Securing SAP Systems Against the Ever-Growing SAP Malware and AI Threat

Arndt Lingscheid and Gabriele Fiata, SAP

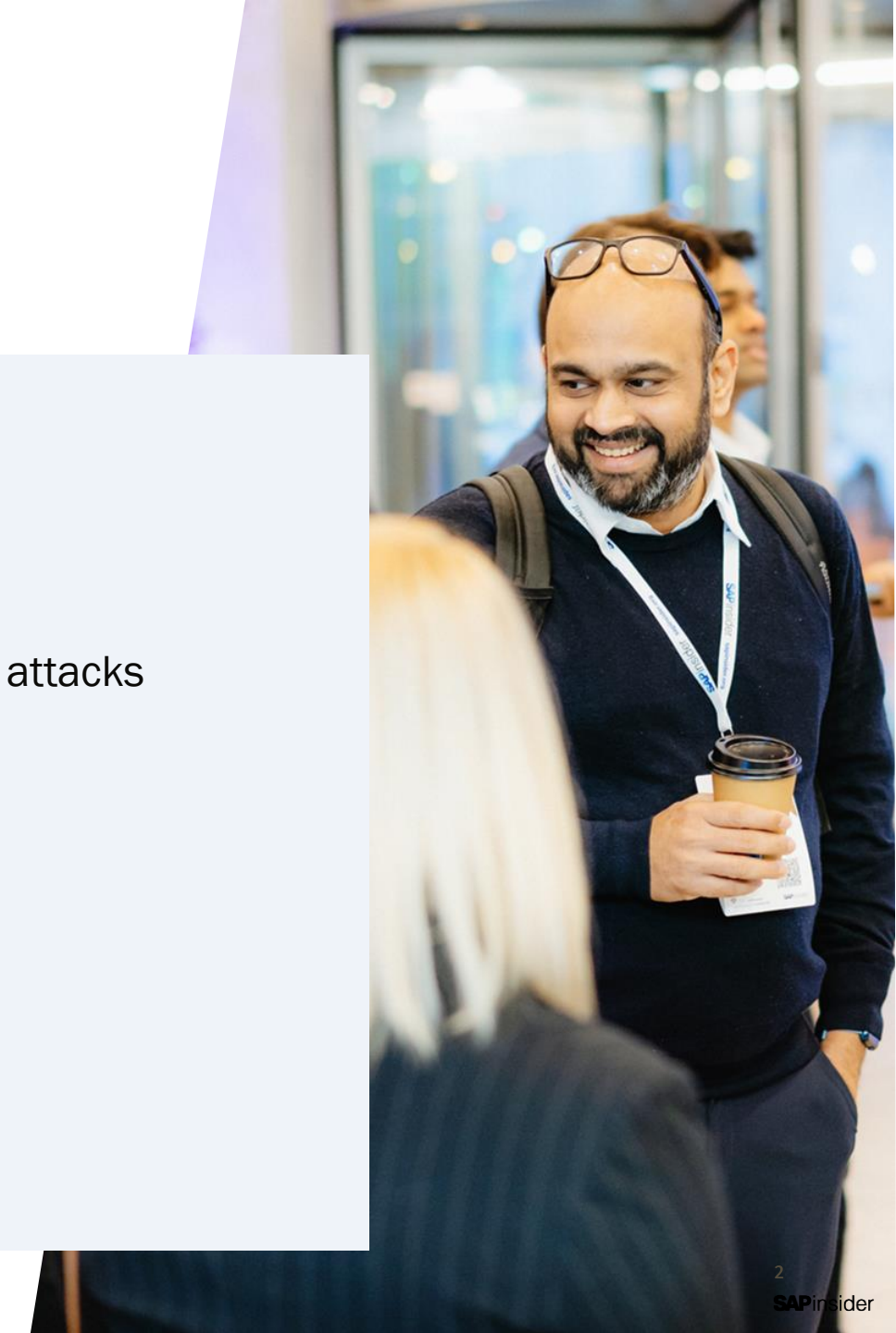
Las Vegas

2024

SAPinsider

What We'll Cover

- Once upon a time…
- Usage of AI (LLMs): Offense
- The raise of SAP Malware
- How to defend SAP systems from AI powered attacks
- Key Points to take home



