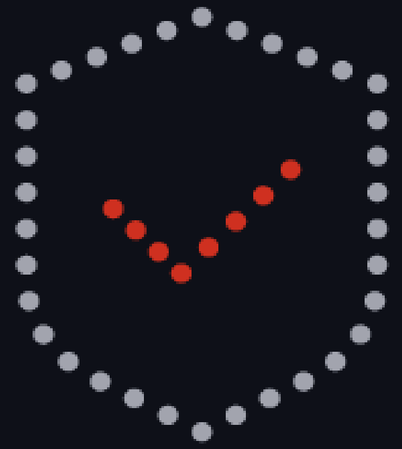
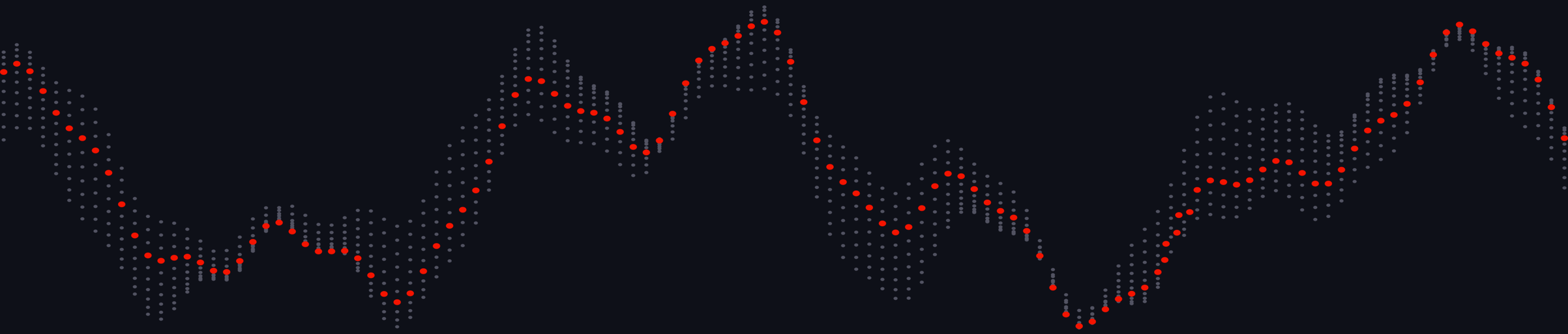
Der Leitfaden zur effektiven Bedrohungserkennung in SAP



Was klassische Kontrollen leisten, wo ihre Grenzen liegen und wie verhaltensbasierte Überwachung die SAP-Erkennungslücke schliesst



exeon

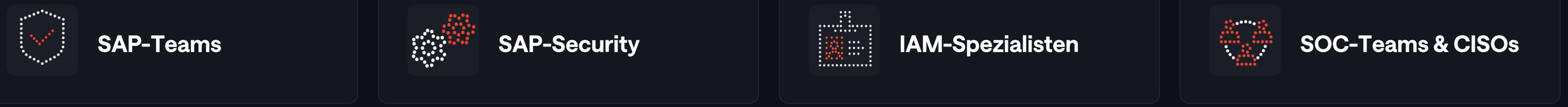
exeon.com

01 Warum klassische SAP Security nicht mehr ausreicht

SAP-Systeme stehen im Zentrum vieler Unternehmen. Sie verarbeiten Finanztransaktionen, Produktionsabläufe, HR-Daten, Beschaffung, Supply-Chain-Prozesse sowie geschäftskritische Reports.

Mit S/4HANA-Migrationen, hybriden Architekturen und RISE wächst die Angriffsfläche deutlich. Gleichzeitig nutzen Angreifer vermehrt gültige Zugangsdaten, missbrauchte Rechte und vertrauenswürdige Zugriffe statt technischer Exploits.

Angreifer müssen nicht in SAP einbrechen, wenn sie sich einfach einloggen und sich darin bewegen können.
Das betrifft:



ZENTRALE FRAGE

Wie unterscheidet man legitimes von gefährlichem Verhalten in SAP?

Klassische SAP Security Controls bleiben unverzichtbar. Für moderne Threat Detection reichen sie allein jedoch nicht mehr aus.

