



# SAP Enterprise Threat Detection **cloud edition**

## The cloud-based managed cyber security service

Arndt Lingscheid, SAP  
Q1, 2023

Public

# Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

# Challenges concerning SAP Security Management

# Cyber-attacks are increasing dramatically

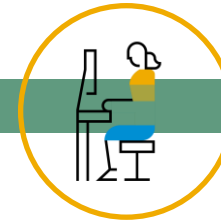
**38%** participants in the Ponemon study say the level of **application security** risk is high, but only **17%** of the data protection and security budget is allocated to application security!

In contrast, only **20%** rate network risk as high, but **38% of the budget is designated for network security.**

Over **80%** of breaches within Hacking involved brute force or the use of lost and stolen credentials.

The data breach lifecycle of a malicious or criminal attack in 2020 took an **average of 315 days.**

The average data breach costs in 2021 is **\$4.24 million**, a **10%** rise from 2020.



***...protecting SAP applications organizations have to go beyond perimeter security***

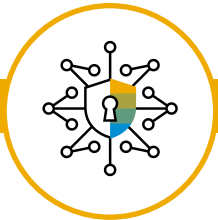
# Cyber-attacks are increasing dramatically



There are **3.5 million** unfilled cyber security jobs worldwide.



**Automation** is identified as a key factor to reduce cyber risks.



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

# 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

## Confidentiality

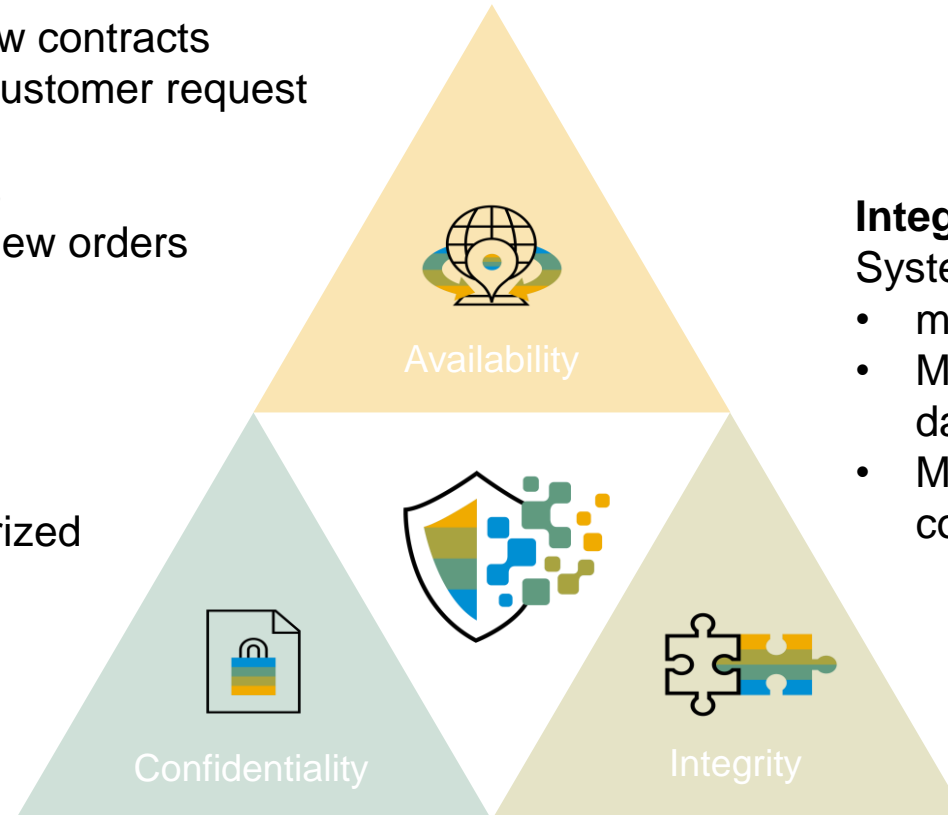
Data has been disclosed to unauthorized individuals

- Reputational damage
- Financial loss (loss of business)
- Legal action

## 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)



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

## 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 therefore 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



# 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.



# **SAP Enterprise Threat Detection** **cloud edition**

# SAP Enterprise Threat Detection

## cloud edition



### Definition

SAP Enterprise Threat Detection gives **transparency into suspicious (user) behavior and anomalies in SAP business applications** to identify and stop security breaches in real-time.



### Objective

SAP 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.



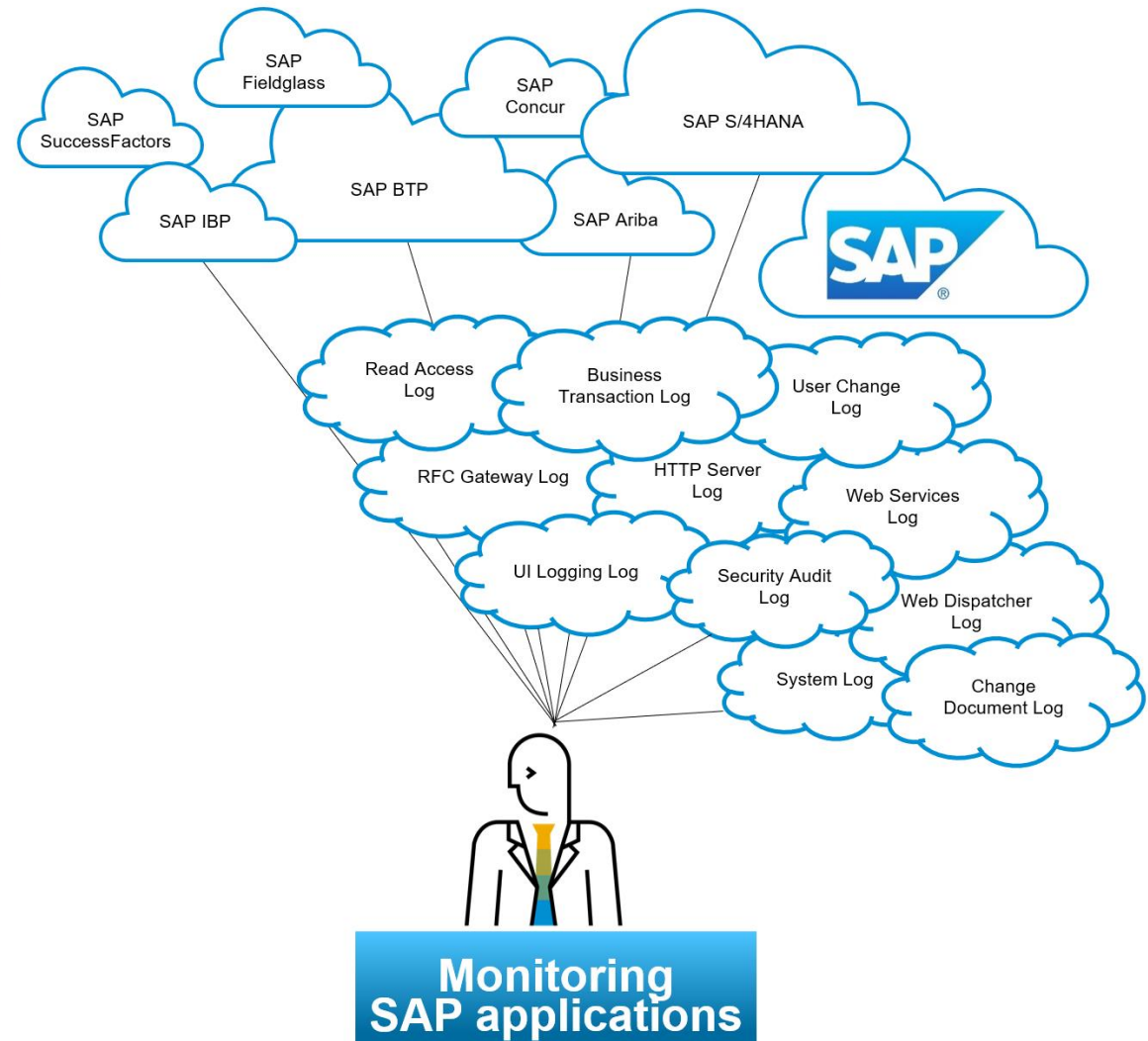
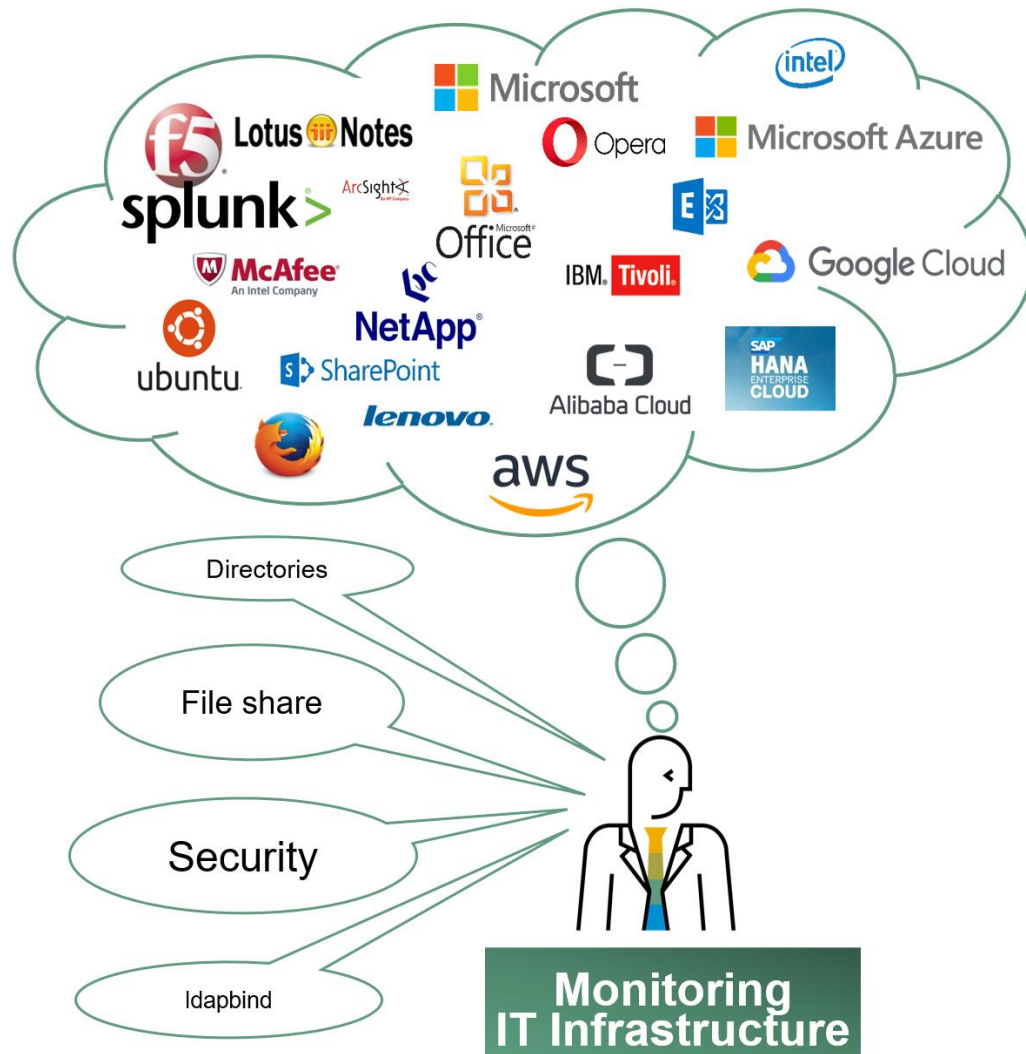
### What's in