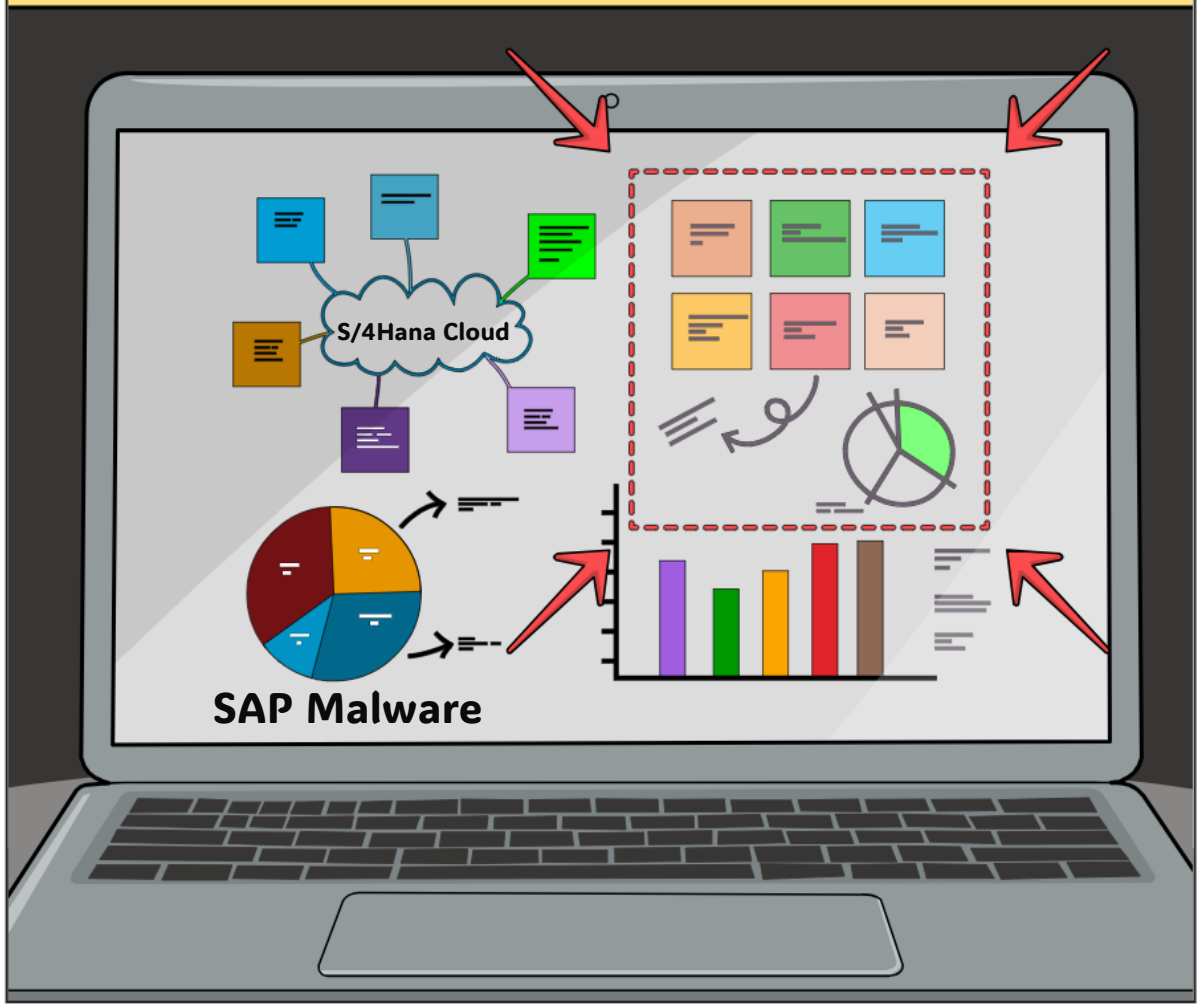
Once upon a time...

In a tech-driven metropolis, TechConnect, a global innovator, relies on SAP systems for efficient operations...

It begins innocuously enough, with an unsuspecting employee receiving an email purportedly from a trusted supplier...

