Discover What's New in SAP Cyber Security and Data Protection
Get Hands On with ETD - Quick Training on Enterprise Threat Detection

Kirthi Singh, SAP, Michael Schmitt, SAP, Arndt Lingscheid, SAP
November, 2023

SAP

Agenda

1st hour

Examples of real life security incidents

- Consequences of a hacker attack on SAP applications

- Zero Trust Aspects of Security Monitoring

- Attack Demo Scenario 1

- Attack Demo Scenario 2

2nd hour

- The flavors of SAP Enterprise Threat Detection

- Hands on Session

Examples of real life security incidents

Information about new products stored in SAP applications appeared in the internet before product launch.

New published SAP Security vulnerability was used two days after SAP's security patch day to access critical data.

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

Download of chemical compositions in the ERP test environment via developer rights. The employee left the company and started at a competitor.

Privileged user manipulated his/her salary.
Press published salary information and travel costs of a CEO.

What can be the consequences of a hacker attack on an SAP application?

Availability

Processes or systems are not available when needed by a user, the organization, or customer

- cannot create new contracts
- cannot process customer request
- process bill's
- change contracts
- cannot process new orders

Integrity

System itself can or has been modified

- modification of a system configuration
- modification of business documents & data
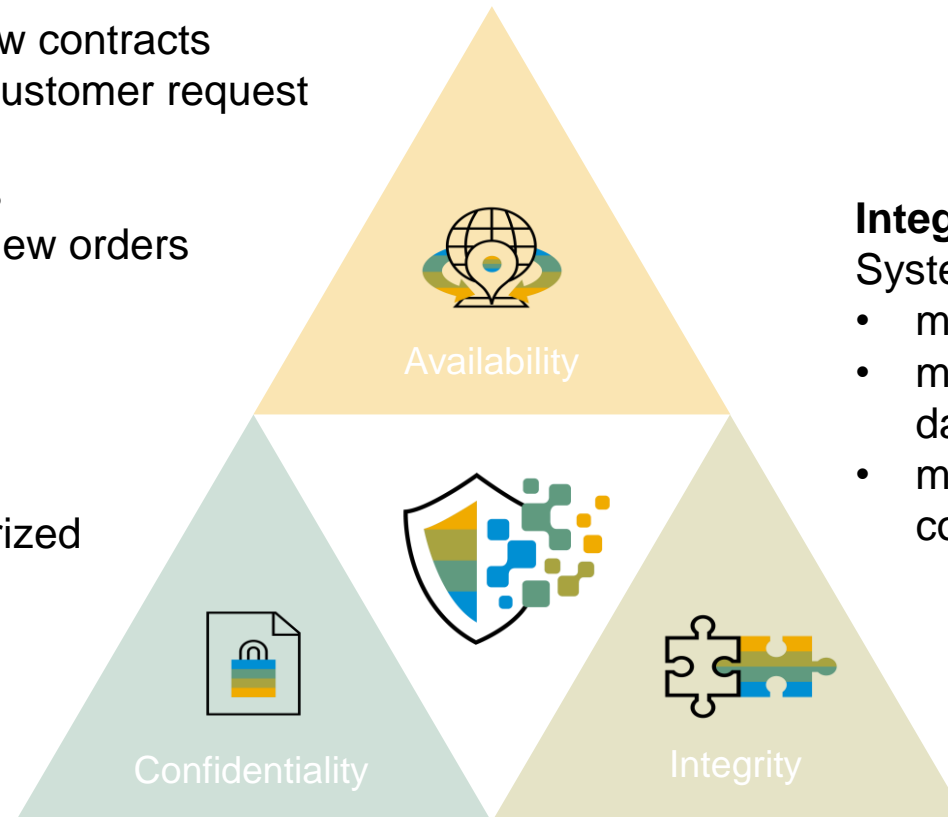- modification of business related configuration (e.g. tax information)

Confidentiality

Data has been disclosed to unauthorized individuals

- reputational damage
- financial loss (loss of business)
- legal action

Availability

Confidentiality

Integrity

Consequences of a hacker attack on SAP applications

Logistics
- Planning gets delayed
- Confidential partner and customers information ("ship to") can be lost
- Manipulation of delivery quantity and changes of recipients can occur

