SAP Security Monitoring and Incident Response

Arndt Lingscheid, SAP

Las Vegas

2024

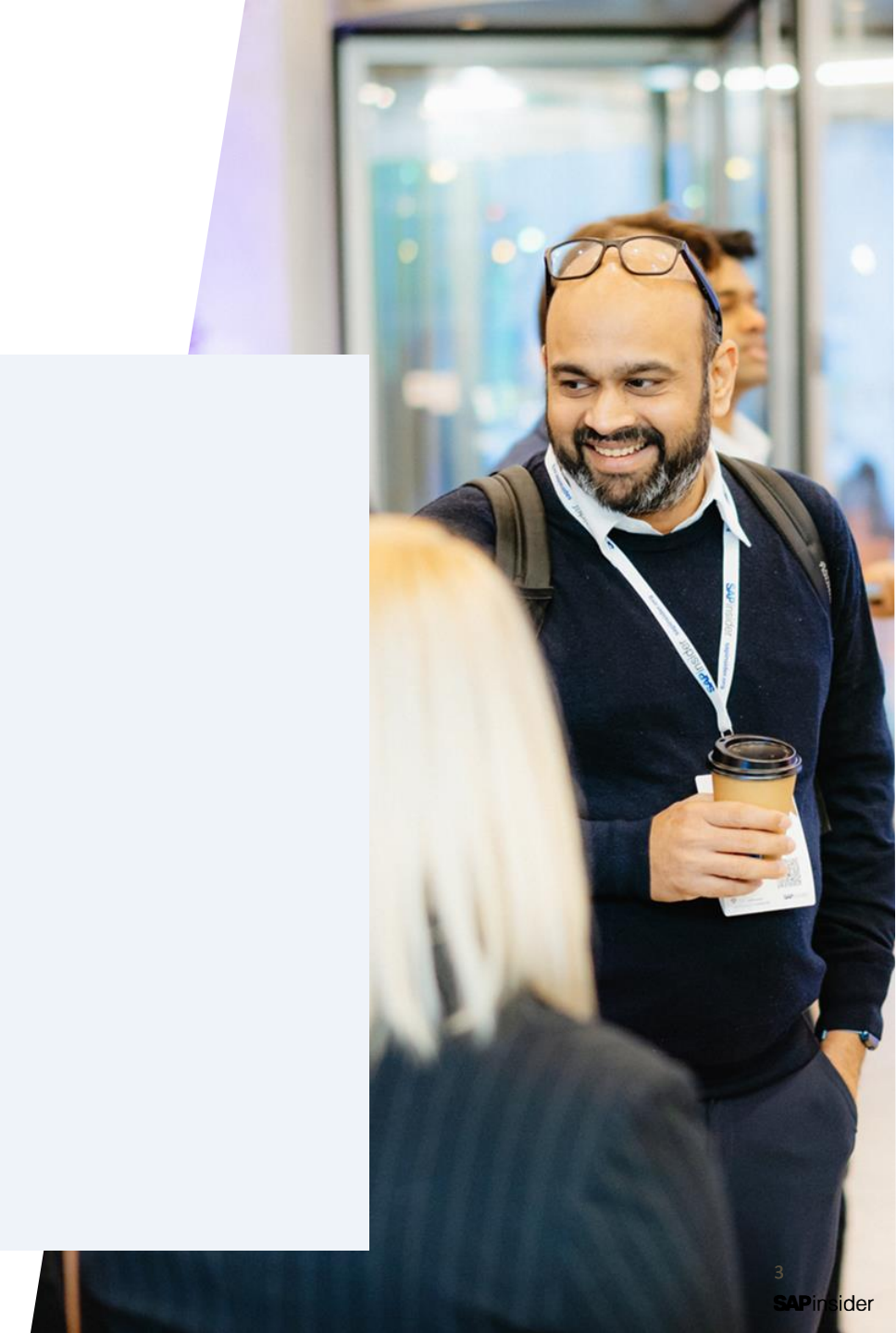
SAPinsider

In This Session

One of the biggest challenges from a cybersecurity perspective is detecting and identifying threats. In this session you will learn about effective security monitoring techniques and incident response strategies for SAP systems. We will discuss real-world examples and case studies to highlight the importance of proactive security measures. We will also explore a comprehensive set of cutting-edge techniques and strategies essential for safeguarding SAP systems. The focus will be on imparting actionable insights into effective security monitoring, ensuring that participants gain a profound understanding of the intricacies involved in securing SAP environments.

What We'll Cover

- Market Trends for application security
- Required Capabilities for application security
- Demo 1 Walk-Through
- Demo 2 Walk-Through
- Demo 3 Walk-Through
- Demo 1 Walk-Through part b
- SAP Enterprise Threat Detection
- Key Points to take home



Market Trends for application security

81%

of breaches used lost, stolen or weak passwords.

Three-quarters **(75%)** of breaches were perpetrated by outsiders, which, of course, means that one-quarter **(25%)** involved internal actors.