- 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

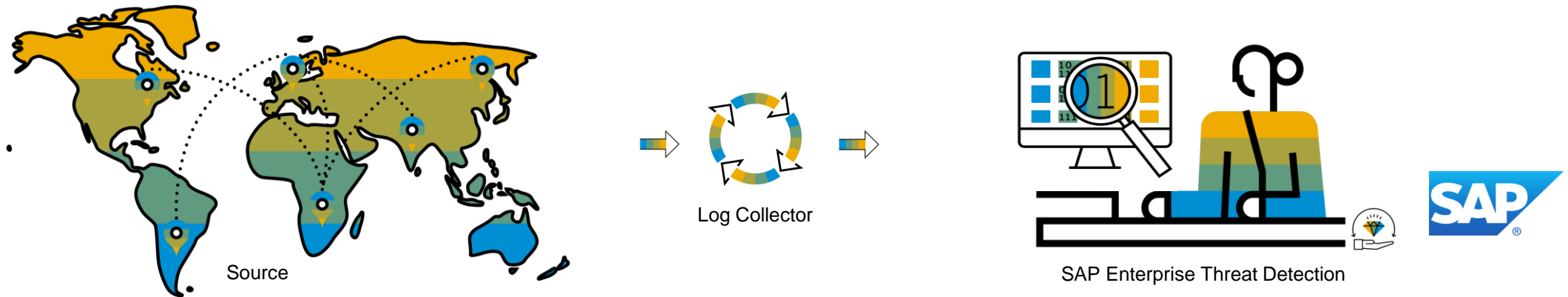
The screenshot shows the SAP Investigation Reports interface. At the top, there's a header with the SAP logo and 'Investigation Reports'. Below that, there's a sub-header 'Tenant SmartInvest'. The main area has tabs for 'Investigation Reports' and 'Monthly Reports'. There are search filters for Severity, Description, and ID. A table below shows three investigation reports.

Severity	ID	Creation Date	Description	Customer Notification
<input type="checkbox"/> High	443	02/02/2022 12:28:03 AM GMT+01:00	Potential User Account Miss-Use	No
<input type="checkbox"/> Low	400	02/02/2022 03:15:13 PM GMT+01:00	Debugging in Prod Systems	No
<input type="checkbox"/> Medium	417	02/02/2022 04:18:03 PM GMT+01:00	Critical Function call	No

# Why customers prefer SAP Enterprise Threat Detection over a generic SIEM

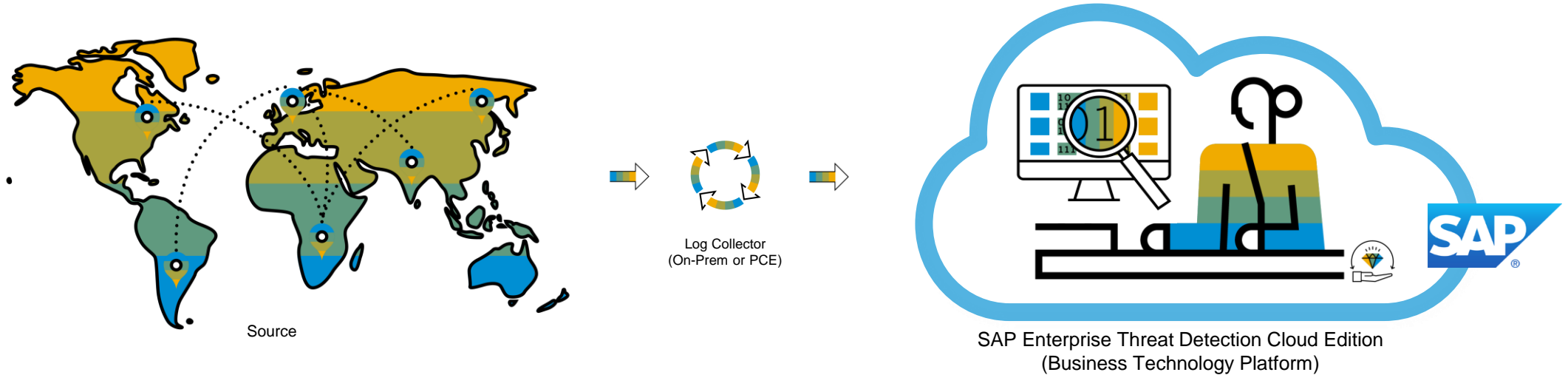


# Protecting the crown jewels with SAP Enterprise Threat Detection



- ✓ System events and contextual data are sent 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



## Basis service

- Cloud provisioning
- Integrated managed security service
- Ships with over 45 standard attack use cases
- 24x7 alerting & 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