Sales and Distribution
- Customers are unable to make purchases
- Credit card, bank details, customer PII, pricing information can be lost
- Modification of business documents & data misstatement of the financial books

Controlling
- Business units unable to work, business processes can be interrupted
- Loss of pricing and revenue information
- Modification of business documents & data can lead to misstatement of the financial books

Finance and Treasury
- Financial data might not be available therefor decisions based on that information must be delayed
- Revenue information can be lost
- Modification of business documents & data can lead to misstatement of the financial books

Zero-Trust Principles

Eliminate Implicit Trust:

There should be no implicit trust based on physical location or device ownership. All user, device, network, application must be treated as "untrusted".

Verify all data flows/sessions:

All data flows or sessions must be authenticated and authorized with principle of least privilege. Access to resources must support dynamic security policies.

Limit the Blast Radius:

Design Micro-segment the network with software defined network perimeter. It is important to prevent threats moving laterally on the network by architecting and enforcing micro-segmentation with an associated security policies on each application layer and database layer.

Role Based and Context Aware Access:

Authorization to access resources must be provided in a secure and consistent manner with Role and Context based decisions. The policy engine should support creation of dynamic and statics policies.

The NIST Special Publication (SP) 800-207 Zero Trust Framework provides a comprehensive understanding on zero-trust principles.

Zero-Trust Principles

Least Privileged Access:

Only minimum access should be granted to users based on the concept of least-privileged access to every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Dynamic and Adaptive Policies:

The policy enforcement points, and policy decision points are key elements to zero trust principles. The control plane for Policy Enforcement must be centralized and support dynamic and adaptive reacting to changes to an environment.
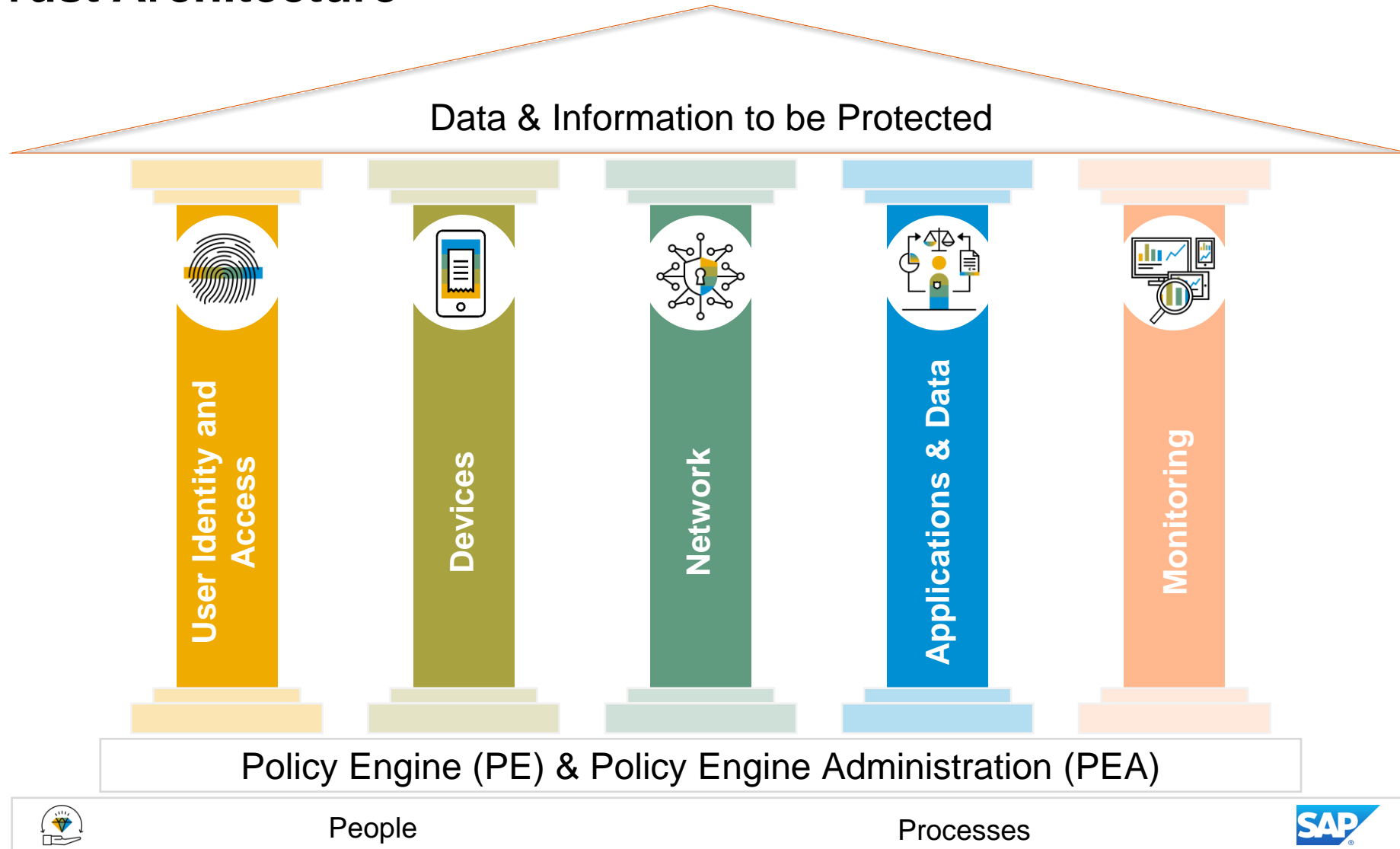
Data Protection:

