der Security, legitime Berechtigungen garantieren jedoch kein legitimes Verhalten.

Ein Benutzer kann über legitime Berechtigungen verfügen und dennoch auf eine Weise handeln, die:

- Ungewöhnlich
- Riskant
- Verdächtig
- Böswillig

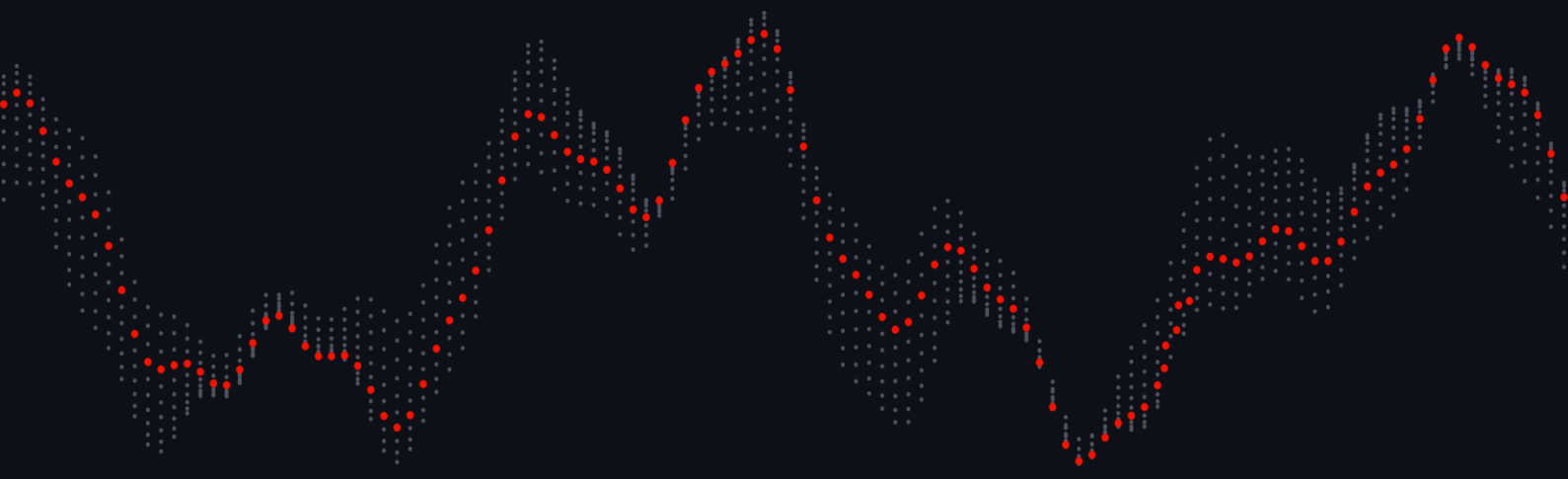
ist.

Diese Unterscheidung wird zunehmend wichtig.

07

ABSCHNITT 07

Der Detection Gap



Traditionelle Kontrollen operieren in der Regel in einem von zwei Zeitrahmen.

VOR DER AKTIVITÄT

Zugriffskontrollen bestimmen:

- Wer Zugriff haben sollte
- Welche Privilegien er erhält
- Welche Risiken zu mindern sind

NACH DER AKTIVITÄT

Audits bestimmen:

- Was geschehen ist
- Ob Richtlinien eingehalten wurden
- Ob Verstösse aufgetreten sind

Beide Kontrollen sind wichtig. Sie beschreiben jedoch den Zugriff vor einer Aktivität und liefern Nachweise danach. Keine von beiden zeigt zwingend, was während der Aktivität geschieht. Dadurch entsteht der Detection Gap.

Viele Organisationen sind sehr gut darin, Zugriff zu regeln und Aktivitäten zu dokumentieren.

Deutlich weniger können Verhalten verstehen, während die Aktivität stattfindet.

Die Erkennungslücke entsteht immer dann, wenn legitime Aktivität nicht von verdächtiger Aktivität unterschieden werden kann.

Beispiele hierfür sind:

- Ein Administrator, der Tools nutzt, die er zuvor nie verwendet hat
- Ein Finanzbenutzer, der ungewöhnlich grosse Datenmengen exportiert
- Ein Dienstkonto, das sich anders als üblich verhält
- Ein privilegierter Benutzer, der ausserhalb erwarteter Muster agiert
- Ein Drittparteien-Konto, das auf unbekannte Systeme zugreift
- Ein Klinik-Mitarbeiter, der Patientenakten abruft, die nichts mit seiner Rolle zu tun haben
- Ein Bank-Administrator, der ungewöhnliche Konfigurationsänderungen vornimmt

Einzeln betrachtet mag jede Handlung legitim erscheinen.
Das Risiko wird oft erst sichtbar, wenn man es als Verhalten über die Zeit betrachtet.