64%

of organizations rate their cybersecurity posture as important or very important.

65% of organizations, understand the connection between a strong cybersecurity structure and the reduction of data protection risk for employees, business partners and customers.

87%

of organizations are experiencing a shortfall of security talent.

Global cybersecurity job vacancies grew by **350%**, from 1 million openings in 2013 to **3.5 million in 2021**, according to Cybersecurity Ventures.

88%

of board members said that cybersecurity is viewed as a business risk, up from 58% in 2016.[4]

$6 trillion

is drained from the global economy through cybercrime annually

38%

of organizations can identify risks before it is too late to take action on them.

SAP S/4HANA Source-to-Pay Process

What could go wrong?

Application hacking by malicious actors is a never-ending process leading to black mail, ransom, loss of trust, revenue and penalties.

Malware attacks can lead to the loss of confidentiality, integrity, and availability.

integrity

Modification and changes of business documents.

Privileged user manipulated books, duplicated bills and changed bank details.

Unsecure company secrets and books can lead to a loss of competitive advantage or & misstatement of the financial books.

Breach of Confidentiality: sensitive information has been disclosed to unauthorized individuals.

Loss of Integrity: consistency, accuracy and trustworthiness of data over its lifecycle is lost. Data can be altered by unauthorized individuals.

Loss of Availability: the information is not consistent and readily accessible to authorized persons.

confidentiality

Exfiltration of sensitive credit card, bank details, customer PII, pricing information, order **data** to hackers.

Financial reporting information has been sent automatically to an external e-mail address, to help to predict stock growth.

Vulnerable systems and in-house built apps leading to data breaches and ransomware leading to loss of trust and high penalties.

availability

Customers are unable to make purchases,

Financial or production planning gets delayed

Decision making based on that information must be delayed therefor revenue is lost.

Required Capabilities for application security

1 Managed Service

Simplifying security monitoring in the cloud as SaaS enables a seamless transfer of monitoring activities to SAP or partners, significantly reducing the effort required to manage security resources and lowering the cost of security related tasks by sharing security resources.

2 Audit

Optimize the availability and use of data for complete proof of user behavior, threat and anomaly detection, and forensic analysis in business applications minimizing risk of fraud and hacker attacks.

3 Business

Effectively manage and detect threats at the business application and database level, to ensure smooth operation and comply with legal legislations such as EU NIS2, RCE, KRITIS, GDPR and other local security laws.

4 Scalable

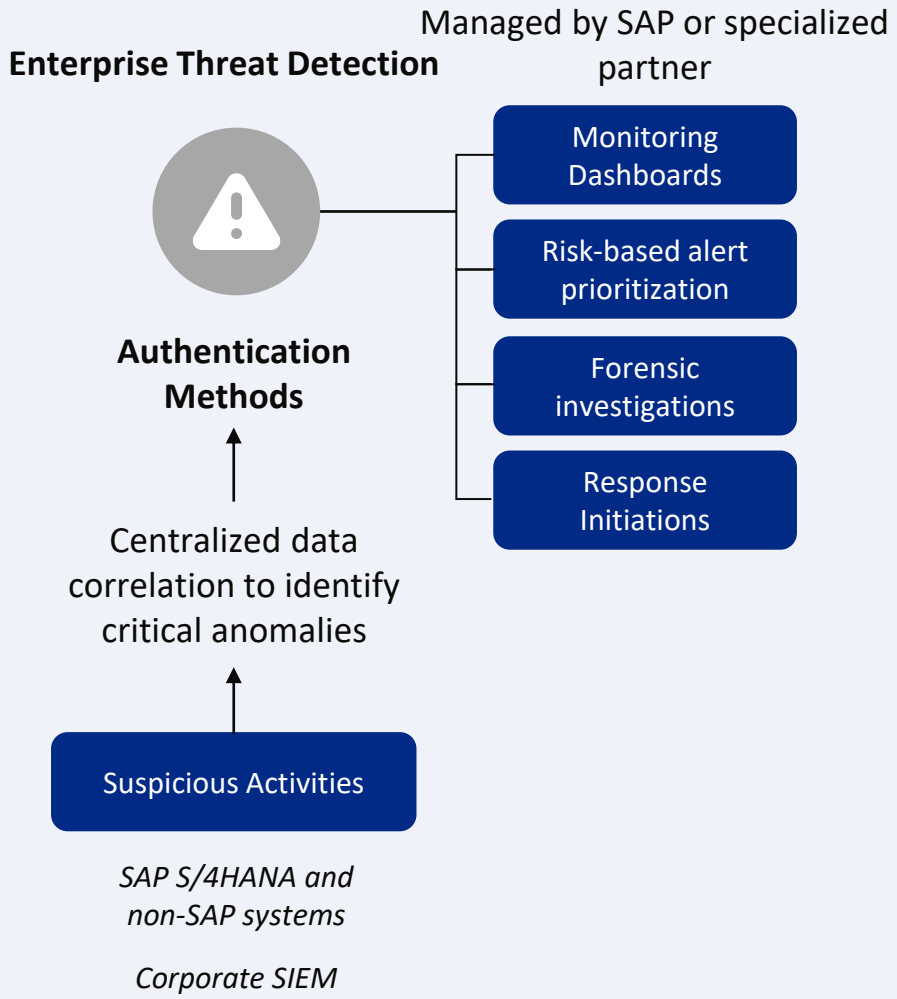
Economically analyze a vast quantity of log data and correlate information cross systems over long time to achieve transparency cross SAP business applications to maximize high value outputs and safeguard the applications.