DIESER LEITFADEN ZEIGT

Wofür klassische SAP Security Controls entwickelt wurden

Wo ihre Grenzen beginnen

Warum Behavioral Monitoring immer wichtiger wird

Wie Unternehmen die Detection Gap in SAP schliessen können

02 SAP Hardening und GRC Controls

ETABLIERTE CONTROLS

- Sichere SAP-Konfiguration
- SAP Identity and Access Management (IAM)
- SAP Authorizations und Role-Based Access Controls (RBAC)
- Privileged Access Governance und Emergency Access Management
- SAP GRC und Segregation of Duties (SoD)
- Patch- und Transport-Management
- Sichere RFC-, Interface- und API-Konfigurationen

SAP-SYSTEME ENTHALTEN

hoch privilegierte Accounts

sensible Geschäftsdaten

umfassende Transaktionsfunktionen

systemübergreifende Vertrauensbeziehungen

Hardening reduziert die Angriffsfläche, erklärt aber kein Verhalten.

RESTRISIKO

Auch gehärtete SAP-Systeme können missbraucht werden

- **Gestohlene Zugangsdaten**
- **Missbrauch privilegierter Accounts**
- **Insider-Threats**
- **Missbrauch von APIs und kompromittierten Integrationen**
- **Supply-Chain-Angriffe über vertrauenswürdige Zugriffe Dritter**
- **Legitime Transaktionen in verdächtigen Zusammenhängen**

Viele SAP-Angriffe nutzen autorisierte Aktionen statt Exploits.

Wie der Verizon DBIR zeigt: **Moderne Angreifer brechen nicht ein – sie loggen sich ein.** [1]

03 Segregation of Duties (SoD)

Segregation of Duties ist ein Grundpfeiler der SAP Security und soll verhindern, dass ein einzelner User kritische Geschäftsprozesse ohne Kontrolle missbrauchen kann.

Typische Konflikte sind:

Vendor Creation + Payment Approval

User Administration + Löschen von Audit Logs

Financial Posting + Reconciliation Approval

SAP GRC und Authorization Frameworks erkennen statische Konflikte zuverlässig.

SoD zeigt jedoch nur, was ein User *theoretisch tun könnte,* nicht, ob sein Verhalten zur Laufzeit verdächtig ist.

LAUFZEITRISIKO

Blind Spots von SoD

Ein privilegierter User erhält vorübergehend höhere Rechte

Eine Rolle wird ausserhalb des üblichen Verhaltens geändert

Ein User führt plötzlich Transaktionen aus, die er bisher nie genutzt hat

JE NACH KONTEXT UND REIHENFOLGE KÖNNEN DIESE EREIGNISSE DARAUF HINDEUTEN:

kompromittierte Zugangsdaten

Insider Misuse

Privilege Escalation

vorbereitende Aktivitäten

Klassische SoD Frameworks prüfen Berechtigungsstrukturen und Regelkonflikte. Sie wurden nicht dafür entwickelt, das Verhalten von Identities in produktiven SAP-Umgebungen zu korrelieren.

04 Audit Logs und SAP Security Audit Log (SAL)

ERFASSTE LOG-TYPEN

- SAP Security Audit Log (SAL)
- Change Logs
- Transaction Logs
- User Authentication Logs
- Table Access Logs
- Änderungen an Transports und Konfigurationen

SAL ERFASST

- Login-Versuche
- RFC-Aktivität
- Ausgeführte Transaktionen
- User Changes
- Authorization Events

WICHTIGSTE USE CASES

Audits

Compliance Investigations

Rekonstruktion von Incidents

Logging allein ist noch keine Detection, **denn Events zu sammeln bedeutet nicht, Risiken zu verstehen.**

KONTEXT ZÄHLT

Die Herausforderung bei SAP Logging

SAP-Aktivität ist stark kontextabhängig. Viele Unternehmen kämpfen mit:

- lückenhaftem Logging
- hohem Rauschen
- kurzer Retention
- hohen SIEM-Kosten
- fehlender Korrelation

USR02

Der Zugriff auf die sensible **SAP-Benutzertabelle (USR02)** kann für einen User legitim und für einen anderen verdächtig sein

SU01

SAP User Administration (SU01) ist für einen Administrator Routine, für einen Functional Consultant jedoch ungewöhnlich

SCC4

Änderungen am **SAP Client-Schutz** und an **Client-Einstellungen (SCC4)** können Wartung oder Manipulation bedeuten

Ohne Behavioral Context liefern statische Logs viele operative Daten, aber nur wenig Detection Value. Deshalb werden SAP-Logs häufig erst nach einem Incident geprüft, statt verdächtiges Verhalten kontinuierlich zu überwachen.