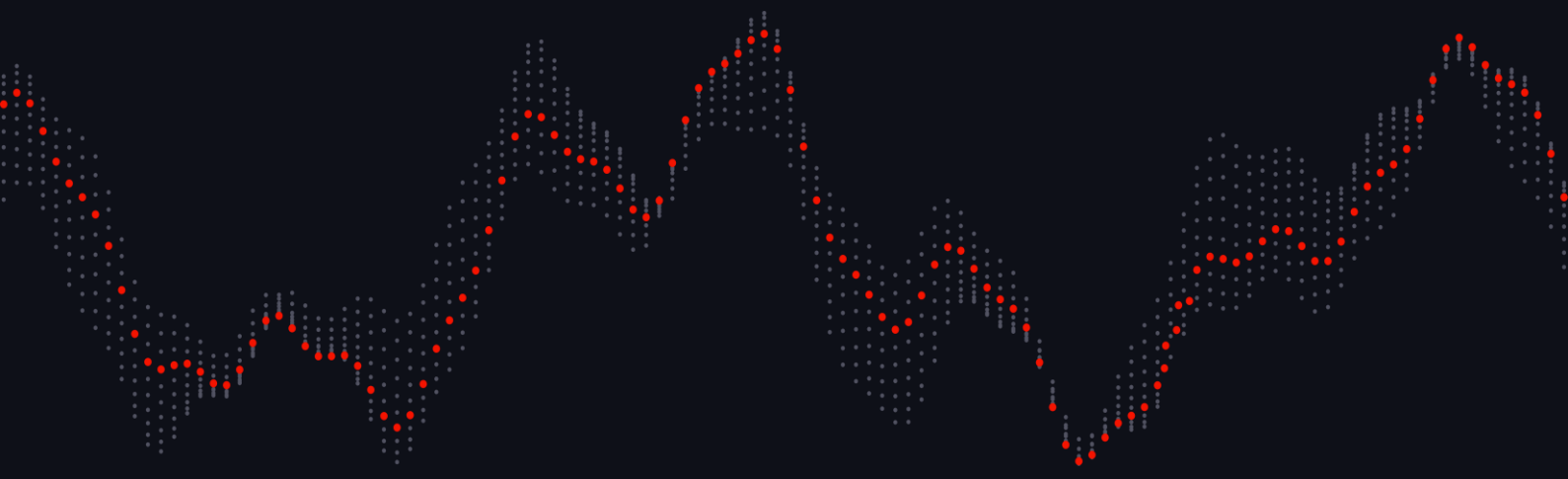
> **Hier stellen viele Organisationen fest, dass Sichtbarkeit - und nicht Zugriffskontrolle – zur nächsten grossen Herausforderung beim Schutz von Kronjuwel-Anwendungen geworden ist.**

Abbildung 3. *Organisationen haben erheblich in die Steuerung von Zugriff, das Management von Risiken und die Dokumentation von Aktivitäten investiert. Dennoch bleibt oft eine kritische Lücke zwischen dem, was Identitäten tun dürfen, und dem, was sie in der Praxis tun.*

08

ABSCHNITT 08

Warum ereignisbasiertes Monitoring zu kurz greift



Den meisten Organisationen fehlt es nicht an Sicherheitskontrollen.

Im Gegenteil: Viele haben über Jahre hinweg kräftig investiert in:

- Identity Governance
- Privileged Access Management
- Security Monitoring
- Audit-Programme
- Security Operations Center
- Compliance Frameworks

Und trotzdem kommt es immer wieder zu schwerwiegenden Sicherheitsvorfällen.

Das führt zu einer unbequemen Frage: Wie kann es sein, dass Organisationen über so viele Sicherheitsdaten verfügen und Missbrauch dennoch kaum erkennen?

Die Antwort liegt oft in einem grundlegenden Unterschied:

Aktivitäten zu erfassen ist nicht dasselbe, wie sie zu verstehen.

Viele Organisationen haben alles griffbereit:

- Authentifizierungslogs
- Audit-Aufzeichnungen
- Transaktionshistorien
- Infrastruktur-Telemetrie
- Anwendungslogs

Werden diese Datenquellen getrennt ausgewertet, entstehen **Aufzeichnungen ohne Kontext:** Organisationen wissen zwar, was passiert ist, können jedoch nur schwer beurteilen, ob es ungewöhnlich ist.

Der Unterschied zwischen Ereignissen und Verhalten

Klassisches Monitoring denkt in einzelnen Ereignissen. Es fragt:

- Hat sich jemand angemeldet?
- Wurden Privilegien (aus-)genutzt?
- Wurde eine Konfiguration verändert?
- Wurde auf eine Datei zugegriffen?

Diese Ereignisse sind wichtig.

Nur verraten sich Angreifer selten durch eine einzelne Aktion.

Das Risiko entsteht vielmehr aus einer Kette von Handlungen, die jede für sich völlig legitim wirken.

Ein Beispiel:

1. Ein Benutzer meldet sich an.
2. Er ruft eine administrative Funktion auf.
3. Er ändert eine Rolle.
4. Er greift auf sensible Daten zu.
5. Er exportiert Informationen.