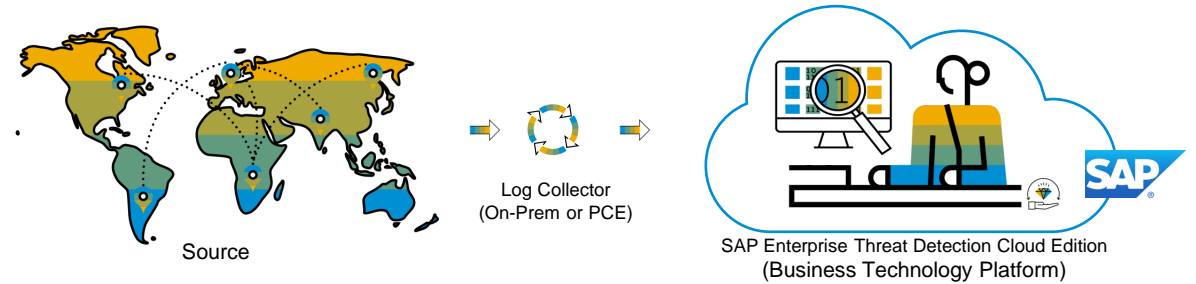


Different datacenters\*

Local Service provision\*

Language: English

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



## 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 & 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

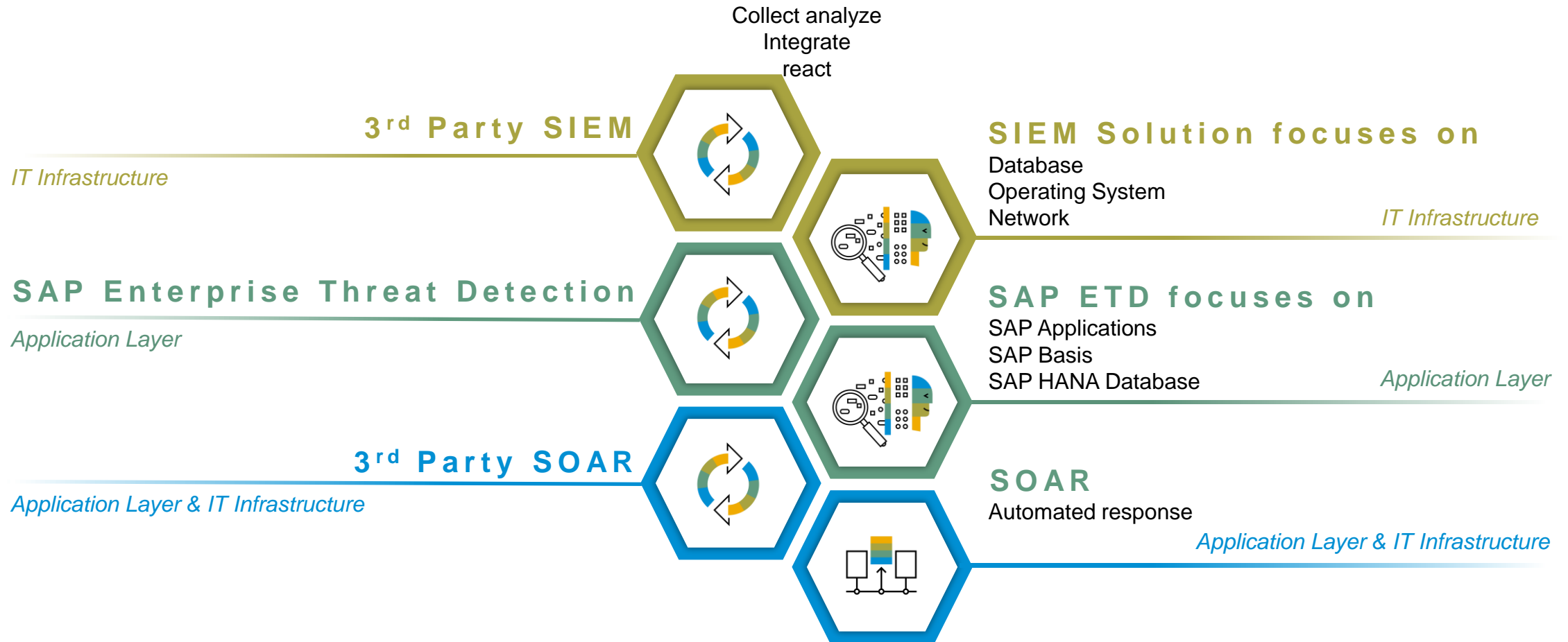


Different datacenters\*

Local Service provision\*

Language: English

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



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



# 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



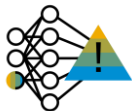
## Debugging

- 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

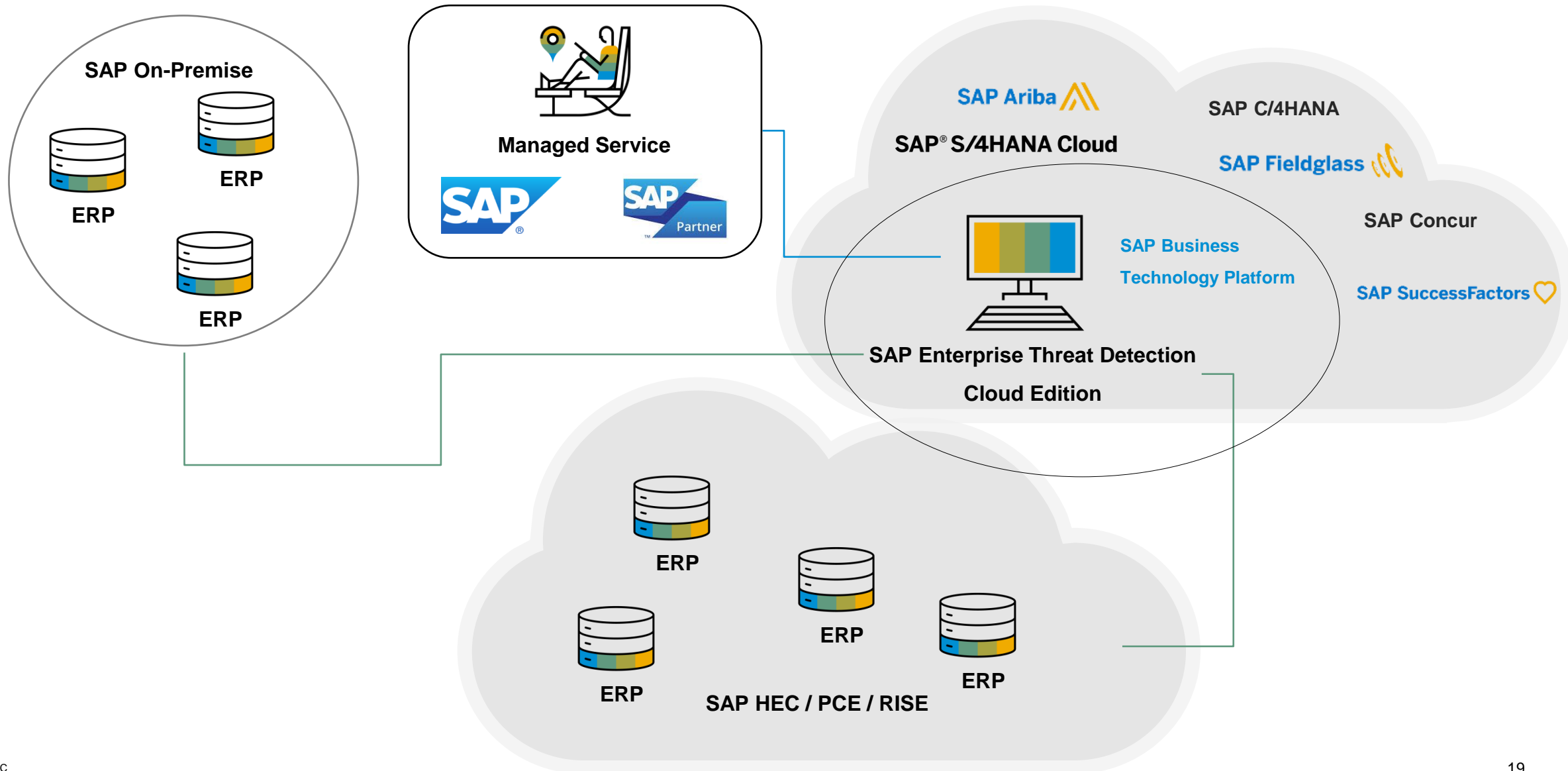
- Dynamic program execution, download
- Dynamic code and system changes

# Benefits

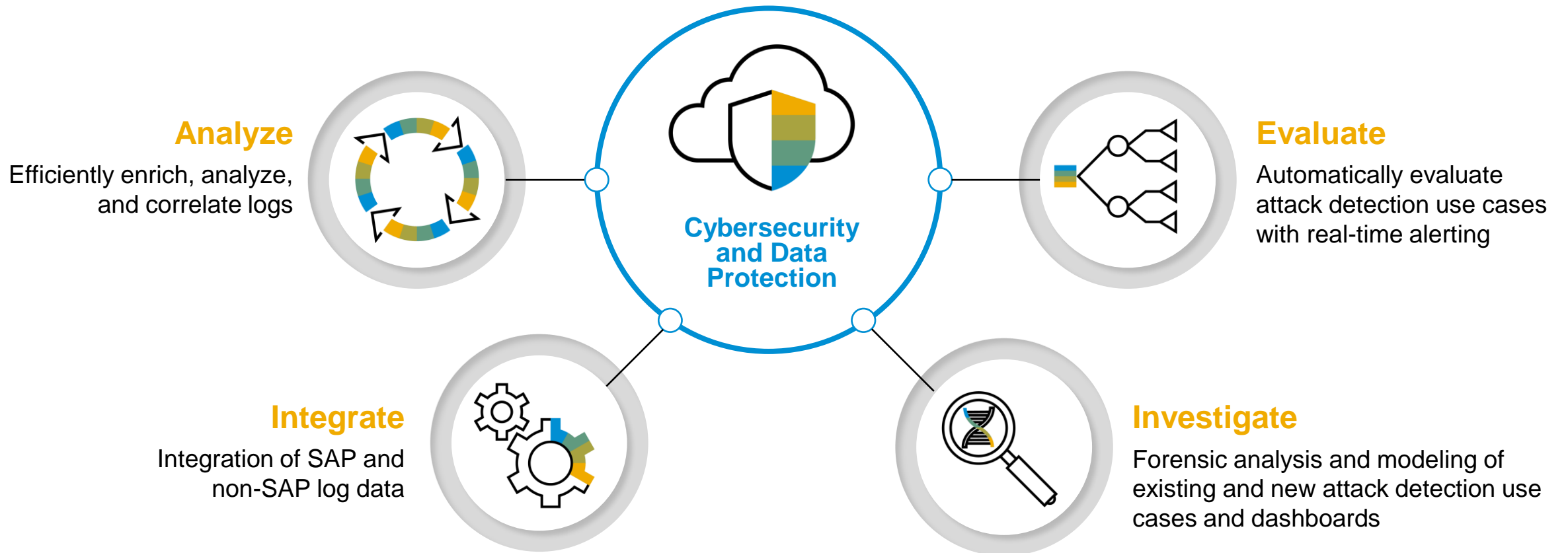
- Security professionals take over so you can **concentrate on your business.**
- **Help safeguard** the operation of your SAP applications and improve the continuity of your business.
- **Improve Threat Detection** with the support of security professionals to help minimize financial & IP loss as well as legal and reputational damage.
- **Sleep better.**