SAP Enterprise Threat Detection

Solution Capabilities

Managed service from either SAP or a specialized partner to help identify, analyse, and report malicious activities in your SAP applications before serious damage occurs.

- Analyze a vast quantity of log data and correlate information to get a complete picture of landscape activities.
- Detect threats at the application server level and at the database level.
- Find SAP software-specific threats related to known attacks by using attack detection patterns.
- Perform forensic threat detection to discover previously unknown attack variants.
- Create attack detection patterns without the need to code.
- Customize the integration of third-party systems and infrastructure components.



SAP Enterprise Threat Detection

Application hacking by malicious actors is a never-ending process leading to black mail, ransom, loss of trust, revenue and penalties.

Brute force attacks, lost and stolen credentials with successful login leading to identity theft and loss of confidentiality, integrity, and availability.

Modification and changes of business documents.

Privileged user manipulated books, duplicated bills and changed bank details.

Unsecure company secrets and books can lead to a loss of competitive advantage or & misstatement of the financial books.

Breach of Confidentiality: sensitive information has been disclosed to unauthorized individuals.

Loss of Integrity: consistency, accuracy and trustworthiness of data over its lifecycle is lost. Data can be altered by unauthorized individuals.

Loss of Availability: the information is not consistent and readily accessible to authorized persons.

Exfiltration of sensitive credit card, bank details, customer PII, pricing information, order **data** to hackers.

Financial reporting information has been sent automatically to an external e-mail address, to help to predict stock growth.

Vulnerable systems and in-house built apps leading to data breaches and ransomware leading to loss of trust and high penalties.

Customers are unable to make purchases,

Financial or production planning gets delayed

Decision making based on that information must be delayed therefor revenue is lost.

SAP S/4HANA Source-to-Pay Process

What could go wrong?

Brute force attacks, lost and stolen credentials with successful login leading to identity theft and loss of confidentiality, integrity, and availability.

Application hacking by malicious actors is a never-ending process leading to black mail, ransom, loss of trust and penalties.

Creation of new users and vial RFC, promise of

Unsecure company secrets and books can lead to

Forensic Analysis

Continuous Threat Monitoring

Monitor Controls

Manage Incident

Sourcing → Contracting + Forecasting → Requesting + Ordering → Receiving + Invoicing → Invoicing Receipt + Processing → Payment Processing

Detection Processes

information has been disclosed to unauthorized individuals.

User Behaviour Analysis

d, information, order **data** to hackers.

Response Planning

make purchases,

Financial or production

Anomalies and Events

cy

Loss of Availability:
the information is not consistent and readily accessible to authorized persons.

Threat Hunting

been sent ddress, to

Vulnerable systems and in-house built apps leading to data breaches and ransomware leading to loss of trust and high penalties.

Integrate SIEM / SOAR

therefor revenue is lost.

Required Capabilities for application security

1 Managed Service

Simplifying security monitoring in the cloud as SaaS enables a seamless transfer of monitoring activities to SAP or partners, significantly reducing the effort required to manage security resources and lowering the cost of security related tasks by sharing security resources.

2 Audit

Optimize the availability and use of data for complete proof of user behavior, threat and anomaly detection, and forensic analysis in business applications minimizing risk of fraud and hacker attacks.