Jeder einzelne Schritt kann isoliert betrachtet autorisiert sein, doch die Abfolge verändert die Bewertung.

Verhalten erhält seine Bedeutung durch den Kontext, einzelne Events liefern ihn nur selten.

KERNAUSSAGE

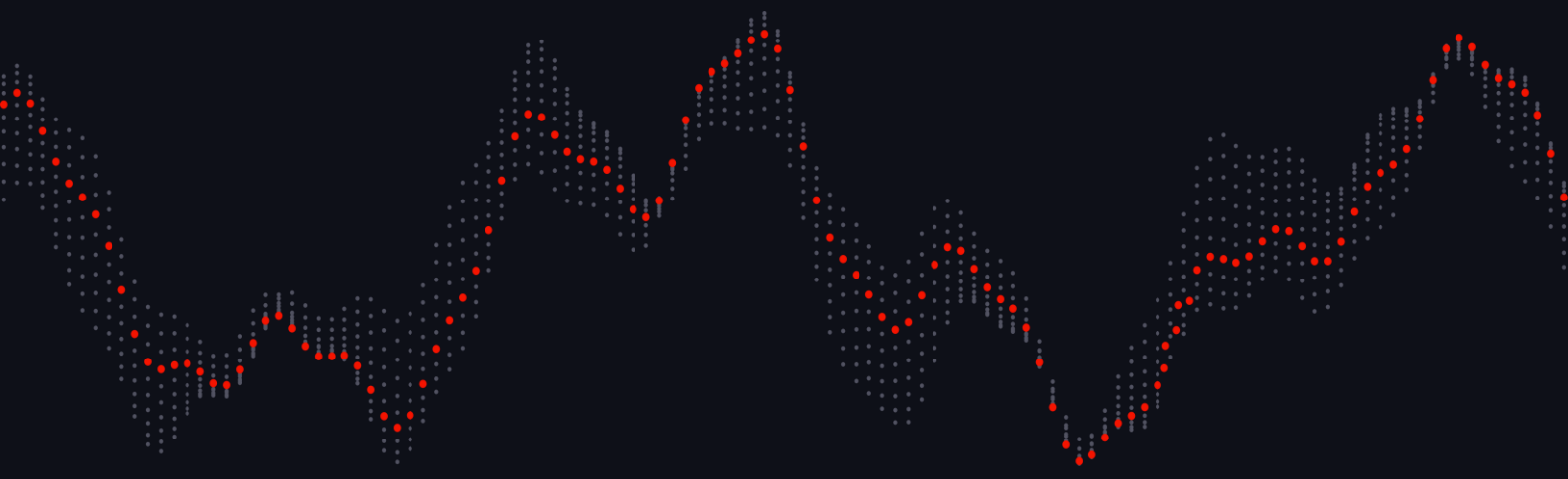
Die wenigsten Vorfälle fliegen auf, weil eine einzelne Aktion verdächtig aussieht.

Sie fliegen auf, weil die Abfolge der Aktionen eine ganz andere Geschichte erzählt.

09

ABSCHNITT 09

Das Sichtbarkeits-problem



Der blinde Fleck in der Organisation

Das Problem ist nicht allein technischer Natur – es ist zunehmend ein organisatorisches.

Über die Jahre haben sich die Sicherheitsaufgaben im Unternehmen stark spezialisiert, und jedes Team betrachtet das Risiko aus seiner eigenen Perspektive.

TEAM	SCHWERPUNKT
IAM	Identitätslebenszyklus und Access Governance
Application Security	Anwendungs-Kontrollen und -Konfiguration
Compliance & Audit	Nachweise und Einhaltung von Richtlinien
Infrastruktur	Verfügbarkeit und Betrieb
SOC	Security Monitoring und Incident Response

Jedes Team leistet wertvolle Arbeit, aber keines sieht das vollständige Bild.
Bei geschäftskritischen Anwendungen zeigt sich eine verdächtige Sequenz nur über Geschäftsprozesse, Berechtigungen, Bedrohungsindikatoren und Compliance-Kontrollen hinweg, wirkt jedoch aus der einzelnen operativen Perspektive harmlos.

Zum Beispiel:

- Das ERP-Team sieht Geschäftsprozesse.
- Das IAM-Team sieht Berechtigungen.
- Das SOC sieht Kompromittierungsindikatoren.
- Das Audit-Team sieht Compliance-Pflichten.

Ein typisches Muster

Die Anwendungsteams fragen:
Läuft die Applikation korrekt?

Die Sicherheitsteams fragen:
Werden wir gerade angegriffen?

Die Compliance-Teams fragen:
Funktioniert die Zugriffskontrolle?

Die Führungsebene fragt:
Sind wir widerstandsfähig?

Allesamt berechtigte Fragen. Nur erklärt keine davon für sich genommen das tatsächliche Verhalten.

Geteilte Verantwortung, wachsende Komplexität

Unternehmens-IT ist heute weit stärker verteilt als früher.