# **SAP Enterprise Threat Detection** **cloud edition – Setup**

# SAP Enterprise Threat Detection - Cloud Edition

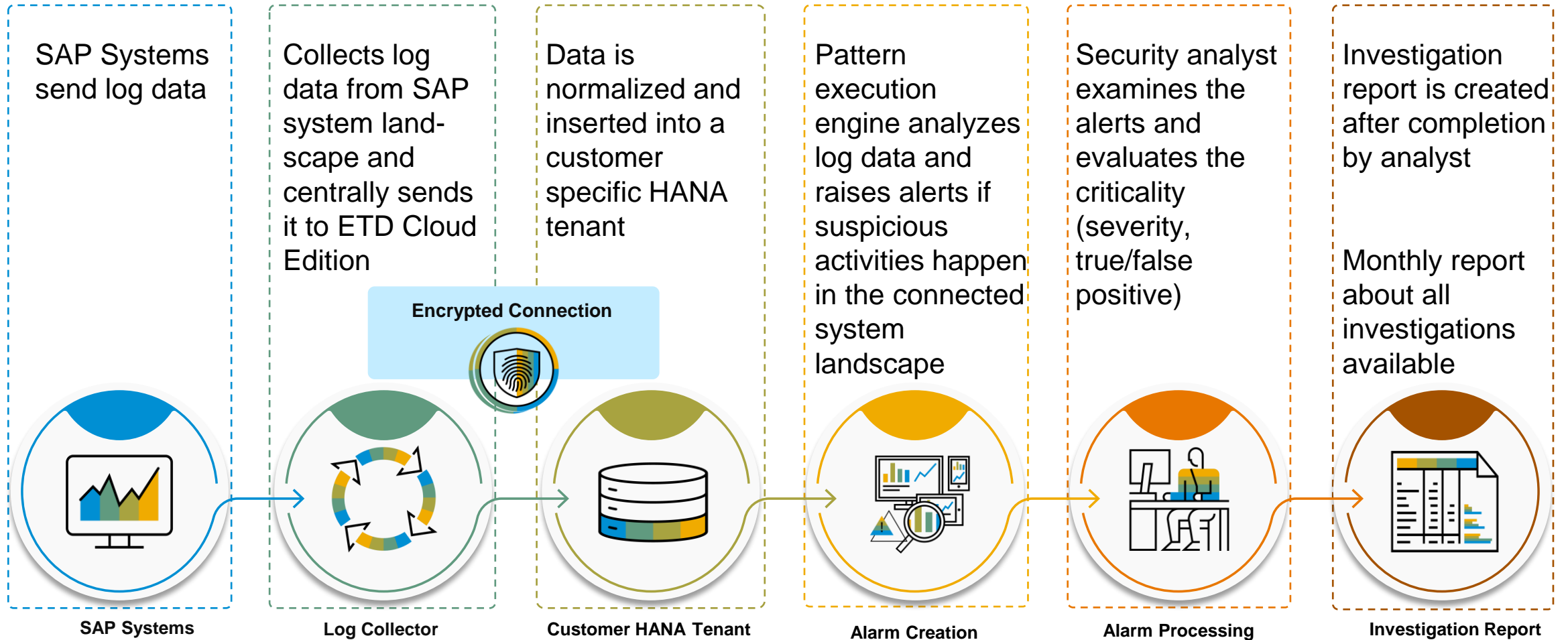


# How does SAP Enterprise Threat Detection work



# **SAP Enterprise Threat Detection** **cloud edition – Workflow**

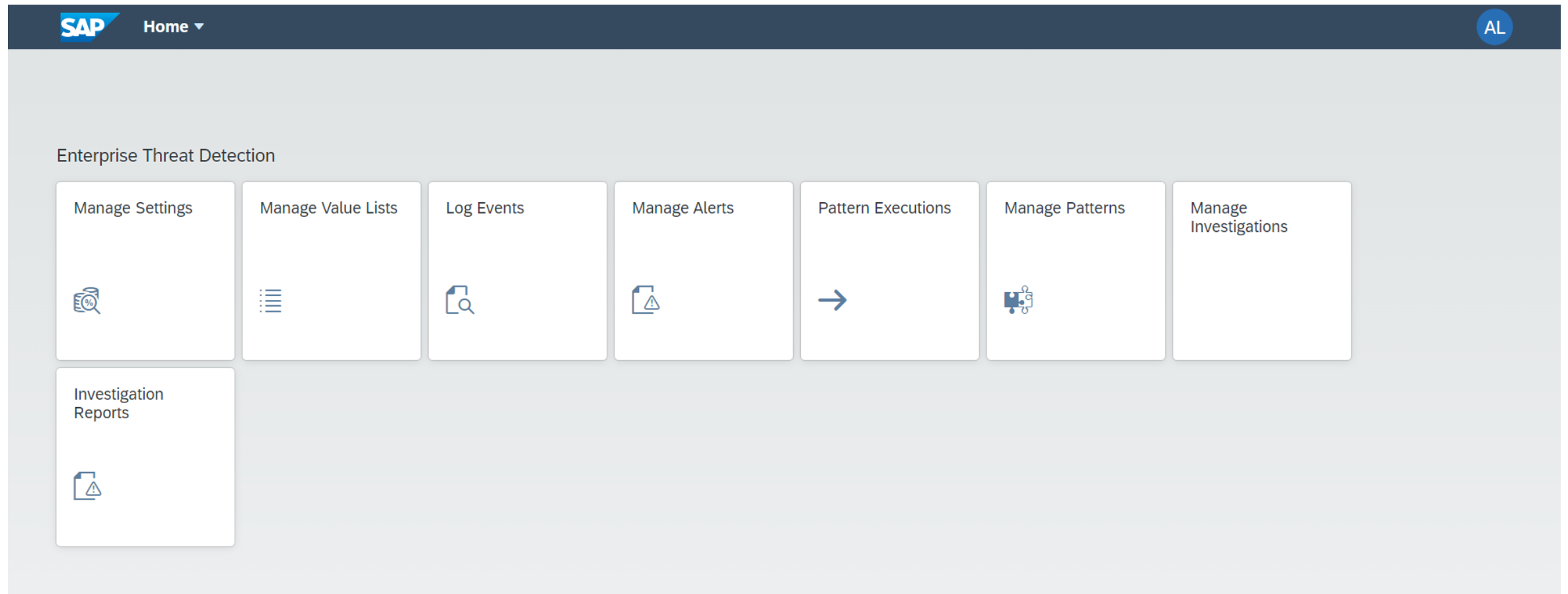
# SAP Enterprise Threat Detection cloud edition Workflow





# **SAP Enterprise Threat Detection** **cloud edition – Demo**

# Demo



# Demo

## Investigation Reports



Tenant SmartInvest

Investigation Reports

Monthly Reports

Go

Hide Filter Bar

Filters

Severity:

Description:

ID:



Investigation Reports

	Severiity	ID	Creation Date	Description	Customer Notification
<input type="checkbox"/>	Medium	453	15/02/2022 10:18:55 AM GMT+01:00	Generic table access via critical transaction	No
<input type="checkbox"/>	Low	454	17/02/2022 11:36:04 PM GMT+01:00	Admin group assignments	No
<input type="checkbox"/>	Medium	455	20/02/2021 10:42:45 AM GMT+01:00	Segregation of Duties	No
<input type="checkbox"/>	Medium	457	20/02/2022 15:52:37 AM GMT+01:00	User type change	No
<input type="checkbox"/>	Medium	458	21/02/2022 06:22:40 AM GMT+01:00	Suspicious http path connect	No
<input type="checkbox"/>	Medium	461	24/02/2022 09:55:21 PM GMT+01:00	System security settings change	No

# Demo



Monthly Reports

	Year	Month
<input checked="" type="checkbox"/>	2022	February
<input type="checkbox"/>	2022	January
<input type="checkbox"/>	2021	December

# **SAP Enterprise Threat Detection** **cloud edition – Investigation Reports**

# Report for Investigation

## SAP Enterprise Threat Detection, Cloud Edition

### Investigation Report for March 2022

#### Investigation Overview

26 Investigations occurred in March 2022:

Investigation Severity	Count
Very High	0
High	5
Medium	11
Low	10

#### Investigations

The following table lists all investigations that occurred in March 2022:

Investigation ID	Description	Customer Notification
531	Investigation for testing report generation 3	No
530	Test investigation for report generation 2	No
532	Investigation for testing report generation 4	No