3 Business

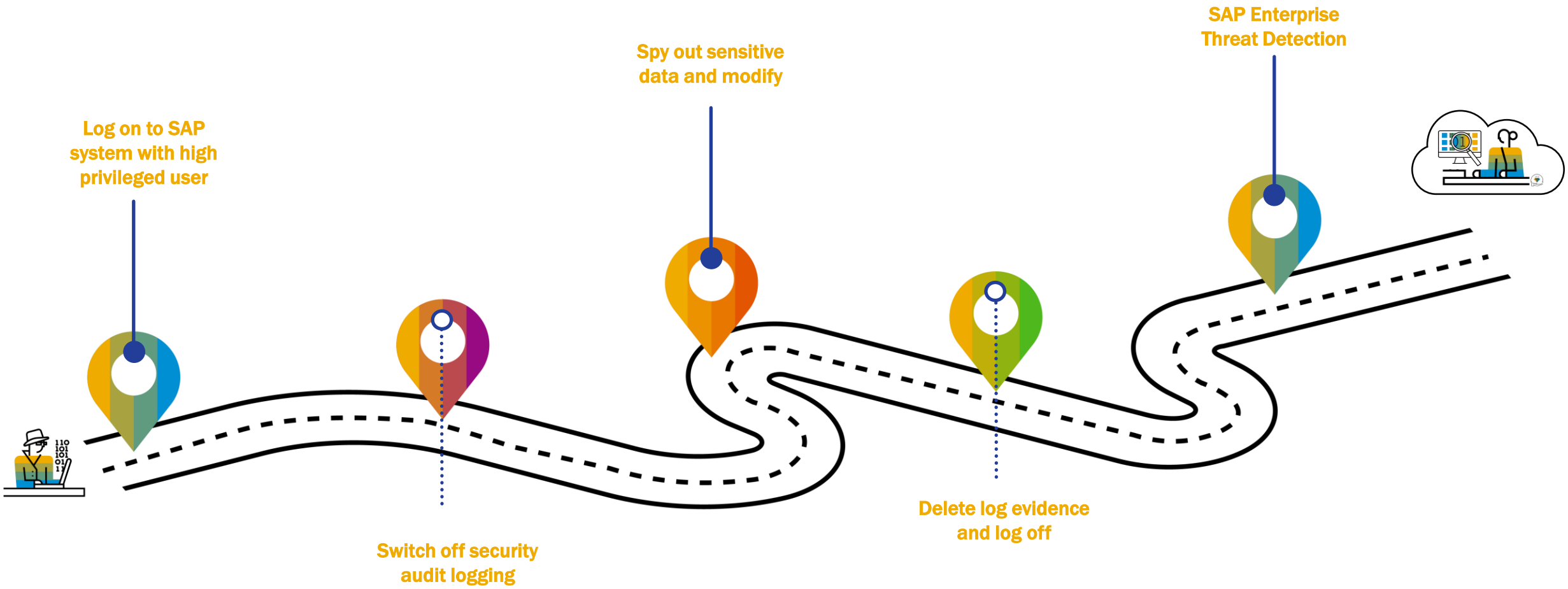
Effectively manage and detect threats at the business application and database level, to ensure smooth operation and comply with legal legislations such as EU NIS2, RCE, KRITIS, GDPR and other local security laws.

4 Scalable

Economically analyze a vast quantity of log data and correlate information cross systems over long time to achieve transparency cross SAP business applications to maximize high value outputs and safeguard the applications.