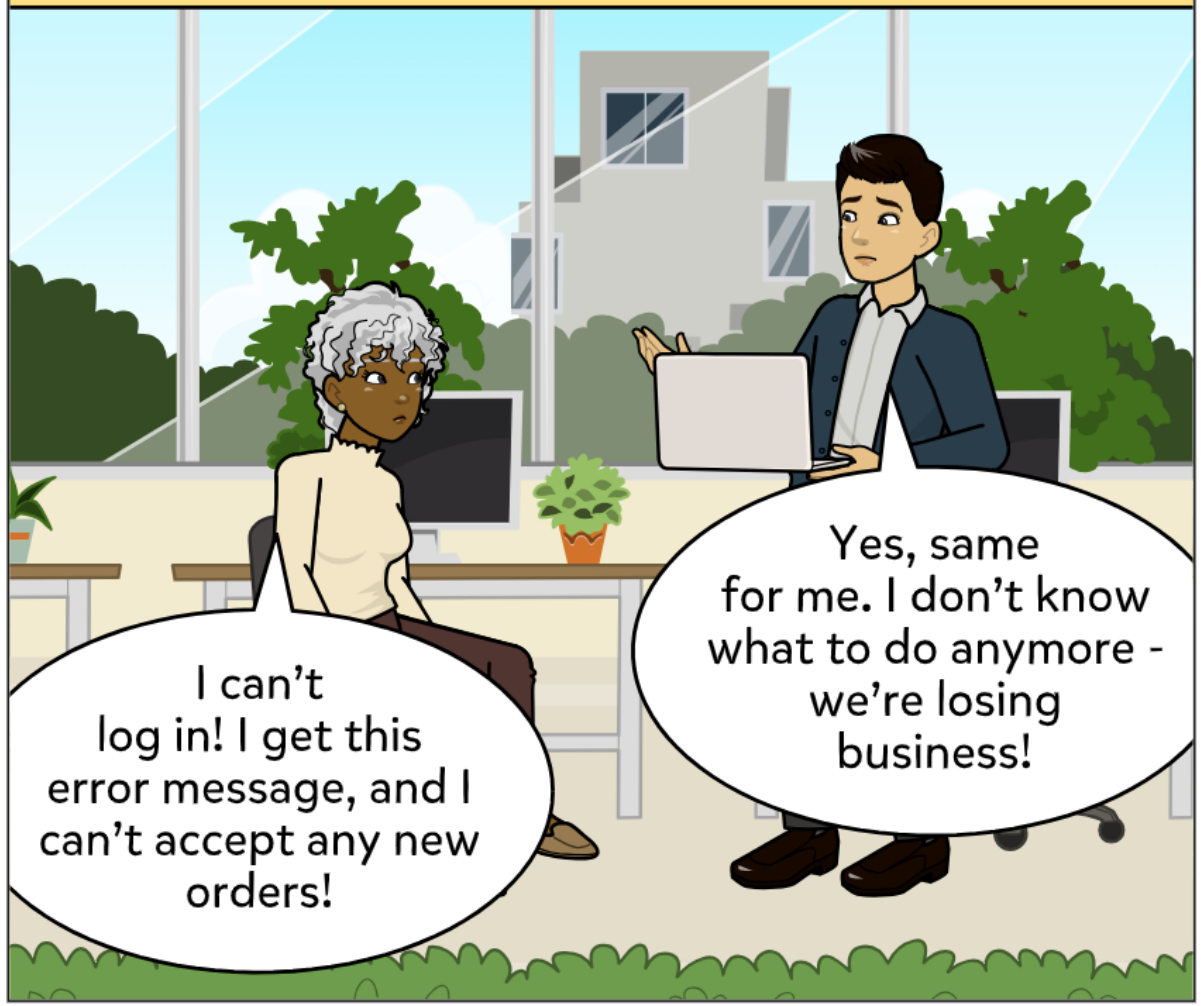
Unbeknownst to TechConnect, a silent intruder lurks in the shadows of cyberspace, patiently waiting to exploit vulnerabilities in its SAP infrastructure...

As the attachment opens, the AI swiftly manoeuvres through advanced algorithms, bypassing security to infiltrate TechConnect's SAP environment...



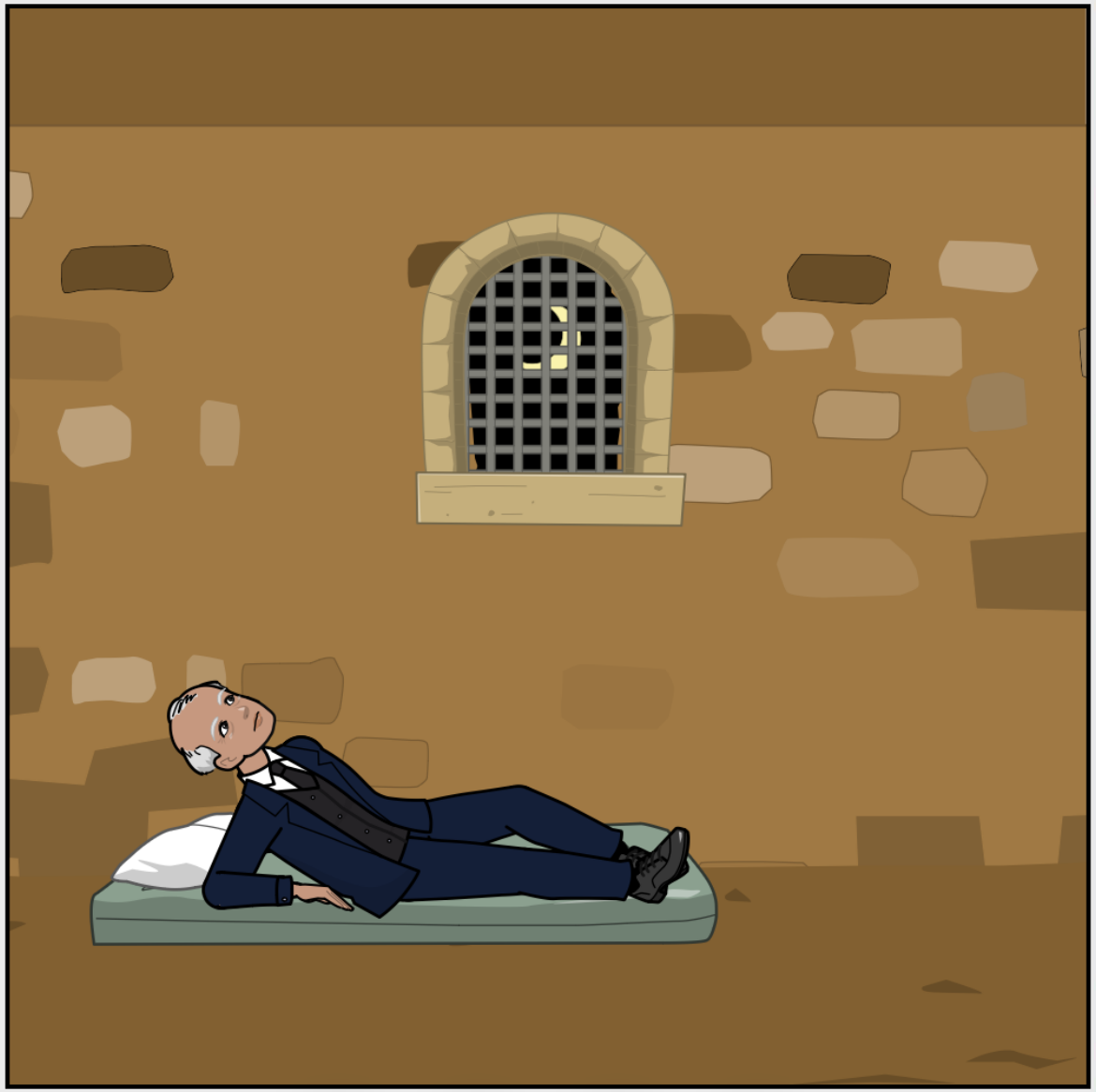
Days turn into weeks, and weeks into months, the AI clandestinely extracts valuable data with the precision of a digital thief in the night...