05 SIEM-basierte SAP-Detection

INTEGRATION VON SAP-LOGS IN SIEM-PLATTFORMEN

- Korrelation über mehrere Systeme
- Zentrale Alarme
- Compliance-Reporting
- SOC-Workflows

WAS SIEM-PLATTFORMEN ERKENNEN

- Fehlgeschlagene Logins
- Bekannte Regelverstösse
- Ausführung bestimmter Transaktionen
- Konfigurationsänderungen
- Übermässig viele Authentication-Failures

Klassische SIEM-Logik ist weitgehend Event- und regelbasiert.

Eine Angriffssequenz kann einen privilegierten Login, eine Rollenänderung, den Zugriff auf sensible Tabellen, den Datenexport und den Lateral Movement umfassen.

> Einzeln kann jede Aktion legitim wirken.
> Das Risiko entsteht aus Timing, Reihenfolge, Kontext und der Abweichung vom bisherigen Verhalten.

Behavioral analytics erweitert die SIEM Visibility, indem es Signale über Identities und Systeme hinweg verbindet – eine zentrale Voraussetzung für Identity Threat Detection and Response (ITDR).

SIEM UND SOC HERAUSFORDERUNGEN

Alert Noise, manuelle Korrelation und fehlendes SAP-Wissen

67%

der Alarme werden wegen Rauschen und False Positives ignoriert [2]

SOC-Teams bearbeiten täglich Tausende Alarme

Analysts wenden viel Zeit für manuelle Korrelation auf [3]

SAP-Terminologie ist hoch spezialisiert

SOC-Analysts fehlt oft SAP-Expertise

SAP-Teams betreiben selten selbst das SOC

Viele SOCs können SAP-Logs aufnehmen, aber SAP-Verhalten nicht im operativen Kontext interpretieren.

06 Die Grenzen von statischen Überwachungsregeln

Statische SAP-Controls zeigen ob:

- eine Regel verletzt wurde
- ein Event auftrat
- oder ein User zu viele Rechte besitzt

Sie beantworten nicht ob:

- Verhalten normal ist
- eine Sequenz auf bösartige Absicht hindeutet
- oder ein User früher schon so gehandelt hat

Diese Unterscheidung ist wichtig, weil moderne SAP-Angriffe zunehmend legitime Betriebsaktivitäten imitieren.

BEISPIELE SIND

- erstmalige Nutzung privilegierter Transaktionen
- Zugriff auf sensible Tabellen ausserhalb des üblichen Verhaltens
- temporäre Role-Escalation
- Data Access mit anschliessendem Export
- ungewöhnliche mandantenübergreifende Aktivitäten

Keines dieser Events muss eine definierte Regel verletzen. Zusammen können sie jedoch eine frühe Kompromittierung sichtbar machen.

Statische Kontrollen zeigen Events, Verhaltens-Monitoring ergänzt jedoch den Kontext zur möglichen Absicht und schliesst damit eine häufige Lücke in Threat Detection und ITDR in SAP-Umgebungen.

07 Wie Verhaltensanalyse SAP-Security verändert

Behavioral Detection erstellt Baselines für:

- Typische Transaktionen
- Normales Login-Verhalten
- Erwarteten Table Access
- Übliche Peer-Group-Aktivität
- Bisherige Nutzung von Privilegien

So werden Abweichungen sichtbar:

- Erstmalige Nutzung von SAP User Administration (SU01) oder SAP Role Management (PFCG)
- Ungewöhnlicher Zugriff auf die sensible SAP Benutzertabelle (USR02)
- Privilegierte Transaktionen zu unüblichen Zeiten
- Neue Kombinationen von SAP-Aktivitäten
- Plötzlicher Anstieg beim Data Access
- Anomalien über mehrere Systeme hinweg