Data must be protected with encryptions (both in transit and at rest), anonymization, tokenization, and various other obfuscation techniques.

Visibility and Control:

Continuous logging and monitoring. Log must be collected at all levels, inspected, and continuously monitored for all configuration changes, resource accesses, and network.

The NIST Special Publication (SP) 800-207 Zero Trust Framework provides a comprehensive understanding on zero-trust principles.

Zero-Trust Architecture

Data & Information to be Protected

User Identity and Access

Devices

Network

Applications & Data

Monitoring

Policy Engine (PE) & Policy Engine Administration (PEA)

People   Processes

Use case categories

Use of critical resource
    Execution of critical functions, reports and transactions
    Change, manipulation or spy out of business data
    Change or manipulation of critical configuration

User Manipulation
    Critical authorization assignment
    User role create, drop or manipulation
    Reference user assignment
    User morphing by changing type or probable identity theft
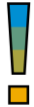
Debugging
    Debugging with change of control flow while debugging
    Debugging with change of variable values during debugging
    Debugging in critical systems
    Debugging in systems assigned to critical roles

System Access
    Failed logon with too many attempts
    Failed Logon with too many password logon attempts
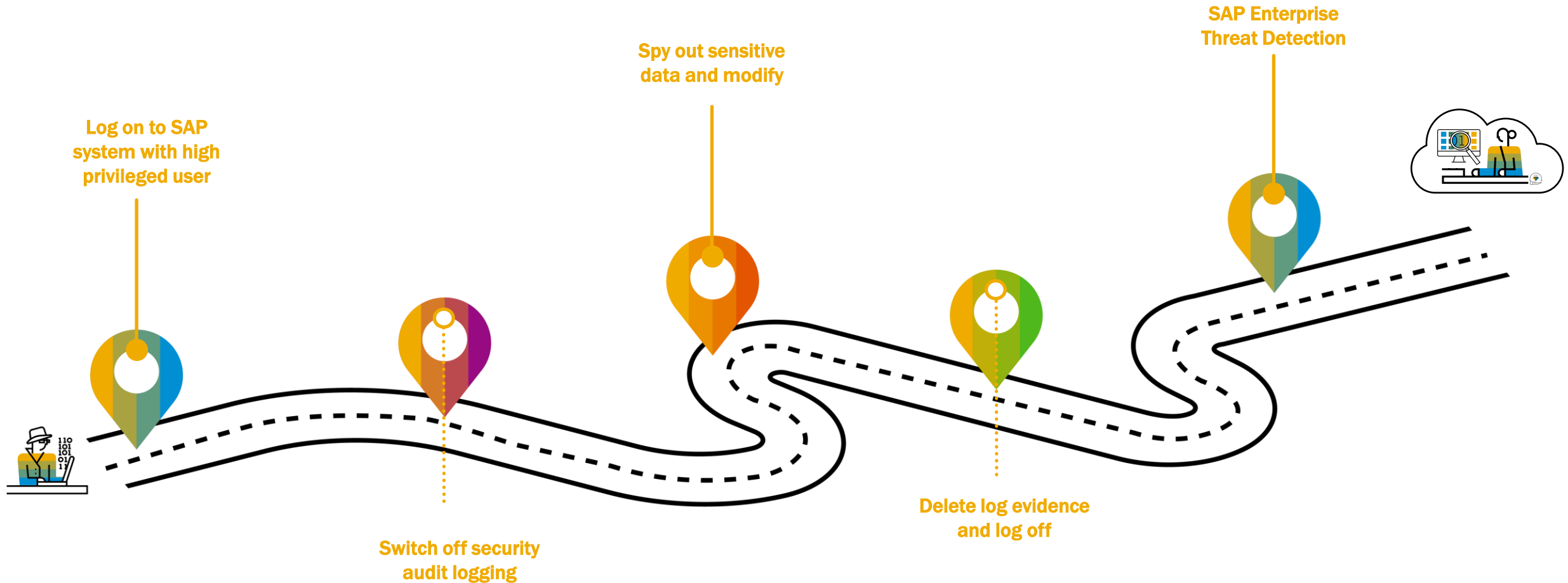   Logon with SAP standard users, or high privileged users
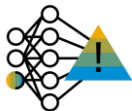
Suspicious Actions
    Dynamic program execution, download
    Dynamic code and system changes

Attack Scenario 1

Sensitive data spy out & manipulation

SAP Enterprise Threat Detection

Spy out sensitive data and modify

Log on to SAP system with high privileged user

Switch off security audit logging

Delete log evidence and log off

Attack Scenario 2

Create new user

Log on to SAP system with admin user

Check system availability (RFC_PING)