The attack shifts its focus to manipulating systems with denial-of-service attacks, rendering TechConnect employees unable to log in and perform their tasks.



...and finally, a hefty ransom demand emerges, holding TechConnect precious data hostage!

The company faces scrutiny from stakeholders, legal entities, and regulators...

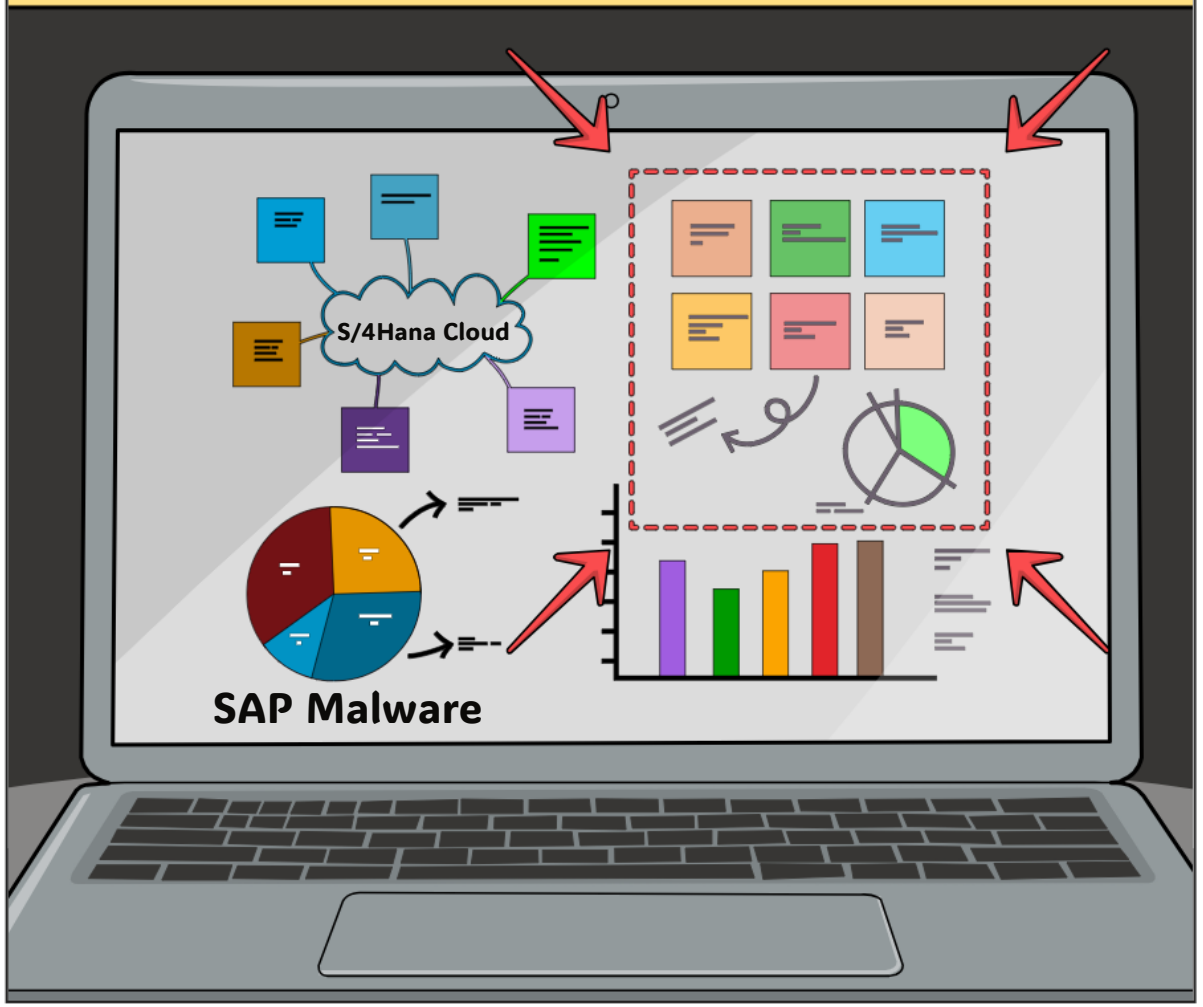



The End

...a better End...