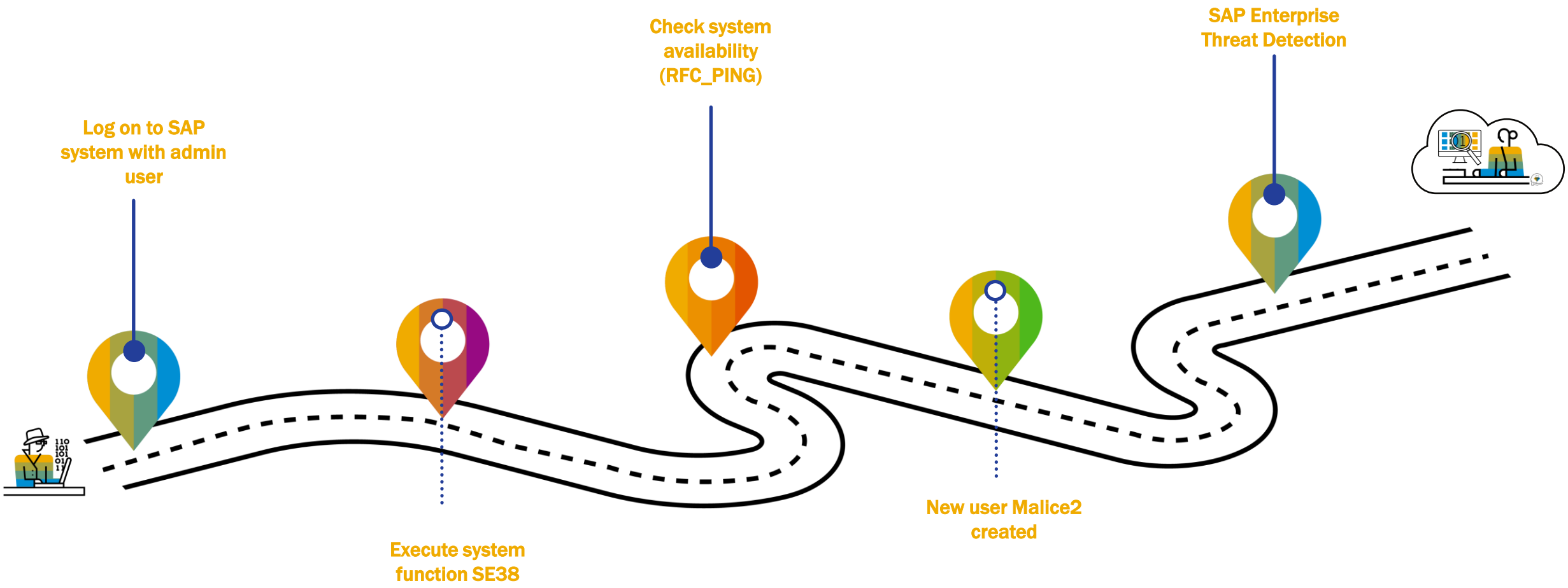
Demo 1 Walk-Through

Sensitive data spy out & manipulation



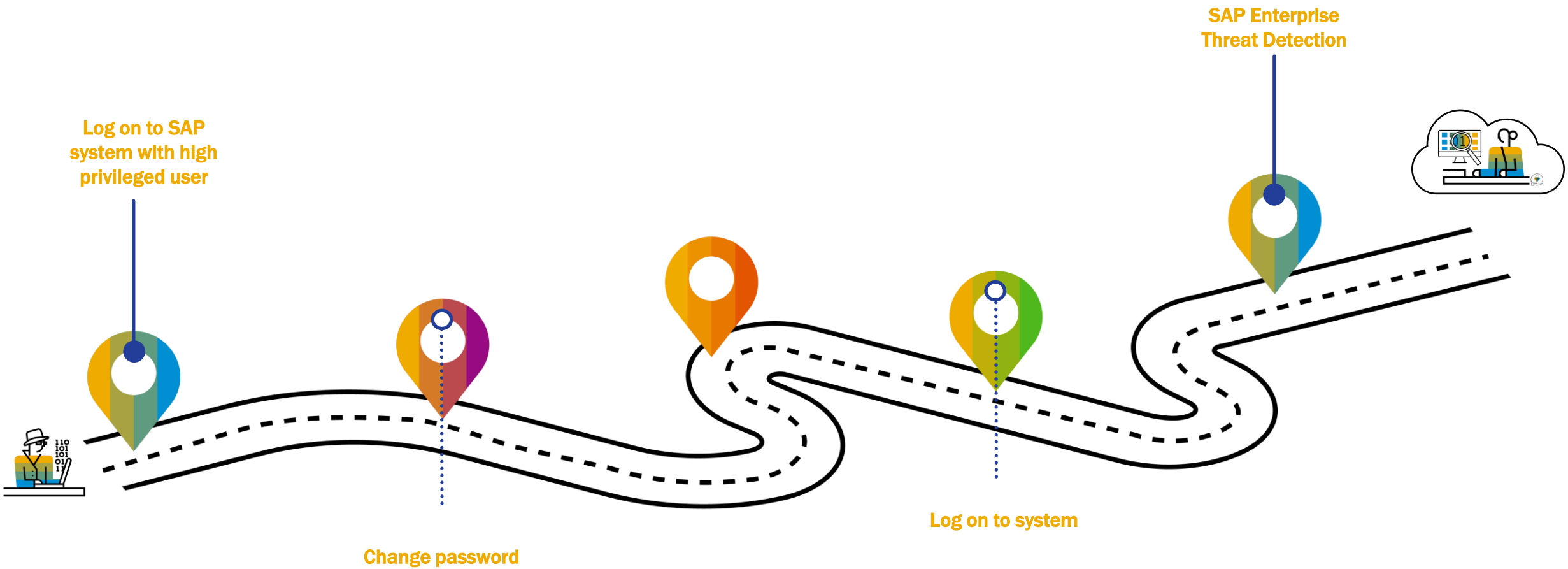
Demo 2 Walk-Through

Create new user



Demo 3 Walk-Through

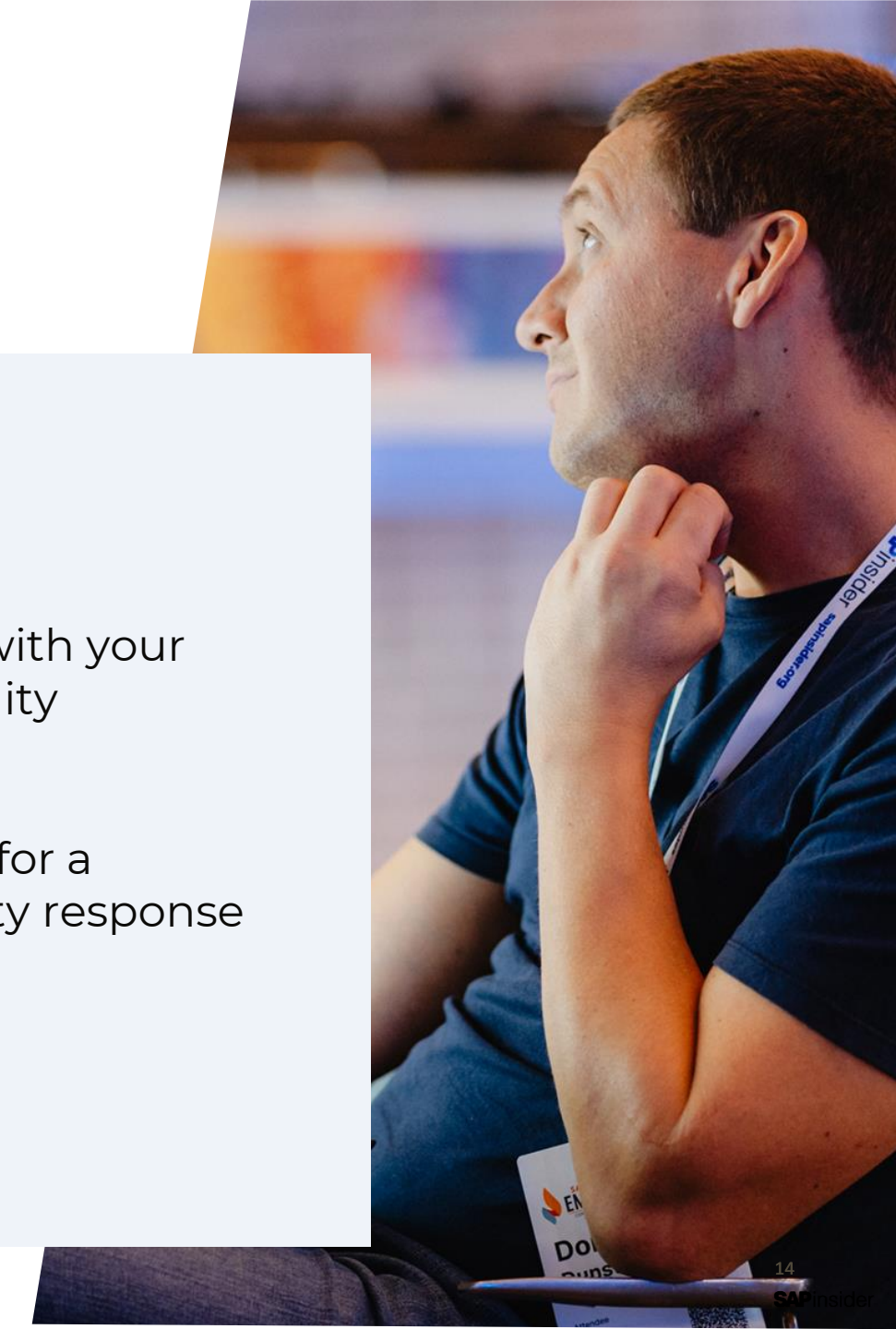