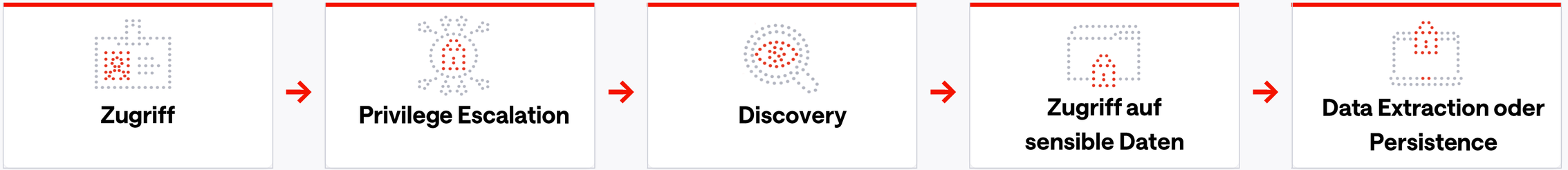
Dieser Kontext hilft dabei, legitime Administration von verdächtiger privilegierter Aktivität zu unterscheiden. Die Detection Quality steigt, während die Alert Fatigue sinkt.

SAP-Teams behalten ihr operatives Wissen	SOC-Teams erhalten kontextreiche Alarme	IAM und Compliance gewinnen Behavioral Visibility

Gemeinsam entsteht ein handlungsorientierter Ansatz für Identity Threat Detection and Response.

08 Kontextbasierte Bedrohungserkennung in Echtzeit

Angreifer führen selten nur eine verdächtige Aktion aus. Sie durchlaufen mehrere Phasen:



BEISPIEL

1. Ein User loggt sich von einem neuen Gerät ein
2. Derselbe User nutzt erstmals die SAP User Administration (SU01)
3. Er ändert eine Rolle im SAP Role Management (PFCG)
4. Kurz danach greift er auf die sensible SAP Benutzertabelle (USR02) zu

Ein neues Gerät oder die erstmalige Nutzung der SAP User Administration (SU01) kann legitim sein. Ändert derselbe User danach eine Rolle im SAP Role Management (PFCG) und greift auf die sensible SAP Benutzertabelle (USR02) zu, bildet die Sequenz ein deutlich verdächtigeres Muster als jeder einzelne Alert.

Die Fähigkeit, eine Bedrohung als Sequenz statt als einzelne Events zu erkennen, wird in hybriden SAP-Landschaften immer wichtiger:

- SAP umfasst mehrere Systeme
- Cloud und On-Prem arbeiten zusammen
- Identities überschreiten Organisationsgrenzen
- APIs und Service Accounts interagieren laufend

Real-Time Sequence Detection kann verdächtiges Verhalten erkennen, bevor geschäftlicher Schaden entsteht. Nicht ein einzelnes Event ist die Bedrohung, sondern das gemeinsame Muster.

09 Datensouveränität und Schutz

FÜR REGULIERTE BRANCHEN

- Banking und Financial Services
- Manufacturing
- Pharma und Healthcare
- Energie und Utilities
- Public Sector und kritische Infrastruktur

Diese Unternehmen müssen unter anderem DORA, NIS2 und DSGVO erfüllen.

Das erschwert SAP-Monitoring:

- Identity Data sind hochsensibel
- Grenzüberschreitende Log-Verarbeitung kann eingeschränkt sein
- Public Cloud Analytics sind nicht immer zulässig
- Manche Umgebungen verlangen Sovereign oder On-Prem Deployment

DEPLOYMENT- UND PRIVACY-OPTIONEN

Sovereign Cloud

On-Prem

Privacy-Preserving Analytics

Identity Anonymization

Minimaler SAP Fussabdruck

Keine zusätzlichen SAP Agents

Diese Optionen ermöglichen moderne Detection ohne unnötige Komplexität oder zusätzliche Risiken für geschäftskritische SAP-Systeme, denn **Security Visibility darf Compliance nicht gefährden.**

ZUSAMMENFASSUNG

Die wichtigsten Erkenntnisse

Klassische SAP Controls bleiben unverzichtbar. Hardening, SoD, SAL-Logging und SIEM-Integration schaffen Governance, Compliance und Visibility. Verdächtiges Verhalten einer autorisierten Identity zur Laufzeit erkennen sie jedoch nicht.