Unbeknownst to TechConnect, a silent intruder lurks in the shadows of cyberspace, patiently waiting to exploit vulnerabilities in its SAP infrastructure...

As the attachment opens, the AI swiftly manoeuvres through advanced algorithms, bypassing security to infiltrate TechConnect's SAP environment...



It's not until TechConnect's astute cybersecurity analyst, stumbles upon unusual patterns in the SAP system...

The IT team launches a full-scale investigation, uncovering the chilling truth—their SAP systems have been compromised by an AI-powered adversary!

It is a race against time. TechConnect scrambles to battle an enemy unlike any it has faced before! After hours of chaos...

As the dust settles and TechConnect rebuilds, the cyberattack serves as a reminder of the constant threat from emerging technologies...

Usage of Artificial Intelligence

Offense

Usage of AI (LLMs): Offense

USING LLMs TO DEVELOP MALWARE

- Uncertain if LLM-based tools offer advantages over traditional hacking resources
- Potential risk: increase in attackers, decrease in effort needed to develop malicious tools
- Most LLMs trained on easily accessible public resources
- LLMs' generalization may not significantly enhance offensive capabilities

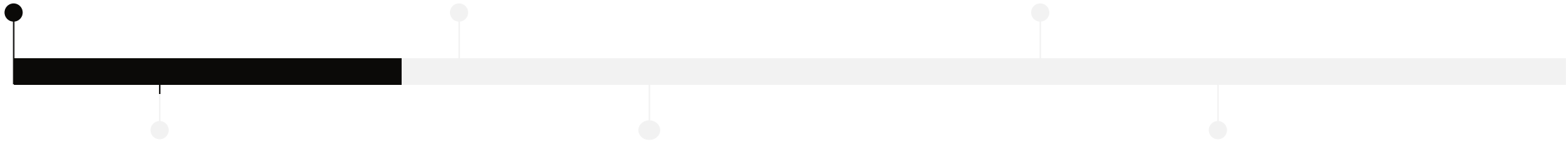
LLMs FOR SOCIAL ENGINEERING

- Scammers can enhance grammar, prose, and content randomization in phishing emails.
- LLMs streamlines spear phishing attacks, increasing their quantity, if not quality.
- With technologies like voice synthesis and text/image generators, LLMs can impersonate specific speech styles and voices, facilitating social engineering, vishing attacks and manipulation of targets.

AI and LLMs powered Attack Example

1. Social Engineering

AI algorithms on **social media** to identify **key individuals**.



2. PHISHING CAMPAIGN

AI-driven analysis to craft highly convincing **phishing emails and vishing calls**. Mimicking the writing, talking style and context of previous communications.

3. CREDENTIAL HARVESTING

Create **deceptive login pages** that imitate legitimate company's portals

4. AUTOMATED SOCIAL ENGINEERING

Generate automated responses to mimic the behavior of the compromised user, **engaging with other employees** to spread the attack.

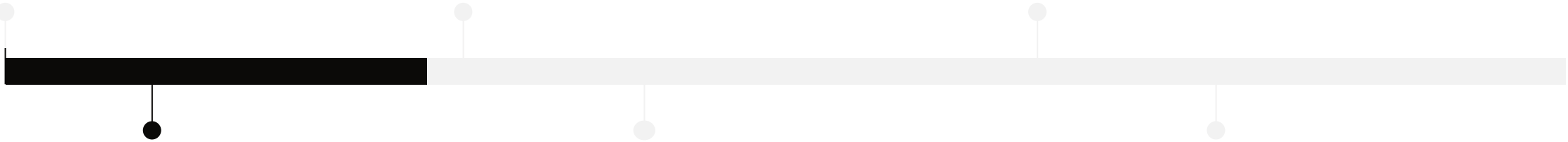
5. SYSTEM ACCESS AND DATA EXFILTRATION

Automate the identification of **critical systems, vulnerabilities, and sensitive data.**

6. EVASION TECHNIQUES

Bypass security monitoring measures, **dynamically change attack patterns** or mimic normal user behavior to **avoid detection.**

AI and LLMs powered Attack Example



2. PHISHING CAMPAIGN

AI-driven analysis to craft highly convincing **phishing emails and vishing calls**.

AI and LLMs powered Attack Example

3. CREDENTIAL HARVESTING

Create **deceptive login pages** that imitate legitimate company's portals

1. EXPLORATION

AI algorithms on **social media** to identify **key individuals**.

2. PHISHING CAMPAIGN

AI-driven analysis to craft highly convincing **phishing emails and vishing calls**. Mimicking the writing, talking style and context of previous communications.