# Report for Investigation

## SAP Enterprise Threat Detection, Cloud Edition Report for Investigation 462

### Investigation Overview

Creation Time	2/2/2022 12:28:03 PM UTC
Created By	securityanalyst1@sap.com
Description	Suspicious behavior of User DDIC
Severity	High
Status	Completed
Customer Notification	No
Management Visibility	Not Needed

### Investigation Actions

The following actions were performed on investigation processing:



# Reporting: Example Investigation Protocol

## Users

The following users occurred in the alerts contained in the investigation:

User	Roles	Alerts
DDIC	Targeted	2074564,2074570,2074577,2074604

## Alerts

The following alerts are part of this investigation:

### Alert 2074577

#### Attributes

Pattern	Logon with SAP standard users
Trigger	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon', 'Network, Hostname, Initiator' = '10.20.30.40', 'System ID, Actor' = 'ABC/904', 'User Name, Targeted' = 'DDIC')
Triggering events count	58
Severity	High
Creation Time	2/2/2022 12:22:26 PM UTC

# Reporting: Example Investigation Protocol

## Triggering Events

The following events triggered the alert:

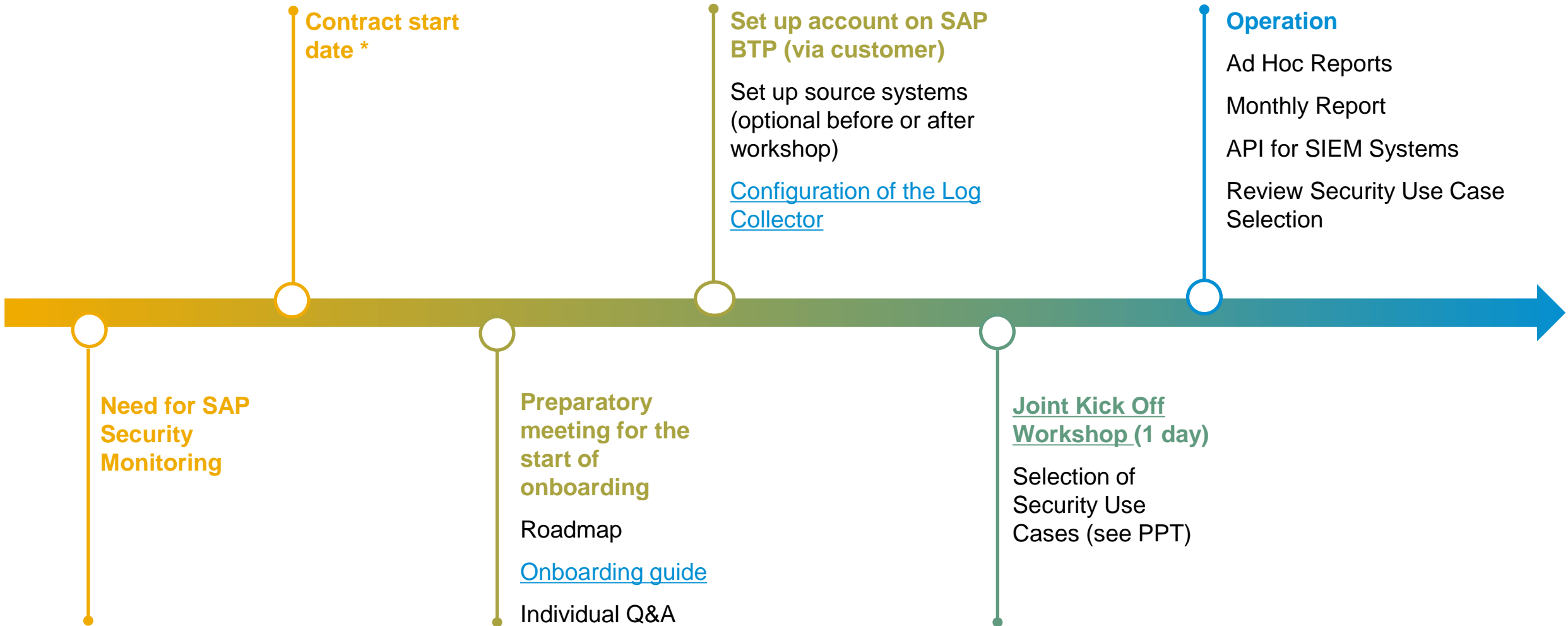
```
2128FEFC1EC74C69B1171067E76146C1,2022-02-02T12:10:05.758,1643803810316,pcpaction:MESSAGE pcp-body-type:text  
logentry:SAL sid:ABC instance_name:ldai1ABC_ABC_32 instance_host:vlgai1ABC client:904 user_name:DDIC  
user_ip:10.20.30.40  
epp_ctxid:42010AEE28741EECA0B41E23C58FF685  
epp_connid:00000000000000000000000000000000 counter:4527037 utc:1643803805.758  
E="AU1",SEN="00032",SET="B",STN="S000",SPN="RSBTCRTE",ESC="5",EM="B&0&A",Security  
AuditLog,10.238.40.116,,127.0.1.1,10514
```

```
12AF340E4D17401DA54CBB8ED4641D1A,2022-02-02T11:55:05.651,1643802907479,pcpaction:MESSAGE pcp-body-type:text  
logentry:SAL sid:ABC instance_name:ldciABC_ABC_32 instance_host:vlgciABC client:904 user_name:DDIC user_ip:10.20.30.40  
epp_ctxid:42010AEE28741EECA0B41E23C58FF685  
epp_connid:00000000000000000000000000000000 counter:4468363 utc:1643802905.651  
E="AU1",SEN="00046",SET="B",STN="S000",SPN="RSBTCRTE",ESC="5",EM="B&0&A",Security  
AuditLog,10.238.40.112,,127.0.1.1,10514
```

...

# **SAP Enterprise Threat Detection** **cloud edition How to Run**

# Timeline SAP Enterprise Threat Detection cloud edition



\* SAP needs 4 weeks to start with the baseline security service

# Workshop Content

## Technical Part

- Architecture
- Log Collector



## Additional Part

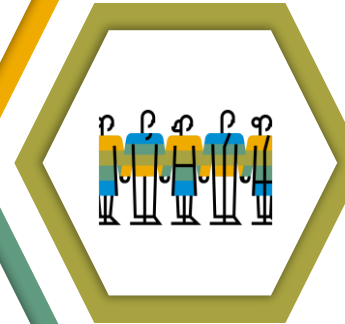
- Log Collector Installation/Configuration
- Security Follow Ups on Customer side

*Not part of the basic service*



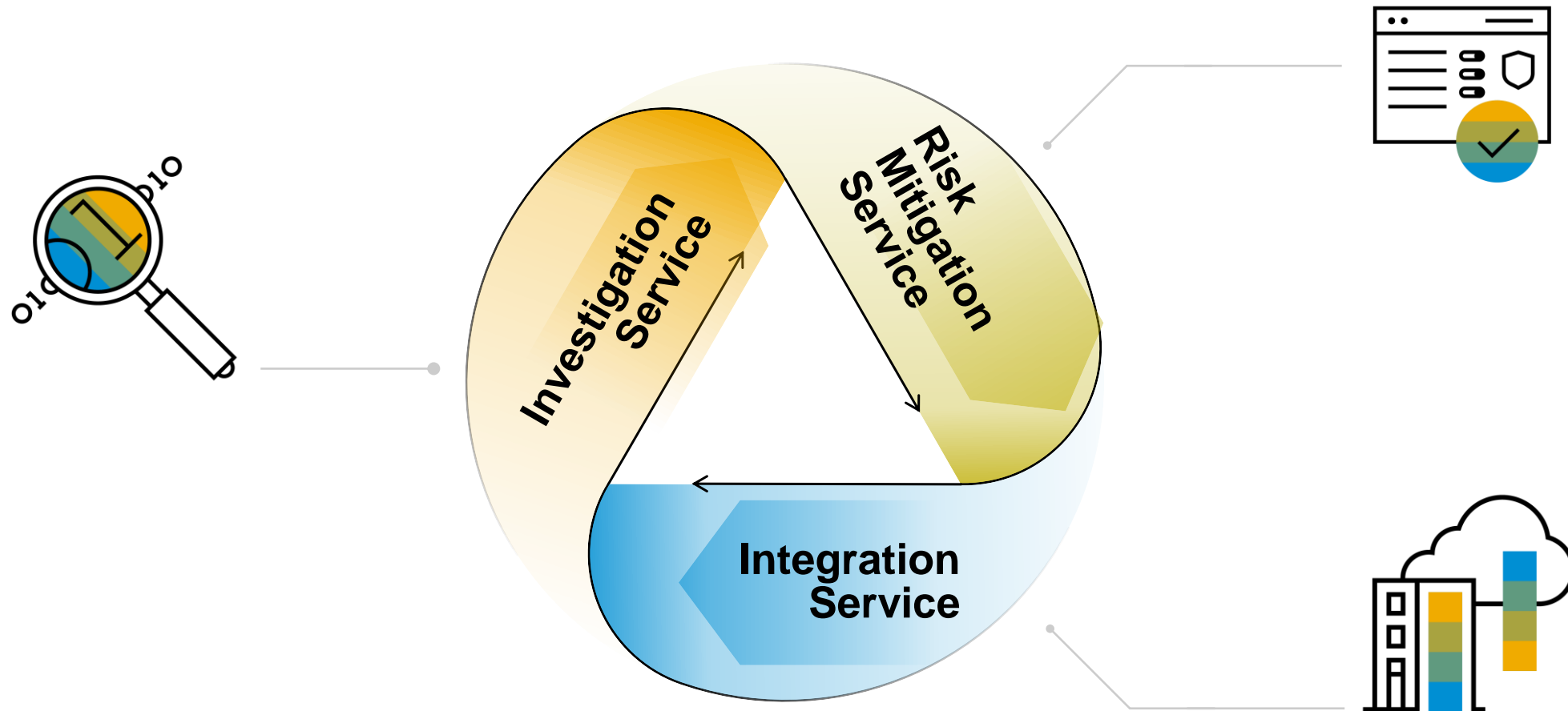
## Security Part

- Pattern discussion based on Sample Report
- Pattern selection
- Report related action items for customers