Bypass password



Leverage seamless integration elevating your SAP security posture

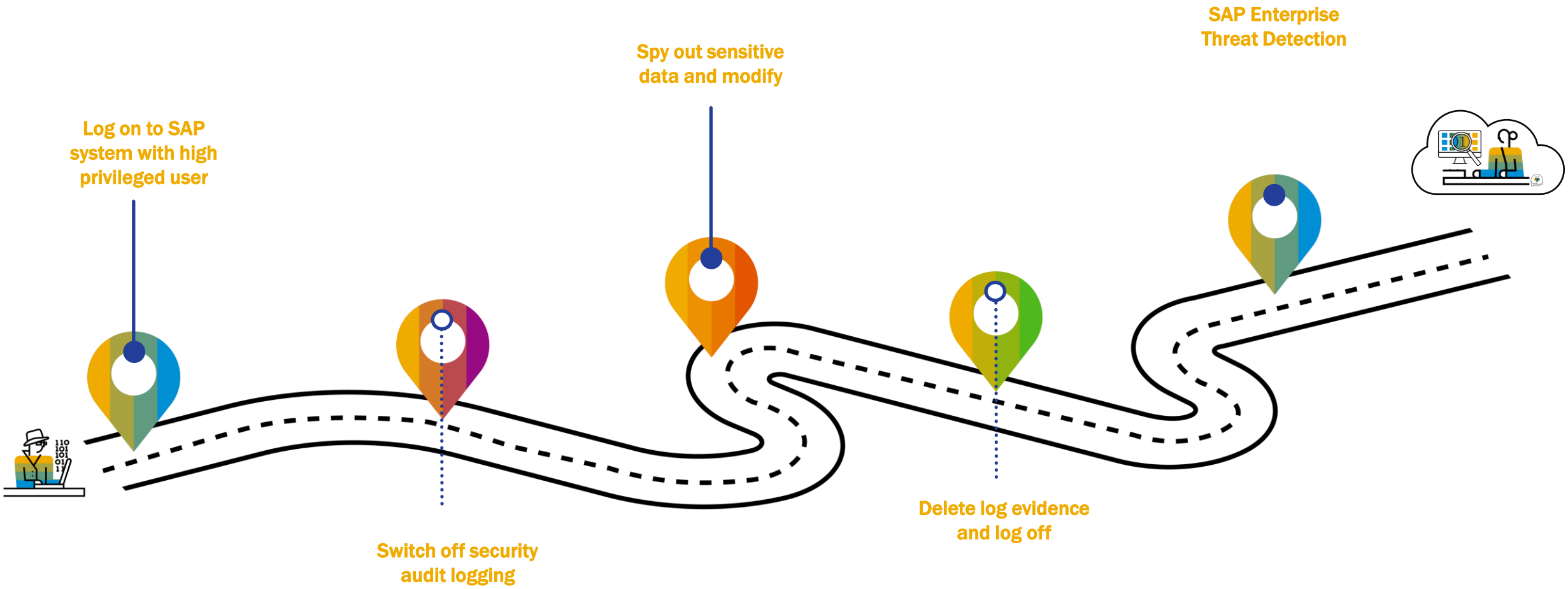
Elevate cybersecurity by integrating with your existing SIEM, enhancing threat visibility