4. AUTOMATED SOCIAL ENGINEERING

Generate automated responses to mimic the behavior of the compromised user, **engaging with other employees** to spread the attack.

5. SYSTEM ACCESS AND DATA EXFILTRATION

Automate the identification of **critical systems, vulnerabilities, and sensitive data.**

6. EVASION TECHNIQUES

Bypass security monitoring measures, **dynamically change attack patterns** or mimic normal user behavior to **avoid detection.**

AI and LLMs powered Attack Example

4. AUTOMATED SOCIAL ENGINEERING

Generate automated responses to mimic the behavior of the compromised user, **engaging with other employees** to spread the attack.

AI and LLMs powered Attack Example

5. SYSTEM ACCESS AND DATA EXFILTRATION

Automate the identification of **critical systems, vulnerabilities, and sensitive data.**

AI and LLMs powered Attack Example

1. EXPLORATION

AI algorithms on **social media** to identify **key individuals**.

2. PHISHING CAMPAIGN

AI-driven analysis to craft highly convincing **phishing emails and vishing calls**. Mimicking the writing, talking style and context of previous communications.

3. CREDENTIAL HARVESTING

Create **deceptive login pages** that imitate legitimate company's portals

4. AUTOMATED SOCIAL ENGINEERING

Generate automated responses to mimic the behavior of the compromised user, **engaging with other employees** to spread the attack.

5. SYSTEM ACCESS AND DATA EXFILTRATION

Automate the identification of **critical systems, vulnerabilities, and sensitive data.**

6. EVASION TECHNIQUES

Bypass security monitoring measures, **dynamically change attack patterns** or mimic normal user behavior to **avoid detection.**