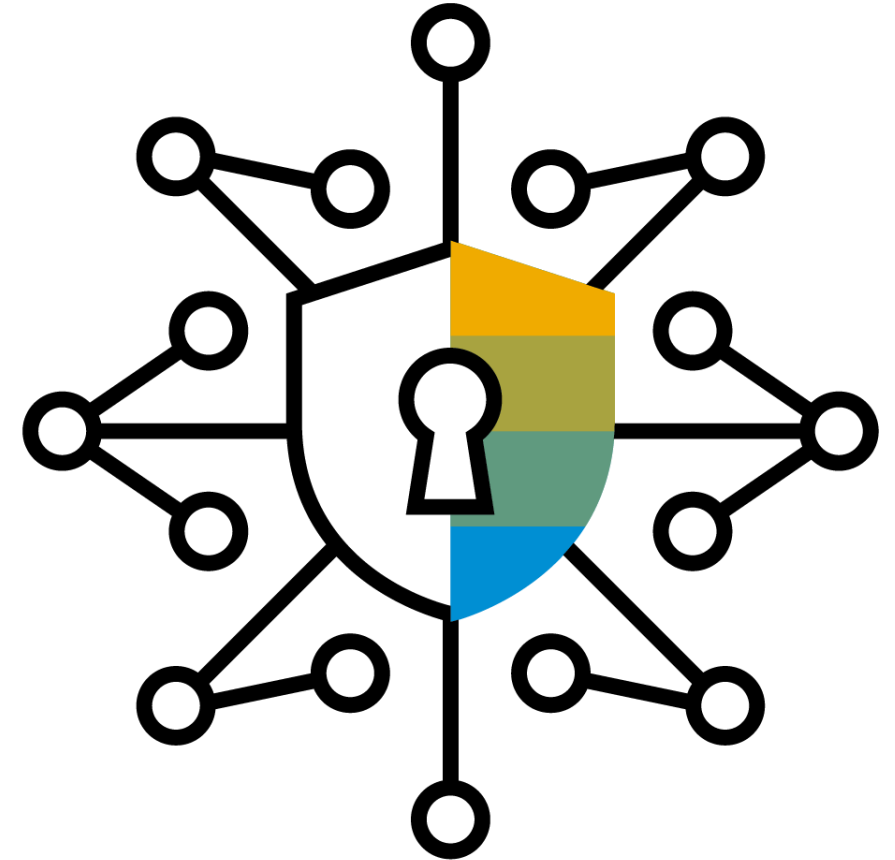
# SAP Enterprise Threat Detection cloud edition

Additional SAP Services for Customer Enablement and Incident Management



# Unique benefits of Enterprise Threat Detection

- **SAP understands SAP log files best**
  - Forensic analyses over months
  - as well as Threat Hunting
  - and Anomaly detection
  - Generic approach (not based on fix test cases)
- **SAP-specific content**
  - Customers give us feedback and extend our use cases
  - Regular expansion of available content (every 2 months)
  - Transparency of SAP security patches not being applied
  - Bridging the gap between security departments
- **Unfiltered SAP logs**
  - Real time manipulation save data transfer to Enterprise Threat Detection
  - Normalization to achieve readability of protocols, which can then also be used by Audit
  - Any log type can be added SAP and non-SAP e.g. Read Access Logging / UI Logging Logs
  - Correlation of all log files to achieve a complete picture, not only puzzle pieces
  - Analysis of e.g.: What else did the user do?