Easily coordinate with SOAR systems for a streamlined and efficient cybersecurity response



Demo (1) – Video with SOAR response Walk-Through

Sensitive data spy out & manipulation

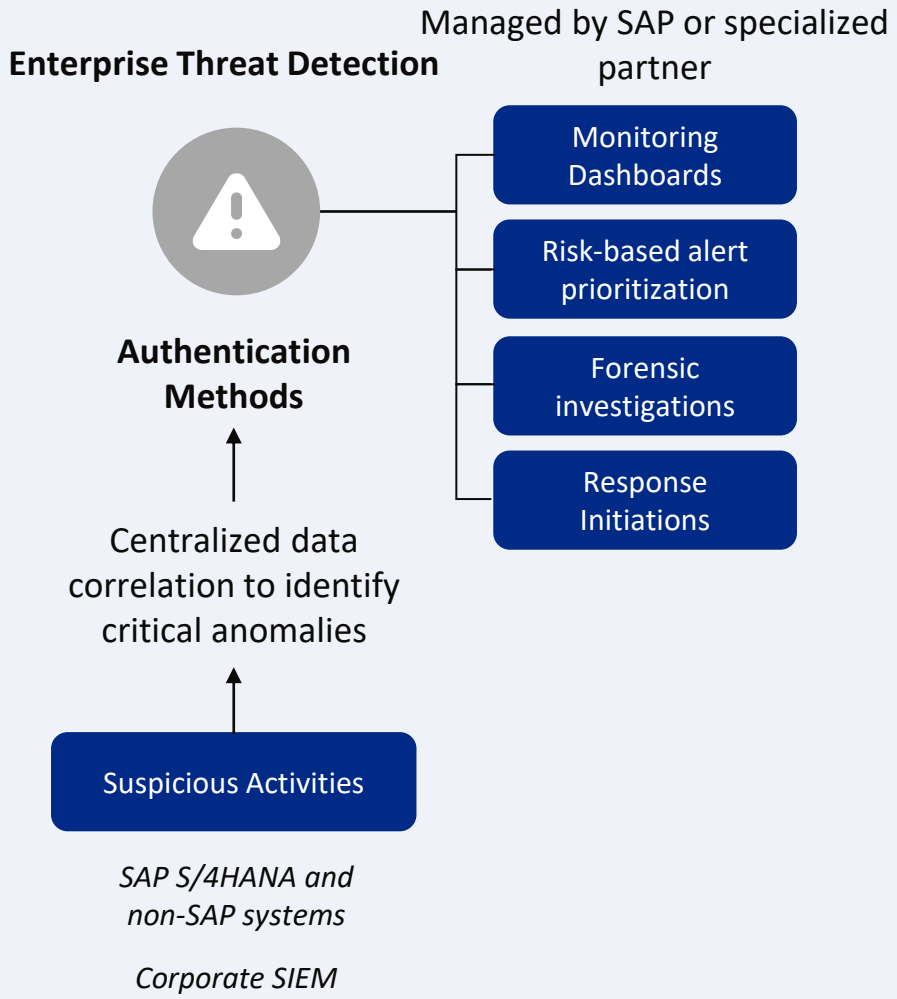


SAP Enterprise Threat Detection

Solution Capabilities

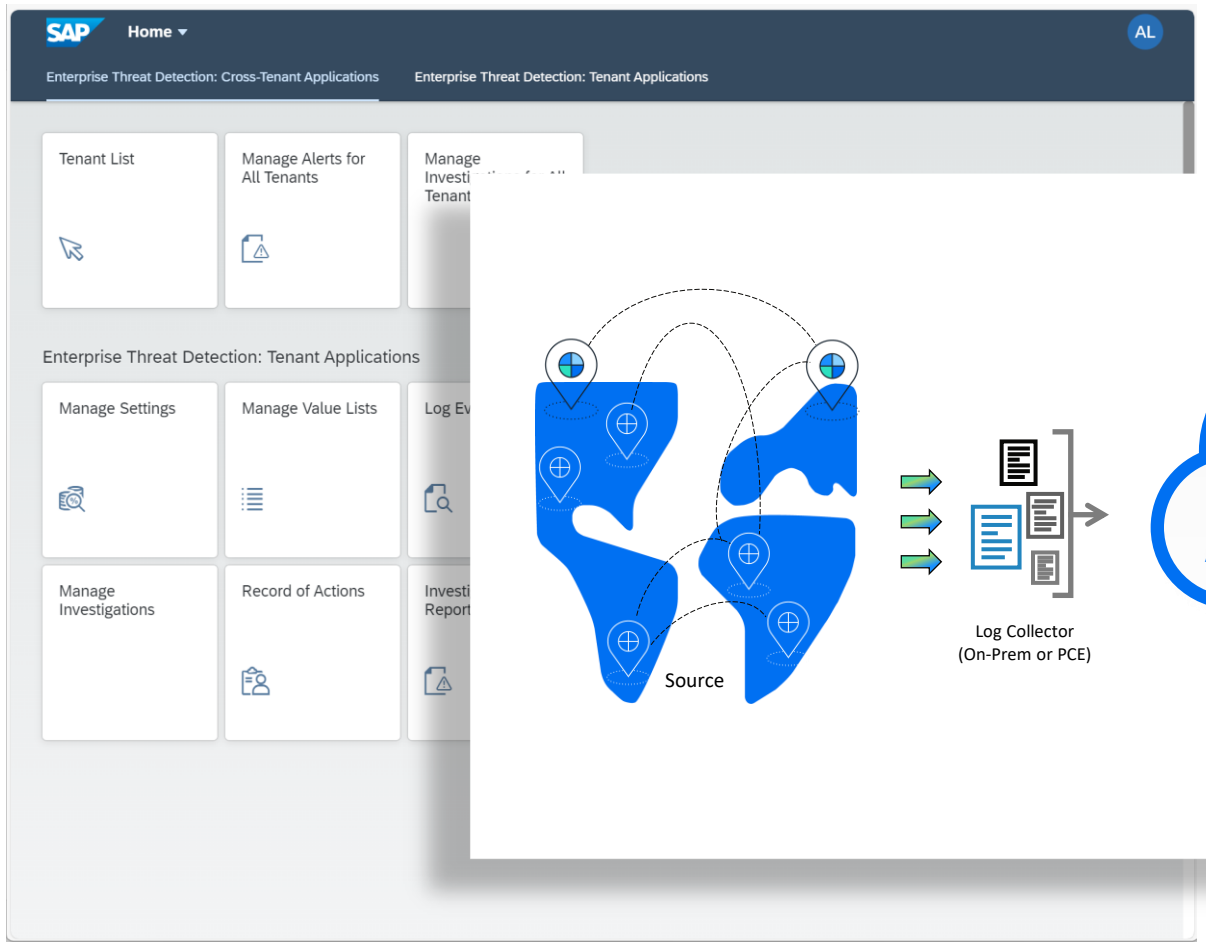
Managed service from either SAP or a specialized partner to help identify, analyze, and report malicious activities in your SAP applications before serious damage occurs.

- Analyze a vast quantity of log data and correlate information
  to get a complete picture of landscape activities.
- Detect threats at the application server level and at the database level.
- Find SAP software-specific threats related to known attacks by using attack detection patterns.
- Perform forensic threat detection to discover previously unknown attack variants.
- Create attack detection patterns without the need to code.
