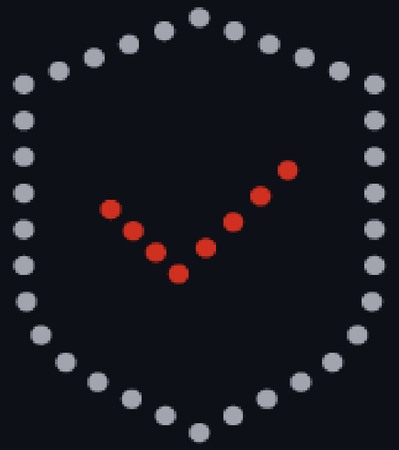
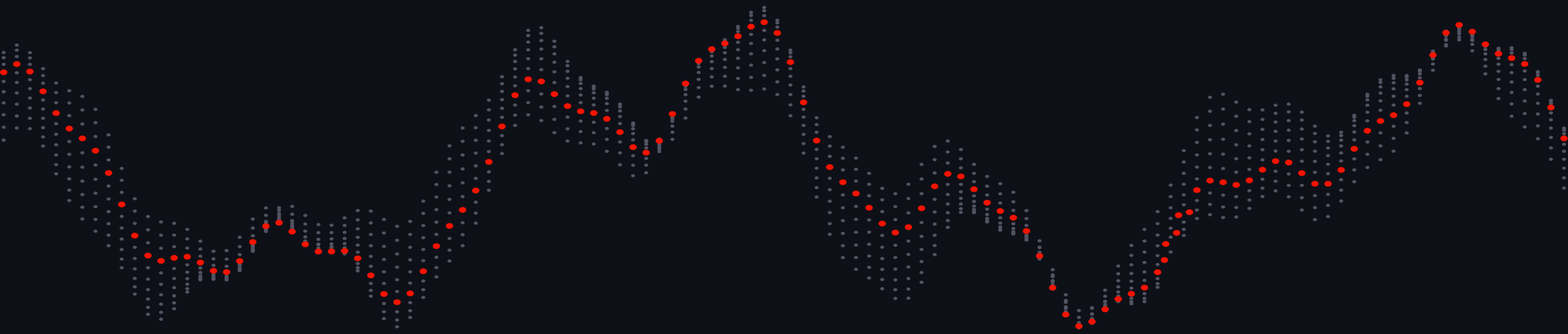
The Complete Guide to SAP Security Monitoring and Threat Detection



What traditional controls were built to do, where their detection limits begin, and how behavioral monitoring closes the SAP detection gap



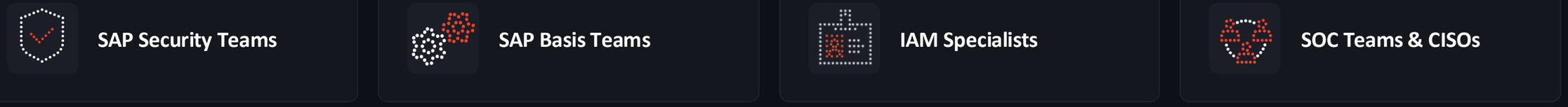
exeon

01 Why Traditional SAP Security Is No Longer Enough

SAP systems sit at the center of the enterprise. They process financial transactions, production workflows, HR data, procurement, supply chain operations and business-critical reporting.

As organizations modernize SAP landscapes through S/4HANA migrations, hybrid architectures, and RISE deployments, the attack surface expands significantly. At the same time, attackers increasingly rely on valid credentials, privilege misuse, and trusted access rather than technical exploits.

Attackers do not need to break SAP when they can simply operate inside it.
This creates a fundamental challenge for:



THE CORE CHALLENGE

How do you distinguish legitimate SAP activity from malicious behavior hidden inside normal operations?

Traditional SAP security controls remain essential. But on their own, they are no longer sufficient for modern threat detection.