Was Organisationen einst selbst in der Hand hatten:

- Infrastruktur
- Anwendung
- Daten
- Betriebsprozesse

verteilt sich heute auf viele Schultern:

- Interne IT-Teams
- Managed Service Provider
- Softwareanbieter
- Hyperscaler, SaaS-Anbieter
- Drittpartner

Das Shared-Responsibility-Modell verbessert Skalierbarkeit und Flexibilität, verteilt den Security-Kontext jedoch auf mehrere Beteiligte. Wenn niemand den vollständigen Aktivitätsfluss sieht, wird es schwieriger, klare Verantwortlichkeiten aufrechtzuerhalten.

Kronjuwel-Anwendungen werden zu Ökosystemen

Kaum eine Organisation betreibt ihre kritischen Anwendungen heute noch als abgeschottete Insellösungen. Stattdessen sind sie Teil grösserer digitaler Ökosysteme: Vernetzte Umgebungen, in denen Infrastruktur, Anwendungen, Benutzer, Maschinenidentitäten, Daten und externe Partner über Organisationsgrenzen hinweg zusammenspielen.

Ein solches Umfeld umfasst typischerweise:

- ERP-Systeme
- Identity Provider
- Kollaborationsplattformen
- Cloud-Dienste
- Data Warehouses
- Externe Schnittstellen
- Managed Services
- Drittanbieter

Diese Ökosysteme schaffen komplexe Abhängigkeiten, die sich deutlich schwerer überwachen und absichern lassen als einzelne Systeme. Die eigentliche Herausforderung besteht immer mehr darin, nachzuvollziehen, wie sich geschäftskritische Prozesse quer über verschiedene Plattformen, Anbieter und Identitäten hinweg bewegen.

Warum reines Infrastruktur-Monitoring nicht mehr genügt

Viele Sicherheitsprogramme sind rund um die Infrastruktur herum entstanden:

Server | **Netzwerke** | **Endpunkte** | **Perimeter-Kontrollen**

Anwendungen galten lange als separate operative Domäne, doch moderne Angriffe überschreiten diese Grenze zunehmend. Angreifer können in einer legitimen Business-Anwendung erhebliche Risiken verursachen und dabei nur wenige Signale in der Infrastruktur hinterlassen.

Etwa durch:

- betrügerische Finanztransaktionen
- unbefugte Datenexporte
- Privilege Escalation
- Missbrauch administrativer Rechte
- Manipulation von Konfigurationen

Da diese Handlungen innerhalb legitimer Business-Anwendungen stattfinden, kann klassisches Security Monitoring die Session erkennen, ohne die geschäftliche Bedeutung der Aktivität zu verstehen.

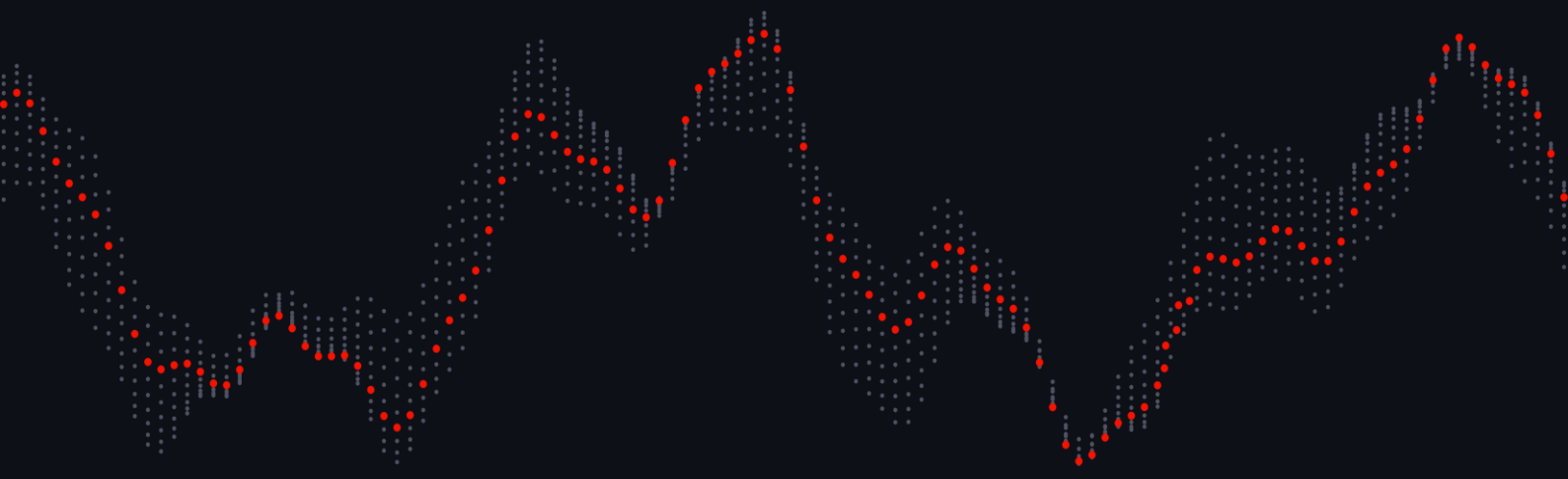
Infrastruktur-Sichtbarkeit zeigt, wo etwas passiert.