- Customize the integration of third-party systems and infrastructure components.



Cloud Managed SAP Security

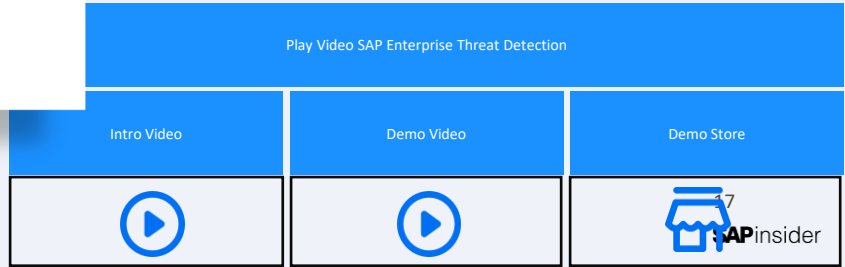
Continually track and report cross-system malicious activities.



Lowering cost of handling security

Adhere to legal mandates, such as Article 30 of the GDPR.

High-value alerts cut costs and log volume



Key Points to Take Home

- Monitoring SAP Applications is crucial for Security and Compliance
- Use Managed Security Services to help to detect threats
- SAP systems hold valuable data that is attractive to hackes

Where to Find more Information

- **SAP Enterprise Threat Detection**
  - Product Page
  - Community Page
  - Help Page
- **SAP Generative AI Cybersecurity Strategy**

Thank you! Any Questions?

Speaker Name

Arndt Lingscheid, SAP SE

Arndt Lingscheid | LinkedIn

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.