WHAT THIS GUIDE COVERS

What traditional SAP security controls are designed to do

Where their detection limitations begin

Why behavioral monitoring is becoming essential

How organizations can close the SAP detection gap

02 SAP Hardening and GRC Controls

CONTROLS IN PLACE

- Secure SAP configuration
- SAP Identity and Access Management (IAM)
- SAP authorizations and role-based access control (RBAC)
- Privileged access governance and emergency access management
- SAP GRC and Segregation of Duties (SoD) controls
- Patch and transport management
- Secure RFC, interface, and API configurations

WHAT SAP SYSTEMS CONTAIN

Highly privileged accounts

Sensitive business data

Extensive transaction capabilities

Cross-system trust relationships

Hardening reduces exposure, but it does not explain behavior.

A hardened SAP system can still be abused through:

Stolen credentials

Misused privileged accounts

Insider threats

API misuse and compromised integrations

Supply-chain compromise through trusted third-party access

Legitimate transactions executed in suspicious ways

This is especially relevant because many SAP attacks involve authorized actions rather than exploits. According to Verizon's DBIR, **attackers increasingly “log in, not break in”.** [1]

03 Segregation of Duties (SoD)

Segregation of Duties is one of the foundational pillars of SAP security.

The goal is straightforward: **No single user should have enough permissions to abuse critical business processes without oversight.**

Examples include preventing combinations such as:

Vendor creation + payment approval

User administration + audit log deletion

Financial posting + reconciliation approval

SAP GRC and authorization frameworks are highly effective at identifying static conflicts. However, SoD identifies what a user *could theoretically do*, not whether the activity is operationally suspicious.

RUNTIME EXPOSURE

SoD Blind Spots

A privileged user may temporarily receive elevated access

A role may be modified outside normal behavior

A user may suddenly begin using transactions they never used before

WHAT THESE MAY INDICATE

Credential compromise

Insider misuse

Privilege escalation

Malicious staging activity

Traditional SoD frameworks were not designed to detect suspicious behavior during runtime. They evaluate authorization structures and rule conflicts, not how users actually behave inside productive SAP environments.

04 Audit Logs and SAP Security Audit Log (SAL)

LOG TYPES COLLECTED

SAP Security Audit Log (SAL)
Change logs
Transaction logs
User authentication logs
Table access logs
Transport and configuration changes

WHAT SAL RECORDS

Logon attempts
RFC activity
Transaction execution
User changes
Authorization events

PRIMARY LOG USE CASES

Audits

Compliance investigations

Incident reconstruction

Logging alone does not provide detection. **Collecting logs is not the same as understanding risk.**

SAP activity is highly contextual

Many organizations struggle with:

- Incomplete logging coverage
- Excessive log noise
- Lack of contextual correlation
- High SIEM ingestion cost
- Limited retention windows

In practice, SAP logs are often reviewed reactively after incidents rather than continuously monitored behaviorally.

USR02

Access to the sensitive SAP **user table** USR02 may be legitimate for one user but suspicious for another

SU01

Use of SU01 (SAP **user administration**) may be routine for an administrator but abnormal for a functional consultant

SCC4

Changes in SCC4 (**client protection and client settings**) may reflect planned maintenance or malicious manipulation

Without behavioral context, static logging produces **large volumes of operational data** but **limited detection capability.**

05 SIEM-Based SAP Detection

INTEGRATION OF SAP LOGS INTO SIEM PLATFORMS

- Correlation across systems
- Centralized alerting
- Compliance reporting
- SOC workflows

WHAT SIEM PLATFORMS DETECT

- Failed logins
- Known rule violations
- Specific transaction execution
- Configuration changes
- Excessive authentication failures

Traditional SIEM logic is largely event-driven and rule-based.

A SINGLE ATTACK SEQUENCE

SAP attacks rarely unfold as isolated events

Privileged login

↓

Role modification

↓

Sensitive table access

↓

Data export

↓

Lateral movement

Individually, each action may appear legitimate.

The risk emerges from: Timing / Sequence / Context / Deviation from historical behavior.

SIEM & SOC CHALLENGES

67%

of alerts are ignored due to noise and false positives [2]

SOC teams handle thousands of alerts daily

Analysts spend substantial time manually correlating events [3]

THE EXPERTISE GAP

SAP terminology is highly specialized

SOC analysts often lack SAP expertise

SAP teams rarely operate the SOC themselves

Many SOCs can ingest SAP logs, but cannot truly interpret SAP behavior.