SAP Enterprise Threat Detection

Execute system function SE38

New user Malice2 created
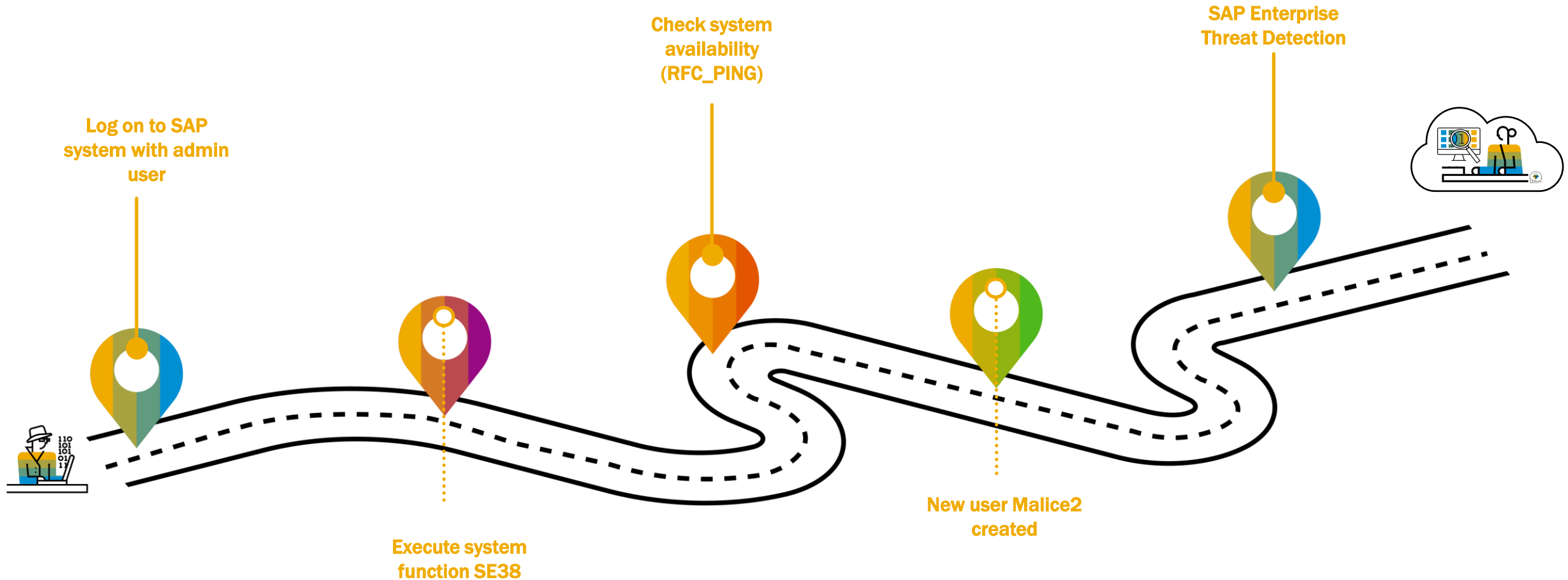
Coffee Break

SAP Enterprise Threat Detection

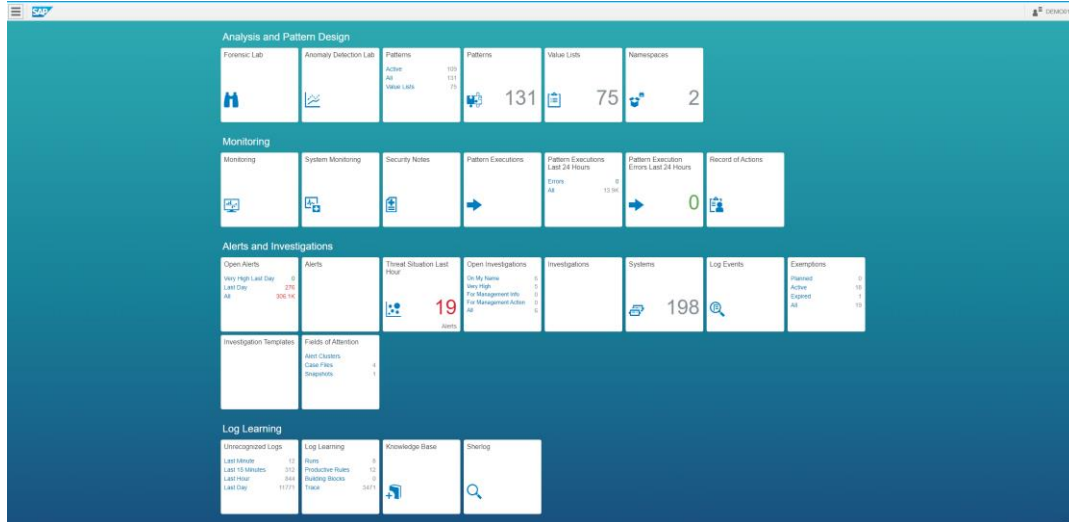### Definition

SAP Enterprise Threat Detection provides visibility into suspicious (user) events and anomalies in SAP business applications to detect and stop security breaches in real time.