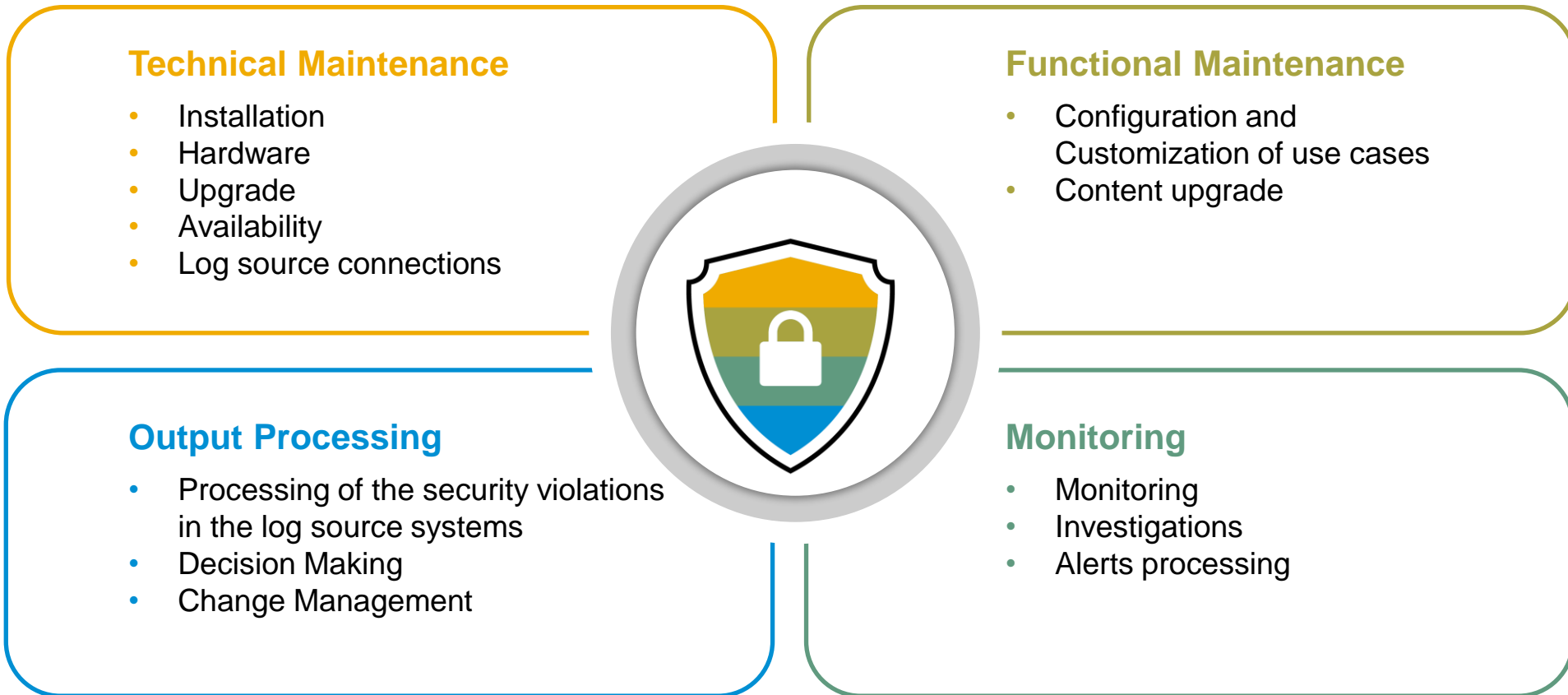
# Appendix



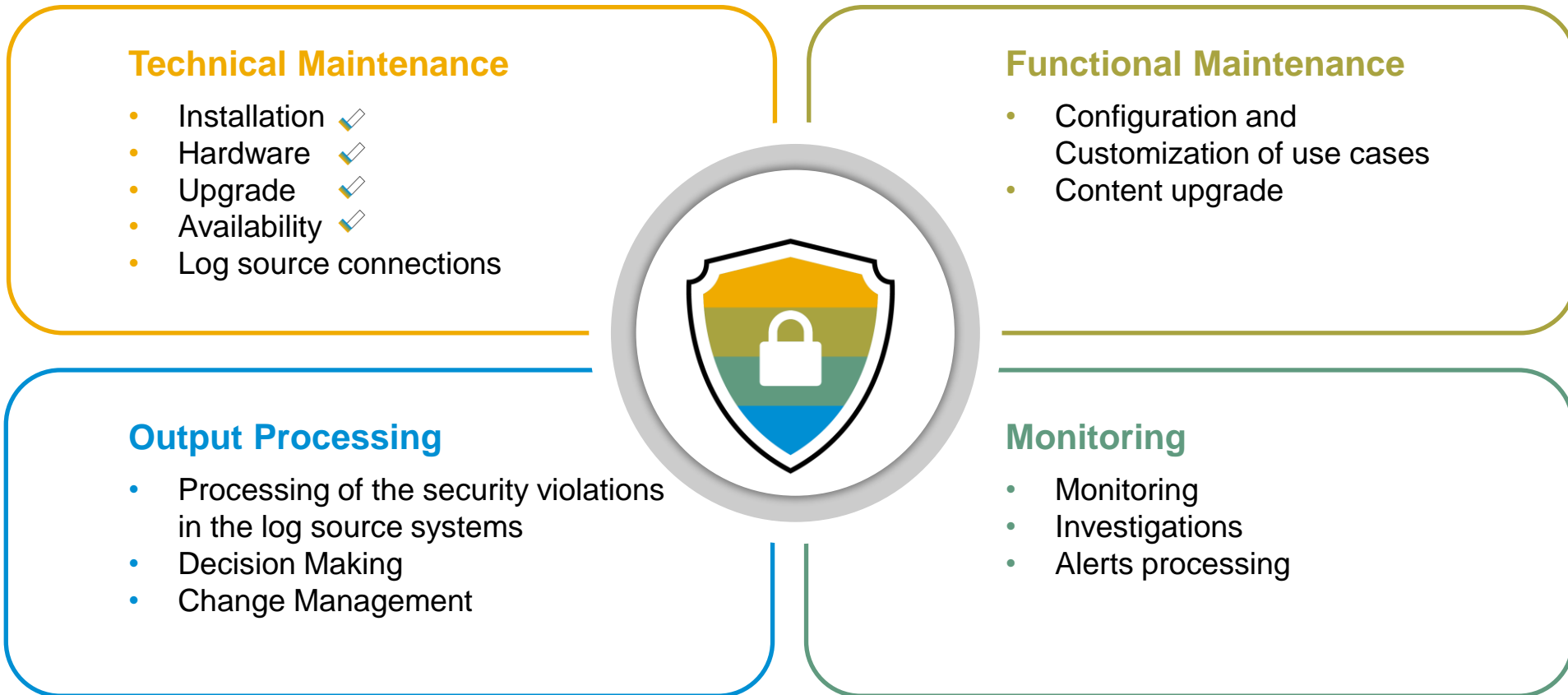
# **SAP Enterprise Threat Detection** **cloud edition vs. On-Prem & PCE**