06 The Limitations of Static Monitoring

Static SAP security controls answer:

Was a rule violated?

Did an event occur?

Does a user have excessive permissions?

They do not answer:

Is this behavior normal?

Does this sequence indicate malicious intent?

Has this user ever behaved this way before?

This distinction matters because modern SAP attacks increasingly mimic legitimate operational activity.

COMMON EXAMPLES

- First-time use of privileged transactions
- Access to sensitive tables outside baseline behavior
- Temporary role escalation
- Data access followed by export activity
- Unusual cross-client activity

None of these necessarily violates predefined rules. Yet they may represent early-stage compromise.

Static controls provide visibility into events. Behavioral monitoring provides visibility into intent.
This is the core detection gap in many SAP environments.

07 Why Behavioral Detection Changes SAP Security

Behavioral detection enables baselines such as:

- Typical transaction usage
- Normal login behavior
- Expected table access
- Common peer-group activity
- Historical privilege usage

Suspicious deviations become visible:

- First-time use of SU01 or PFCG
- Unusual access to USR02
- Privileged transactions executed at abnormal times
- New combinations of SAP activity
- Sudden spikes in data access
- Behavioral anomalies across multiple systems

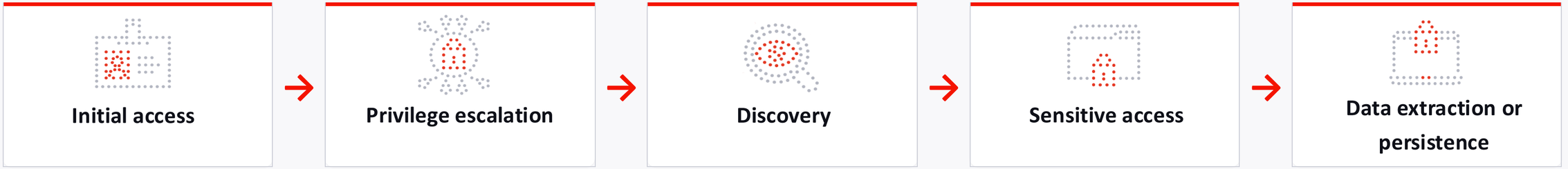
Behavioral detection helps distinguish legitimate administration from suspicious privileged activity. This significantly improves detection quality while reducing alert fatigue. It also supports broader organizational alignment:

SAP teams retain operational understanding	SOC teams receive contextualized alerts	IAM and compliance teams gain behavioral visibility

The result is a much more actionable security posture.

08 Real-Time Sequence Detection

Attackers rarely perform one suspicious action. Instead, they move through stages.



EXAMPLE SEQUENCE

1. User logs in from a new device
2. Executes SU01 for the first time
3. Modifies a role in PFCG
4. Accesses USR02 shortly afterward

The capability of the threat being the sequence is increasingly important in hybrid SAP landscapes where:

- SAP spans multiple systems
- Cloud and on-prem environments coexist
- Identity flows across organizational boundaries
- APIs and service accounts interact continuously

Real-time sequence detection allows organizations to identify suspicious behavior before business impact occurs.

Viewed individually, each action may appear harmless. Behavioral sequence detection identifies when these actions become suspicious together. **The threat is not any single event. It is the sequence.**

09 Sovereign Deployment and Data Privacy

BUILT FOR REGULATED INDUSTRIES

Banking and financial services
Manufacturing
Pharma and healthcare
Energy and utilities
Public sector and critical infrastructure

These organizations face growing pressure from sector-specific regulations such as DORA and NIS2, alongside broader data protection frameworks like GDPR.

This creates additional challenges for SAP monitoring because:

- Identity data is highly sensitive
- Cross-border log processing may be restricted
- Public cloud analytics are not always acceptable
- Some environments require sovereign or on-prem deployment

DEPLOYMENT & PRIVACY CAPABILITIES

Sovereign cloud deployment

On-prem operation

Privacy-preserving analytics

Identity anonymization

Minimal SAP footprint

No additional SAP agents

This becomes particularly important for organizations that want advanced detection without introducing operational complexity or additional risk into business-critical SAP systems.
Security visibility must not come at the cost of compliance.