Angreifer missbrauchen gültige Identities, legitime Transaktionen und vertrauenswürdige Zugriffe, die einzeln normal wirken.
Ein Unternehmen kann daher Rollen kontrollieren, Audits bestehen und umfangreiche Logs sammeln, ohne bösartiges oder riskantes Verhalten rechtzeitig zu erkennen.

Behavioral Monitoring ergänzt den fehlenden Kontext. Die Korrelation von Identity- und Aktivitätssignalen über Zeit und Systeme hinweg stärkt SAP Threat Detection und eine breitere ITDR-Strategie.

Kann ein Unternehmen Rollen prüfen, Audits bestehen und Logs sammeln, aber privilegiertes SAP-Verhalten nicht schnell als normal oder bedrohlich einordnen, fehlt nicht Logging. Es fehlt Detection Context.

NÄCHSTE SCHRITTE

WO IN VIELEN SAP-UMGEBUNGEN RISIKEN BLEIBEN

Privilegierte Transaktionen ohne Behavioral Validation	**Zugriff auf sensible Tabellen ohne kontextbezogene Risk Scores**	**Statische statt verhaltensbasierte Bewertung von Rollenänderungen**	**SAP-Alarme ohne operativen Kontext im SOC**	**Grosse Mengen SAP Logs ohne klare Priorisierung**

Die Frage lautet nicht mehr, “Überwachen wir SAP?” sondern, “Erkennen wir Missbrauch, der sich in legitimem SAP-Verhalten verbirgt?”

Prüfen Sie Blind Spots bei:

 **privilegierten Transaktionen**	 **sensiblen Tabellen**	 **Systemübergreifende Korrelation**	 **Real-Time Anomaly Detection**	 **Interpretation von SAP-Aktivität im SOC**

In SAP ist oft nicht das gefährlich, was blockiert wird, sondern das, was normal aussieht.

QUELLEN

Behavioral SAP Detection live erleben

[1] Verizon Data Breach Investigations Report (DBIR): https://www.verizon.com/business/resources/reports/dbir/

[2] A Unified Framework for Human–AI Collaboration in Security Operations Centers with Trusted Autonomy: https://arxiv.org/html/2505.23397v2

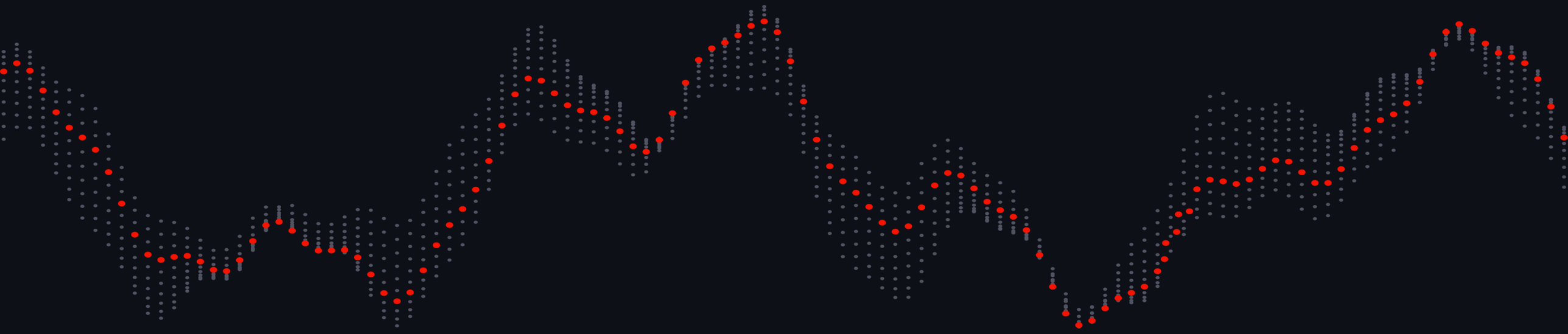
[3] Elastic Security Operations Report: https://www.elastic.co/resources/security/report/global-threat-report

[4] ENISA Threat Landscape 2024: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[5] Gartner – Shadow IT Overview: https://www.ibm.com/think/topics/shadow-it

[6] IBM Cost of a Data Breach Report: https://www.ibm.com/reports/data-breach

Demo buchen



exeon

Gartner

ATTESTA
ISO 27001
CERTIFIED

CYBERSECURITY™
MADE IN EUROPE