# SAP Enterprise Threat Detection (OnPrem)

## Main Tasks

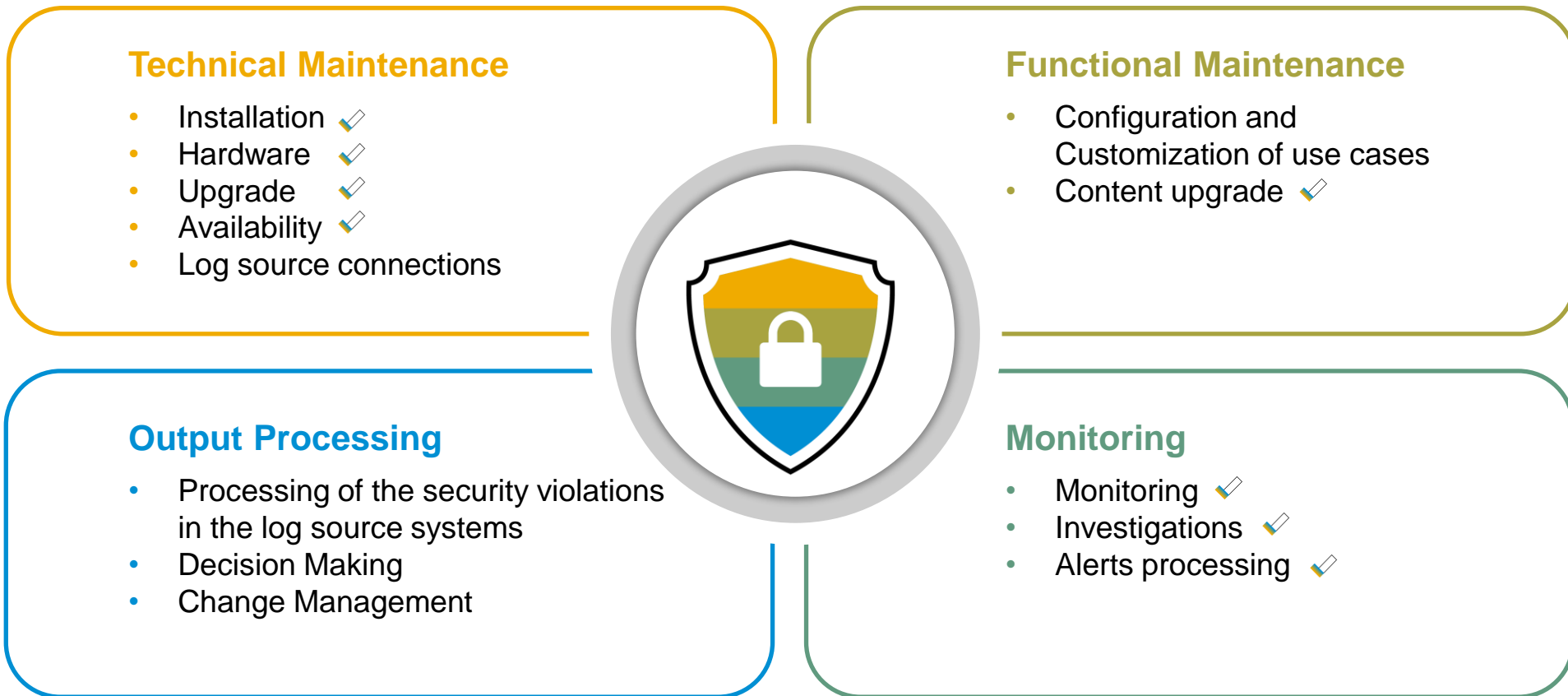


# SAP Enterprise Threat Detection (PCE)



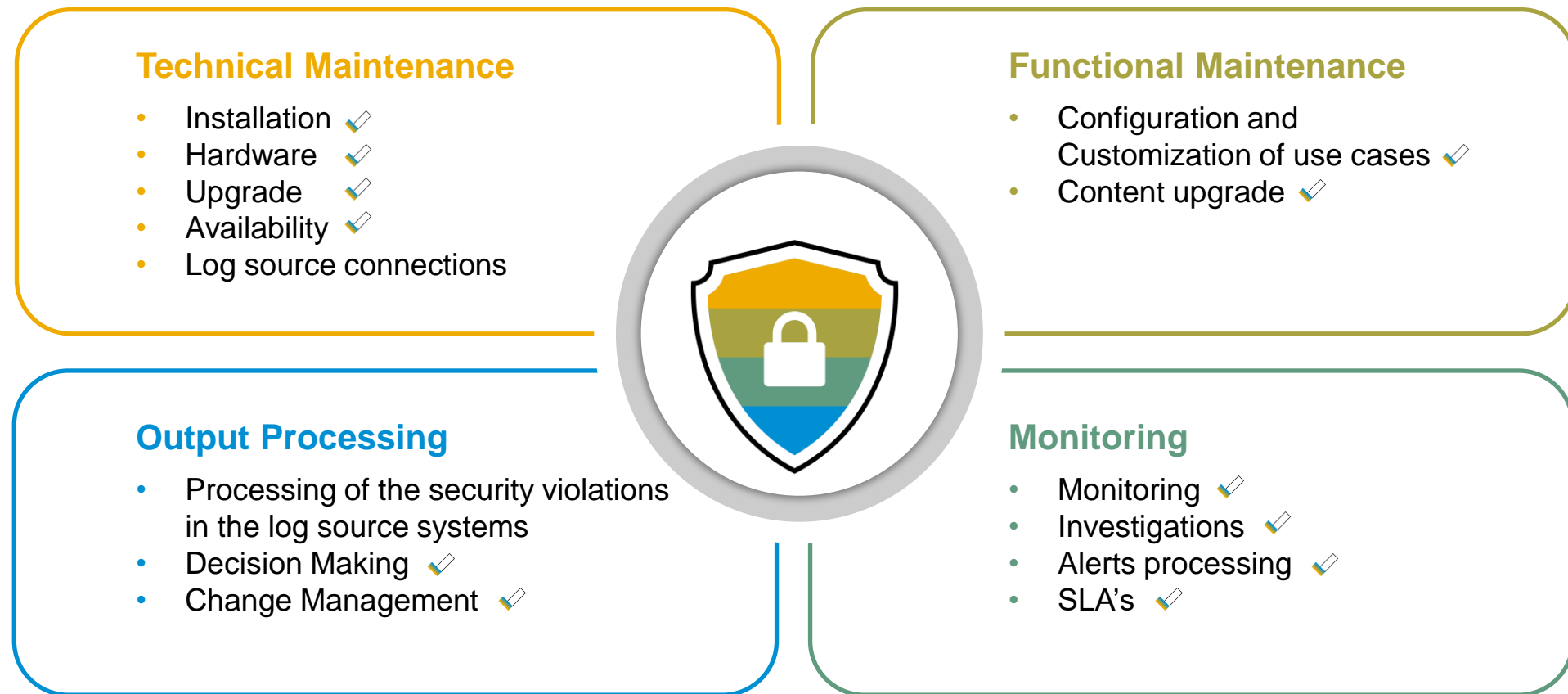
Included in PCE offering

# SAP Enterprise Threat Detection cloud edition - Baseline Service



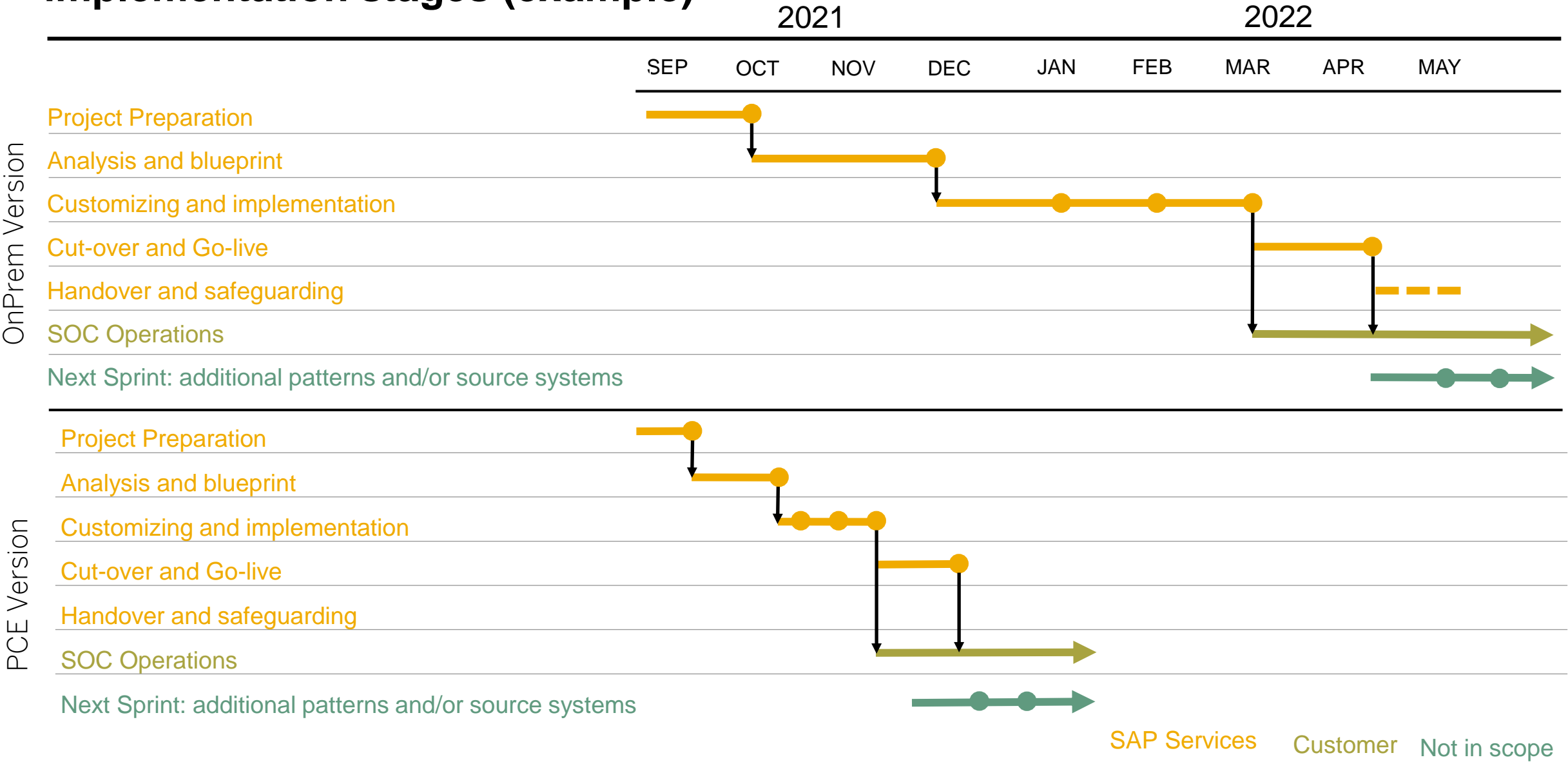
Included in Managed Service

# SAP Enterprise Threat Detection cloud edition (extended service planned in 2023)



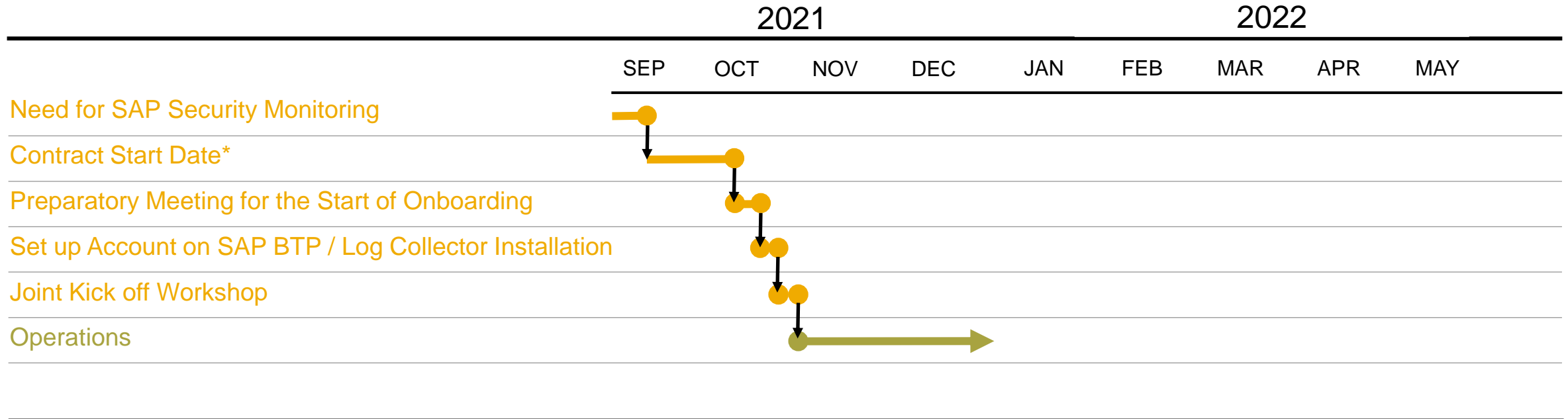
# **SAP Enterprise Threat Detection** **cloud edition vs. On-Prem & PCE** **project plan**

# SAP Enterprise Threat Detection (OnPrem / PCE) project plan and implementation stages (example)



# SAP Enterprise Threat Detection (Cloud Edition) project plan and implementation stages (example)

ETD Cloud Edition

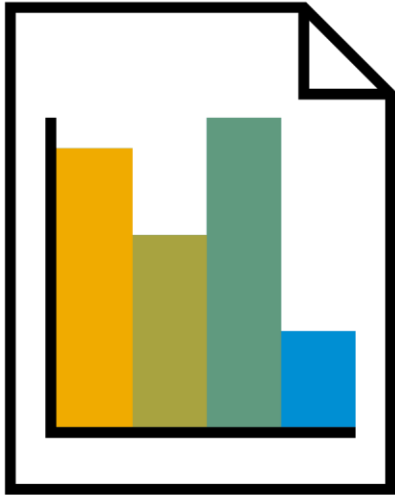


\* SAP needs 4 weeks to start with the baseline security service

SAP Services Customer Not in scope



# Log Data Supported by SAP Enterprise Threat Detection



## SAP NetWeaver / S/4 Log Types

- System Log
- Security Audit Log
- Business Transaction Log
- HTTP Server Log
- RFC Gateway Log
- User Change Log
- Change Document Log
- Read Access Log / UI Log
- SOAP based Web Services Log
- Log HTTP Client and HTTP Server Log
- ABAP and Stand-Alone Web Dispatcher

## ETD Own Monitoring Log

- ETD Configuration Change Audit Log

## SAP NetWeaver Java

- HTTP Access Log (Java)
- Security Audit Log (Java)
- Security Log (Java)

## HANA DB

- HANA Audit Trail

## SAP Business Technologie Platform

- SAP BTP Audit Log (Neo +CF)

## Other SAP business solutions

- SAP Commerce
- SAP C4C

## Linux

- AuditD

### In Planning:

Log Change Reader  
Transport File Analyzer  
Cloud Connector Logs  
Business Objects Log Support

Table Change Log  
SAP Analytics Cloud  
SAP Cloud Solutions

# Thank you.

Contact information:

**Arndt Lingscheid**

a.lingscheid@sap.com

Solution Owner:

SAP solutions for cyber security and data protection

Dietmar-Hopp-Allee 16  
69190 Walldorf, Germany

Follow us



[www.sap.com/contactsap](https://www.sap.com/contactsap)

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

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.

See [www.sap.com/copyright](https://www.sap.com/copyright) for additional trademark information and notices.