The raise of SAP Malware

Types of malware attacks

Email Phishing

Software download

Visiting Compromised Websites

Clicking Malicious Links

Exploiting System Vulnerabilities

Removable Media

Malvertising

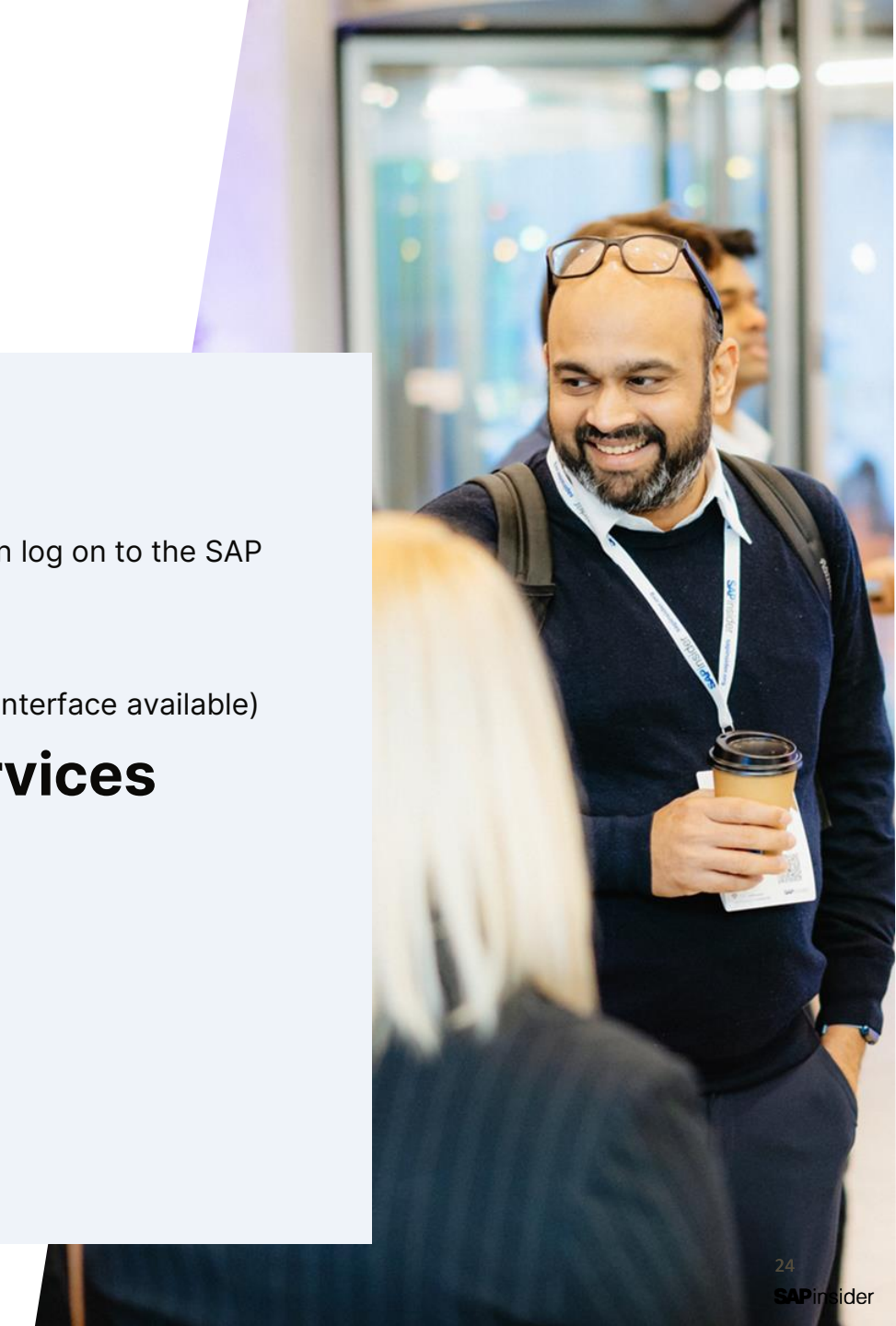
Software Bundling

Remember, the methods of attack are ever-evolving, and organizations must stay informed of the latest cybersecurity threats and ensure their systems are well defended.

Malware facts translated to SAP ABAP

Communication:

- **Lost and stolen credentials**
  Once the malware is in place on the end-user device the malware can log on to the SAP system
- **Upload of documents**
  Infected documents can be uploaded to the SAP system (virus scan interface available)
- **Usage of vulnerable API’s and services**



Malware facts translated to SAP ABAP

Direct coding manipulation:

- **Own customer development**
  (upload coding / code injection)
- **LSMW (Legacy Migration Workbench)**
  upload coding
- **Unpatched SAP applications / systems**
- **Trusted but blackmailed insider**
- **Compromized hosting platform**

Malware facts translated to SAP ABAP

SAP Transport requests:

- 3rd party vendors (verification of source and objects)
- External developers
- Own company ABAP software supply chain / (D,Q,P)
  - Files can be infected in the development system
  - Files can be infected (e.g. replacement) within transport directory

What can be the impact of a malware attack on the SAP system

- Ransomware:
Encryption of business data

- Sabotage:
Immediate shutdown/deletion of SAP systems

- Espionage:
Extraction of mission critical business data

- Destruction:
Slow destruction of business data over time

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.

How to defend SAP systems

from AI and SAP Malware powered attacks

SAP S/4HANA Source-to-Pay Process

What could go wrong

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

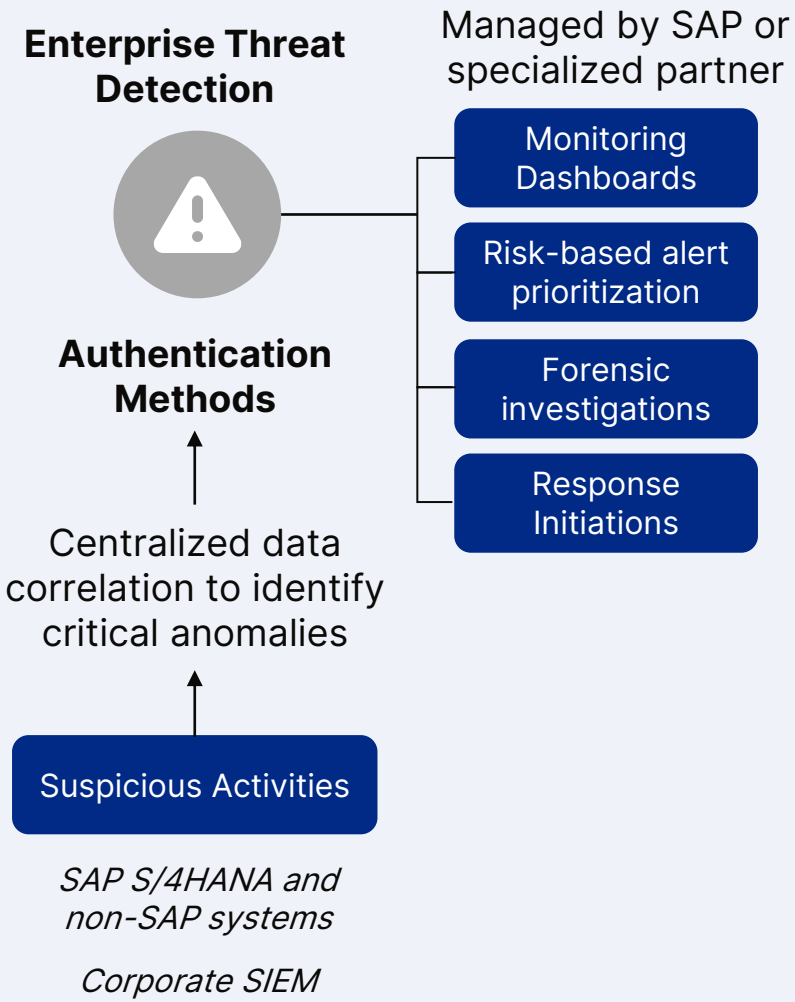
Economically analyze a vast quantity of log data and correlate information cross systems over long time to achieve transparency cross SAP business applications to maximize high value outputs and safeguard the applications.