IN SUMMARY

Key Takeaways

Traditional SAP security controls remain essential. Hardening, SoD frameworks, SAL logging and SIEM integration all provide important layers of governance and visibility. But this alone is no longer enough. **Modern SAP attacks operate inside legitimate activity.**

Traditional SAP security measures are primarily designed to ensure that users receive the appropriate access, policy violations can be identified, and critical activities remain auditable. They are highly effective at governing authorizations, enforcing compliance requirements, and reducing configuration-related risk.
However, they were not designed to determine whether an authorized user behaves suspiciously during runtime. **This is the core SAP detection gap.**

Attackers increasingly abuse valid identities, legitimate SAP transactions, and trusted access paths that appear normal in isolation. As a result, organizations may successfully manage roles, pass audits and collect extensive SAP logs, while still lacking the ability to recognize when legitimate SAP activity becomes malicious, abnormal or high-risk.

If your organization can review roles, pass audits, and collect logs, but still cannot quickly determine whether privileged SAP behavior is normal or threatening, the issue is no longer logging coverage. It is a detection context.

WHERE EXPOSURE REMAINS IN MANY SAP ENVIRONMENTS

Privileged transactions executed without behavioral validation	**Sensitive table access without contextual risk scoring**	**Role changes evaluated statically rather than behaviorally**	**SOC teams receiving SAP alerts without operational context**	**Large volumes of SAP logs without actionable prioritization**

The question is no longer: “Do we monitor SAP?”

The real question is: “Can we detect misuse hidden inside legitimate SAP behavior in real time?”

EVALUATE YOUR NEXT STEPS

Evaluate where your current monitoring may still contain behavioral blind spots, particularly around:

 **Privileged transactions**	 **Sensitive table access**	 **Cross-system activity correlation**	 **Real-time anomaly detection**	 **SOC interpretation capability**

Because in SAP, the most dangerous activity is often not what is blocked. It is what looks normal.

SOURCES

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

[2] Exabeam SIEM & SOC Statistics https://www.exabeam.com/explainers/siem/siem-statistics/

[3] Elastic Security Operations Report https://www.elastic.co/security-labs/security-operations-report

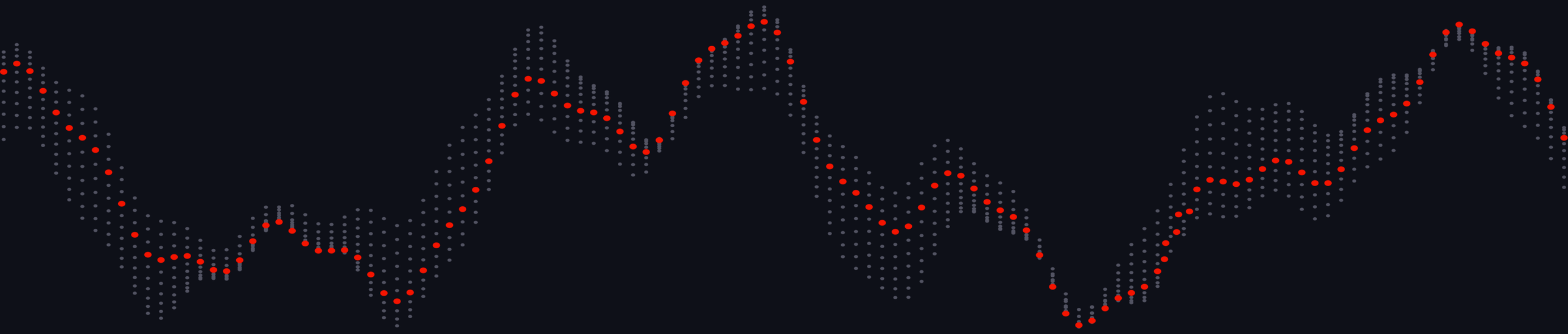
[4] ENISA Threat Landscape https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[5] Gartner – Shadow IT Overview https://www.gartner.com/en/articles/what-is-shadow-it

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

See behavioral SAP detection in action

Book a Demo



exeon

Gartner

ATTESTA ISO 27001 CERTIFIED

CYBERSECURITY™ MADE IN EUROPE