Objective

Enterprise Threat Detection uses highly efficient and automated processes based on HANA technology and machine learning to track hacker activity using SAP's predefined and easy customizable attack paths.
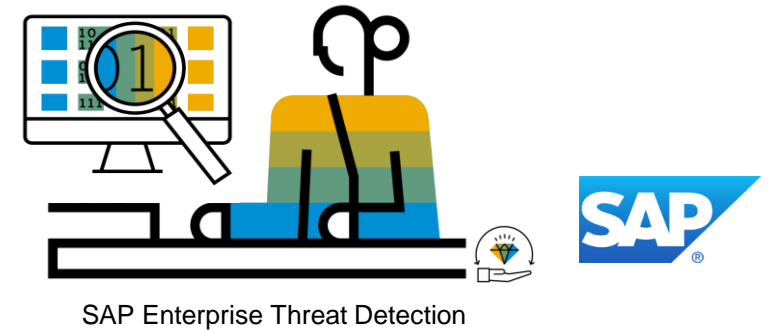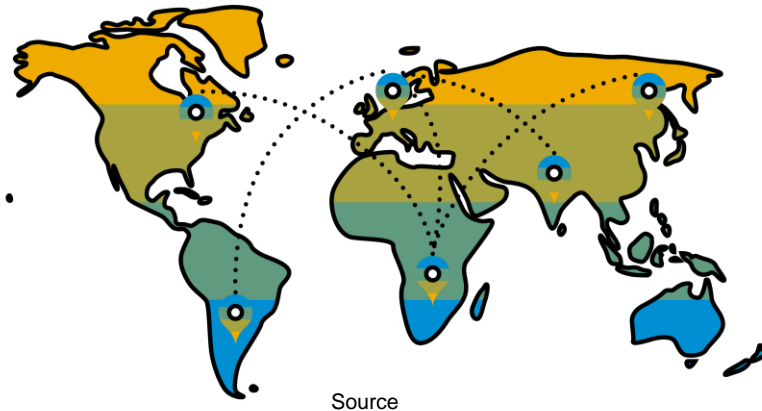
Content

- Ships with standard use cases
- Monthly content delivery
- Collecting and storing of audit relevant information

Customer Adoption

- More than 450 SAP customers worldwide in all industries

Protecting the crown jewels with SAP Enterprise Threat Detection

Source

SAP Enterprise Threat Detection

- ✓ System events and contextual data is send to SAP Enterprise Threat Detection.

- ✓ Data is efficiently enriched, normalized, pseudonymized, analyzed and correlated.

- ✓ Huge amounts of data can be processed.

- ✓ Integration of SAP and non-SAP log data.

- ✓ Automatically evaluate attack detection use cases with real-time alerting.

- ✓ Forensic analysis and modeling of existing and new attack detection use cases and dashboards.

Protecting the crown jewels with managed security service in the cloud
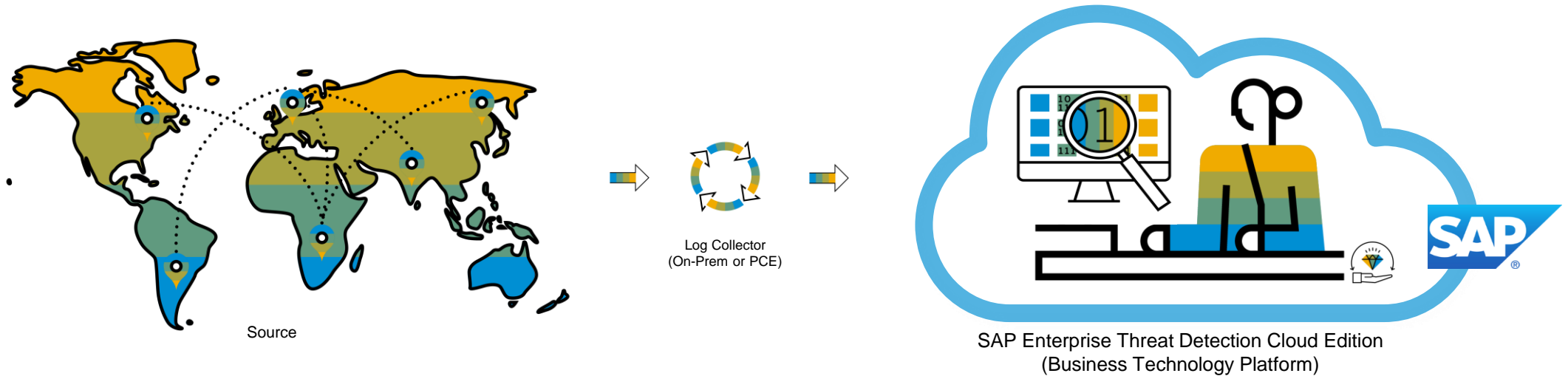
Source

Log Collector
(On-Prem or PCE)

SAP Enterprise Threat Detection Cloud Edition
(Business Technology Platform)