Verhaltens-Sichtbarkeit zeigt, warum es relevant ist und wann es auf Missbrauch hindeutet.

10

ABSCHNITT 10

Der Weg zu verhaltensbasierter Sicherheit



Immer mehr Organisationen erkennen: Access Governance allein kann nicht jede Sicherheitsfrage beantworten. Diese Entwicklung lässt sich am besten in drei aufeinander aufbauenden Ebenen verstehen.

EBENE 01

Zuweisung

Wer darf?

Diese Ebene legt fest:

- wer Zugriff erhält
- welche Berechtigungen vergeben werden
- welche Risiken abzusichern sind

Typische Bausteine sind:

- Identity and Access Management (IAM)
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Segregation of Duties (SoD)
- Access reviews

Die Zuweisung schafft das Fundament des Vertrauens.
Ohne sie ist ein sicherer Betrieb schlicht nicht möglich.

EBENE 02

Laufzeit

Wer ist es?

Diese Ebene legt fest:

- Authentifizierung
- Verlässlichkeit der Session
- Identitätssicherheit
- Vertrauenswürdigkeit des Geräts
- Zugriffskontext

Typische Bausteine sind:

- Multi-Faktor-Authentifizierung (MFA)
- Conditional Access
- Identitätsverifizierung
- Session-Management

Die Laufzeit-Ebene stellt sicher, dass der Benutzer tatsächlich der ist, für den er sich ausgibt.

EBENE 03

Verhalten

Was tun sie?

Diese Ebene richtet den Blick auf die Aktivität und fragt:

- Ist das normal?
- Ist das zu erwarten?
- Passt es zum bisherigen Verhalten?
- Ergibt diese Abfolge Sinn?

Anders als Zuweisung und Authentifizierung verändert sich Verhalten ständig.
Damit wird auch das Risiko kontextabhängig statt statisch..

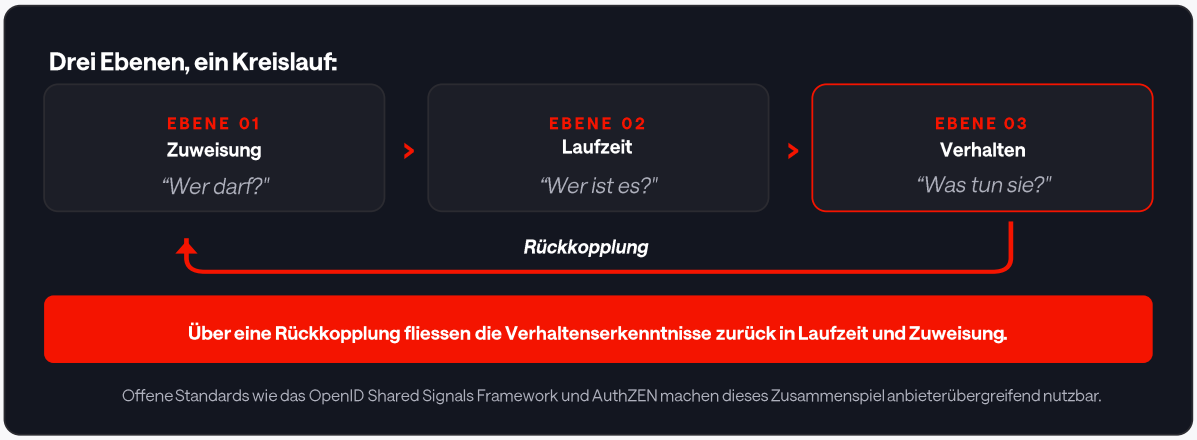
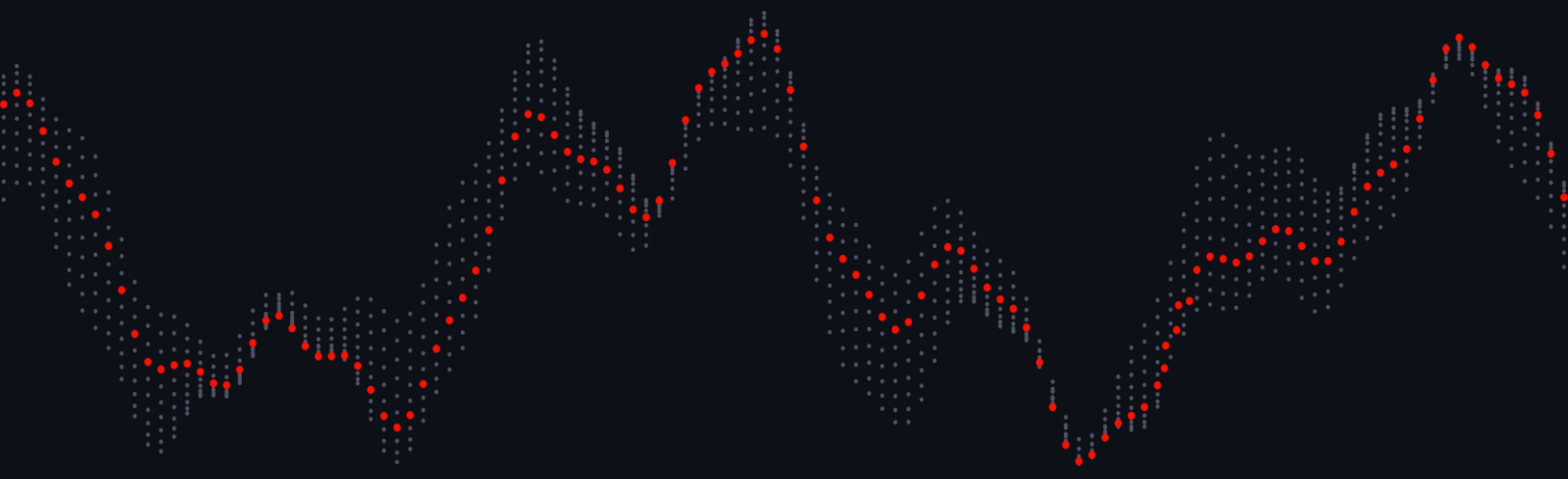