SAP Enterprise Threat Detection

Solution Capabilities

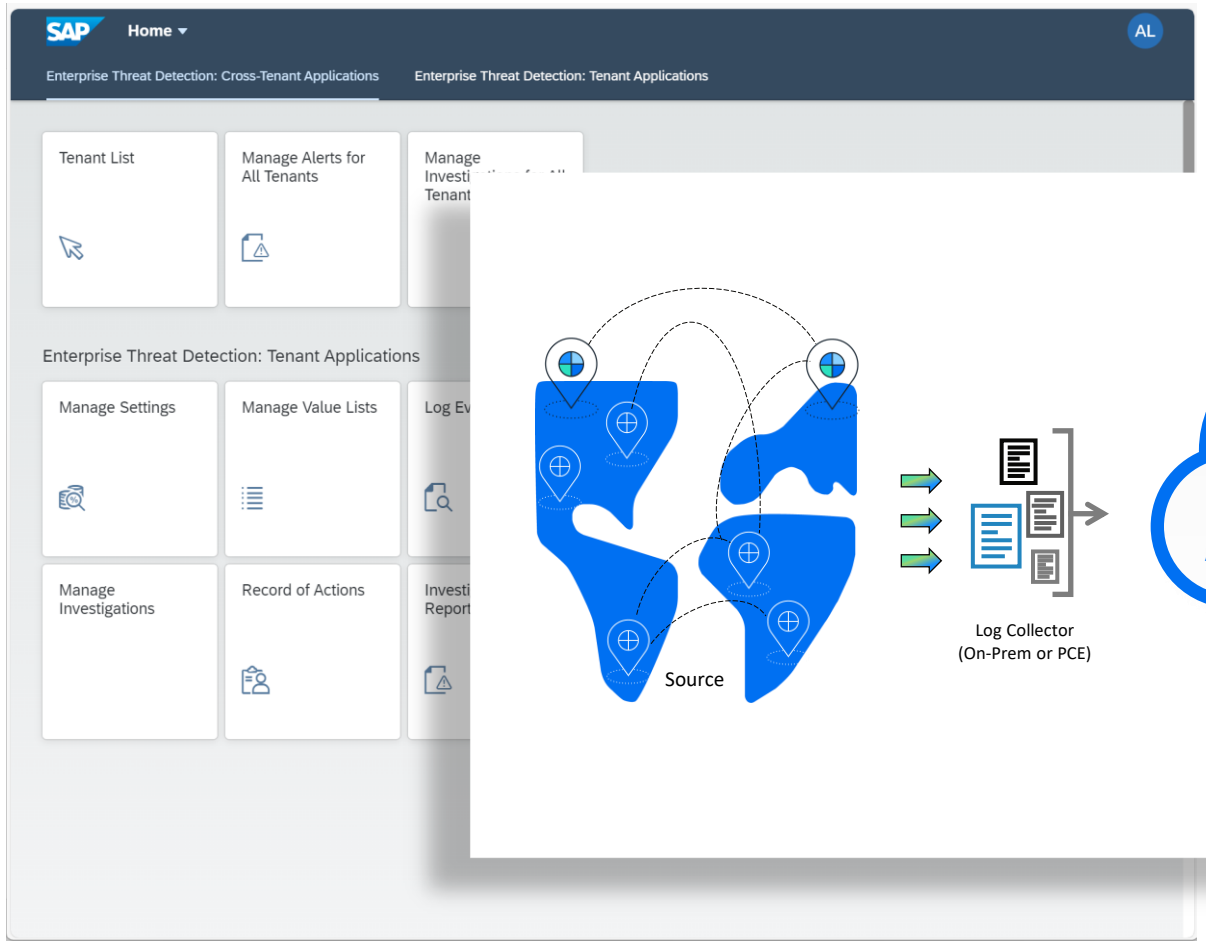
Managed service from either SAP or a specialized partner to help identify, analyze, and report malicious activities in your SAP applications before serious damage occurs.

- 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.



Cloud Managed SAP Security

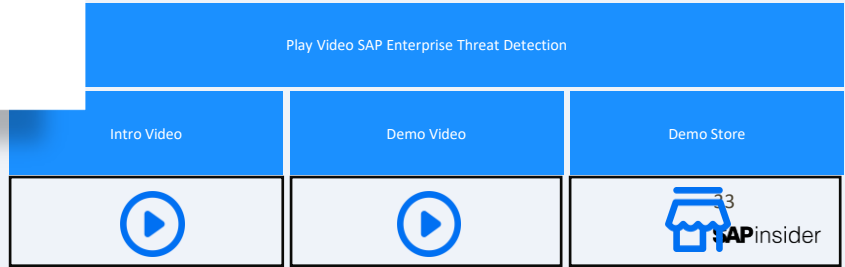
Continually track and report cross-system malicious activities.



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

- More attackers using LLMs, reducing effort for malicious tool creation.
- Additionally, with voice synthesis and text/image generators, attackers can mimic speech styles and voices, aiding in social engineering and vishing attacks.
- Cases of SAP Malware are raising
- Advanced threat detection technologies are required to identify the most sophisticated SAP Malware and AI powered attacks

Where to Find more Information

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

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2024 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

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