Basis service	• Cloud provisioning
	• Integrated managed security service
	• Ships with over 45 standard attack use cases
	• 24x7 alerting & 8x5 risk based & prioritized investigation of alerts
	• Monthly reporting of all incidents and all log data
	• Collecting and storing of audit relevant information
	• Integration to generic SIEM solution

* Europe available. USA and Australia planned. Further Data Centers on Demand

*** Planned in Q2 2023

Protecting the crown jewels with managed security service in the cloud

Source → Log Collector (On-Prem or PCE) → SAP Enterprise Threat Detection Cloud Edition (Business Technology Platform)

Extended service ***
- Committed response times
- Individual adapted security analysis
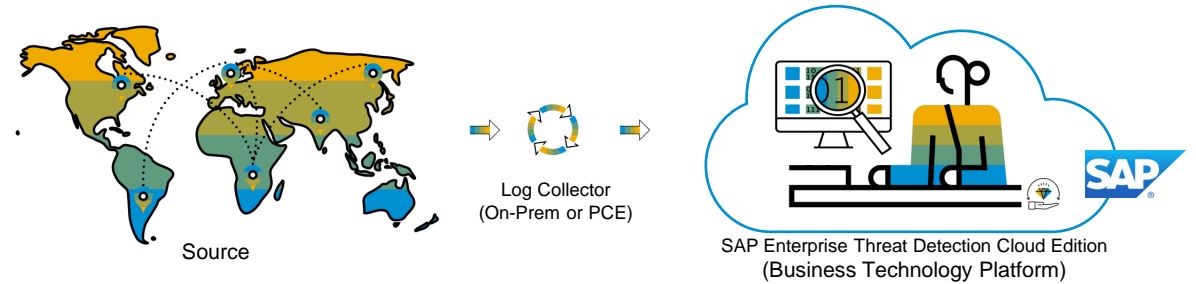- Customized service level agreements

Basis service
- Cloud provisioning
- Integrated managed security service
- Ships with over 45 standard attack use cases
- 24x7 alerting & 8x5 risk based & prioritized investigation of alerts
- Monthly reporting of all incidents and all log data
- Collecting and storing of audit relevant information
- Integration to generic SIEM solution

* Europe available. USA and Australia planned. Further Data Centers on Demand | *** Planned in Q2 2023

How SAP Enterprise Threat Detection integrates with generic SIEM and SOAR solutions

Collect analyze
Integrate
react

3rd Party SIEM

IT Infrastructure

SIEM Solution focuses on

Database
Operating System
Network

IT Infrastructure

SAP Enterprise Threat Detection

Application Layer

SAP ETD focuses on

SAP Applications
SAP Basis
SAP HANA Database

Application Layer

3rd Party SOAR

Application Layer & IT Infrastructure

SOAR

Automated response

Application Layer & IT Infrastructure

…and your SAP systems hold mission critical data which can be a blind spot for IT security teams

Hands-On Workshop: System Access Information

Infos for Hands-On Session
System 1 for Group 1

Systems

ETD Hands-on System 1: IP XXX3.76.244.90

- Welcome page: https://xxx3.76.244.90/7/6/ETDWelcome/index.html

- Exercises: https://xxx3.76.244.90/system-local/private/ETDWelcome/Exercises.pdf

- ETD System: https://xxx3.76.244.90/sap/secmon/ui

- Users: DEMO01, DEMO02, …DEMO20

- Passwords: Provided in Hands-On

PLEASE USE CHROME BROWSER.
If this should not work, please use Firefox Browser

Infos for Hands-On Sessions
System 2 for Group 2

Systems

ETD Hands-on System 1: IP xxx3.78.29.97

- Welcome page: https://xxx3.78.29.97/system-local/private/ETDWelcome/index.html

- Exercises: https://xxx3.78.29.97/system-local/private/ETDWelcome/Exercises.pdf

- ETD System: https://xxx3.78.29.97/sap/secmon/ui

- Users: DEMO01, DEMO02, …DEMO20

- Passwords: Provided in Hands-On

PLEASE USE CHROME BROWSER.
If this should not work, please use Firefox Browser

Thank you.

Contact information:

SAP