Abbildung 4. *Moderne Sicherheit lebt zunehmend vom fortlaufenden Zusammenspiel aus Governance, Authentifizierung und Verhalten – nicht von isolierten Einzelkontrollen.*

11

ABSCHNITT 11

Warum Verhalten wichtig ist



Verhalten liefert etwas, das klassische Kontrollen kaum bieten können: **Kontext**.

Nehmen wir zwei Benutzer, die exakt dieselbe Aktion ausführen.

BENUTZER A

tut dies jeden Tag.

BENITZER B

tut dies zum allerersten Mal.

Technisch gesehen: Die Aktion ist identisch.

Vom Verhalten her: **Das Risiko kann völlig unterschiedlich sein.**

Gerade dort, wo Angreifer mit legitimen Anmeldedaten arbeiten, wird dieser Unterschied entscheidend.

Verhalten als Frühwarnsignal

Veränderungen im Verhalten können sichtbar werden, bevor ein Schaden entsteht.
Solche Signale beweisen keine böswillige Absicht, können aber zeigen, dass eine Aktivität genauer untersucht werden sollte.

Etwa durch:

- ungewöhnliche administrative Aktivitäten
- veränderte Arbeitsmuster
- unerwartete Systemnutzung
- plötzliche Änderungen an Privilegien
- den erstmaligen Zugriff auf sensible Daten
- ungewöhnliche Transaktionsabfolgen

KERNAUSSAGE

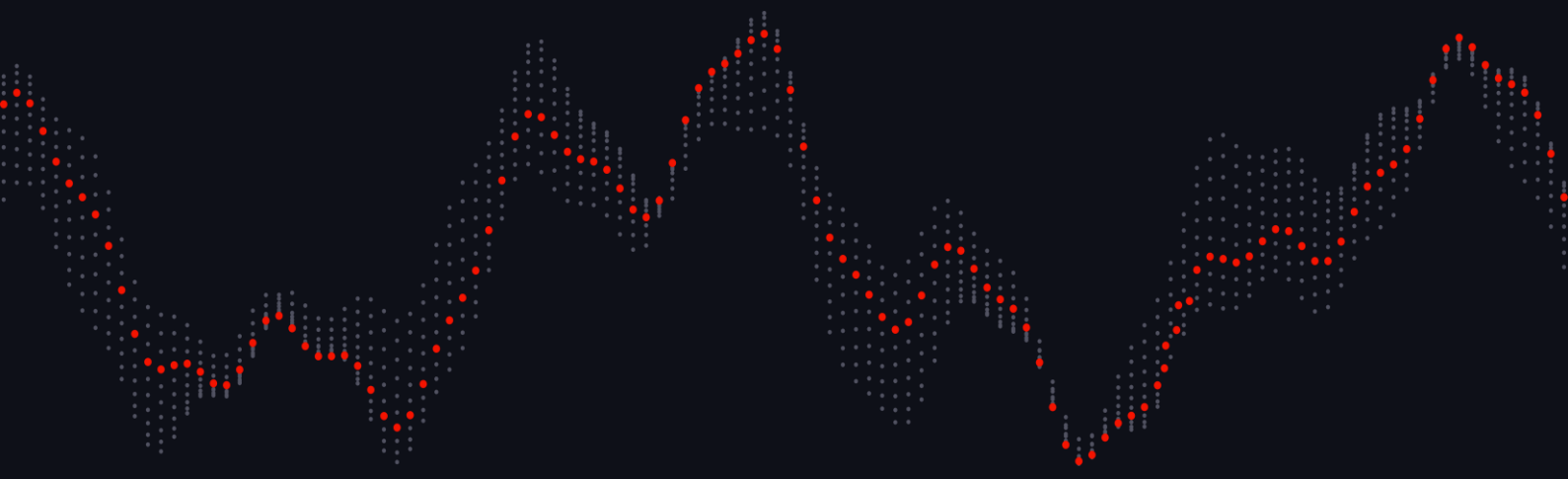
Verhaltenssignale sind selten ein Beweis – sie sind meist ein früher Hinweis.

Es geht nicht um Gewissheit, sondern darum, früher hinzusehen.

12

ABSCHNITT 12

Der regulatorische Wandel



exeon

Compliance-Programme konzentrierten sich traditionell darauf, das Vorhandensein von Kontrollen nachzuweisen. Resilienz-Frameworks fragen zunehmend, ob Organisationen einen Vorfall schnell erkennen, darauf reagieren und ihn melden können, wenn die Prävention versagt.

Das ist ein bemerkenswerter Perspektivwechsel.

Von Organisationen wird nicht mehr nur erwartet, Vorfälle zu verhindern – sondern sie schnell zu erkennen, darauf zu reagieren und sie zu melden, wenn die Prävention versagt.

NIS2

NIS2 legt den Schwerpunkt auf:

- Risikomanagement
- operative Resilienz
- Meldepflichten bei Vorfällen
- die Verantwortung der Unternehmensleitung

Die dahinterliegende Erwartung ist eindeutig: Organisationen müssen wissen, was in ihren kritischen Systemen vor sich geht.

DORA

DORA formuliert ähnliche Anforderungen für den Finanzsektor. Der Blick geht über die reine Prävention hinaus – hin zu:

- operativer Resilienz
- kontinuierlichem Monitoring
- Incident Management

Die zentrale Frage lautet zunehmend: Wie schnell erkennt eine Organisation abnormale Aktivitäten?

Wie sich das Audit-Gespräch verändert

Traditionell drehten sich Audits stark um Zugriffsrechte.

Gefragt wurde:

- Sind die Rollen sauber definiert?
- Werden die Berechtigungen regelmässig geprüft?
- Sind Berechtigungs-Konflikte entschärft?

Diese Fragen bleiben wichtig. Resilienzprüfungen und Audits gehen jedoch zunehmend über Access Governance hinaus und berücksichtigen auch operative Fragen wie:

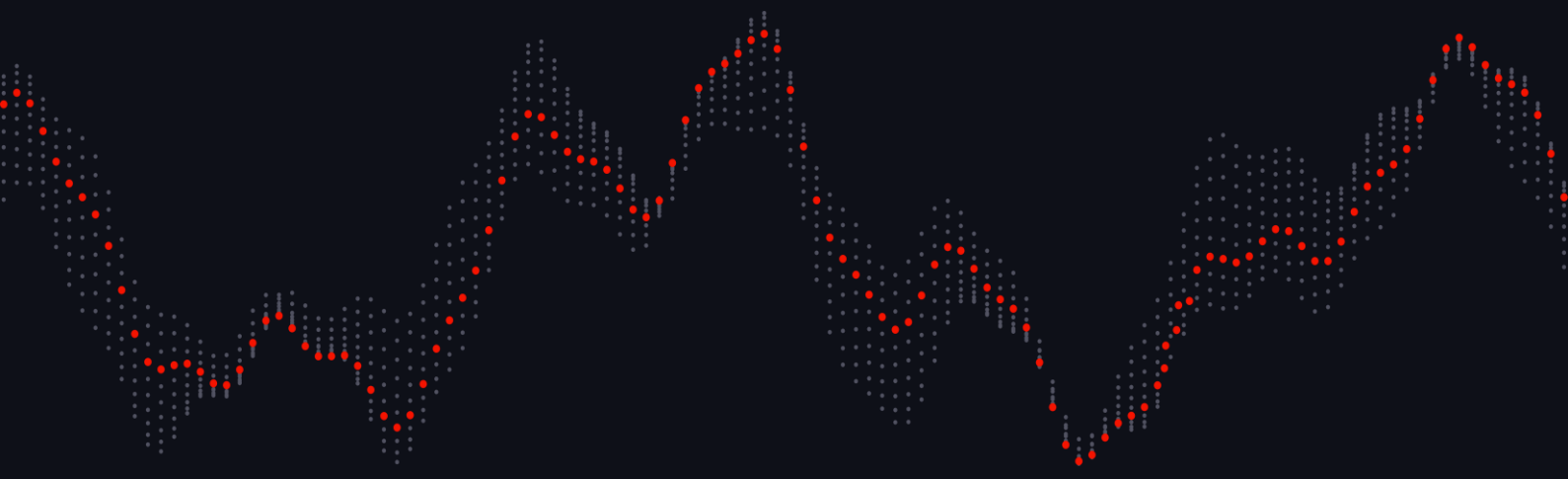
- **Wie schnell lässt sich Missbrauch erkennen?**
- **Wie werden auffällige Verhaltensweisen identifiziert?**
- **Wie wird die operative Sichtbarkeit aufrechterhalten?**
- **Wie werden identitätsbezogene Risiken überwacht?**

Das Audit von morgen fragt womöglich weniger, ob eine Kontrolle existiert – und mehr, wie schnell eine Organisation merkt, wenn diese Kontrolle versagt.

13

ABSCHNITT 13

Kronjuwelen in Zukunft schützen



Die meisten Organisationen verfügen bereits über umfassende Governance-Strukturen.
Der nächste Schritt besteht deshalb kaum in noch mehr Rollen, Richtlinien oder Audit-Nachweisen.
Die schwierigere Aufgabe ist es, sichtbar zu machen, wie Zugriffe tatsächlich genutzt werden.

Je weiter sich Unternehmensumgebungen über Cloud, SaaS, Drittanbieter, Operational Technology und branchenspezifische Plattformen ausdehnen, desto mehr wird Verhalten zur gemeinsamen Sprache, die all diese Welten miteinander verbindet.

Die Frage lautet nicht länger nur:
Ist diese Aktion autorisiert?

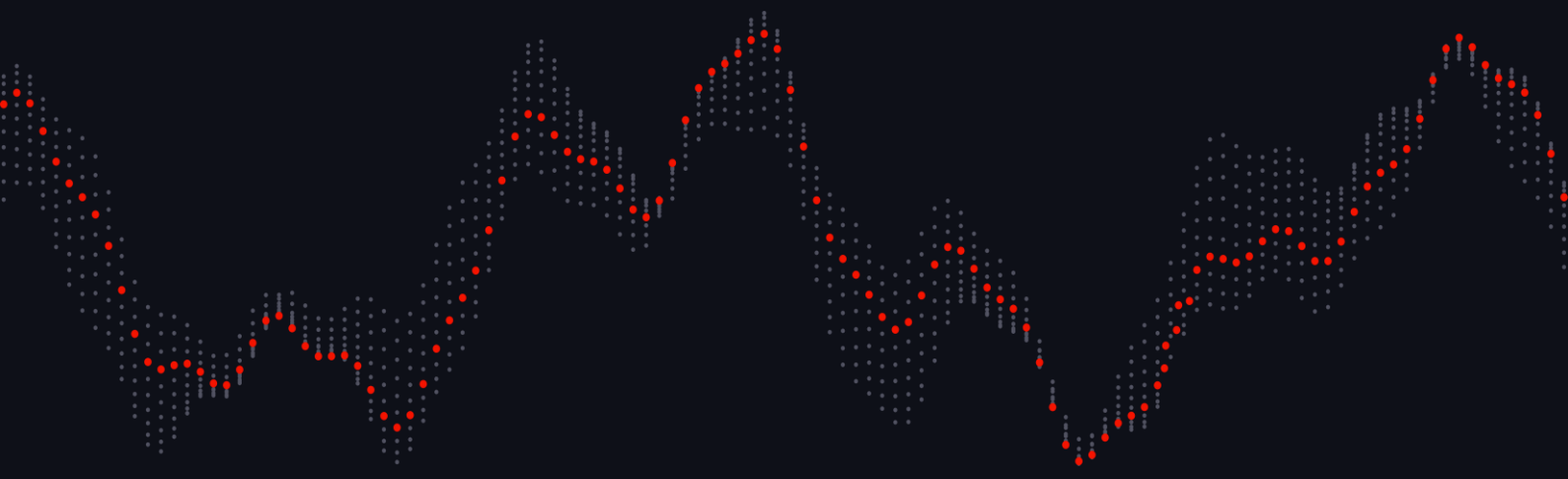
ENTSCHEIDENDER WIRD DIE FRAGE:
Ergibt dieses Verhalten Sinn?

Organisationen, die diese Frage schnell beantworten können, sind besser darauf vorbereitet, Missbrauch einzudämmen, kritische Abläufe zu schützen und ihre Resilienzanforderungen zu erfüllen.

14

ABSCHNITT 14

Fazit



Das nächste Kapitel der Unternehmenssicherheit ersetzt weder Identity Governance noch Compliance, Zugriffskontrollen oder Security Operations.
Verhaltensanalyse wie User and Entity Behavior Analytics (UEBA) und Identity Threat Detection and Response (ITDR) ergänzen diese Disziplinen, indem sie sichtbar machen, wie legitime Zugriffe nach der Authentifizierung tatsächlich genutzt werden.

> Ob SAP, Avaloq, Epic, Oracle, Abacus, ein Kernbankensystem oder eine andere Kronjuwel-Anwendung, die Frage bleibt dieselbe:
>
> **Erkennen wir Missbrauch schnell genug?**

Genau daran kann sich entscheiden, ob aus einem Vorfall eine beherrschbare Situation oder eine handfeste Unternehmenskrise wird.

Die Resilienz der Zukunft hängt nicht nur davon ab, Zugriff zu steuern – sondern Verhalten zu verstehen.

Und in einer Welt, in der Angreifer immer häufiger über legitime Identitäten agieren, könnte genau dieses Verständnis zu einer der wichtigsten Sicherheitsfähigkeiten werden, die Organisationen im kommenden Jahrzehnt entwickeln.

exeon