



TechEd 2021

High-performance threat analytics

protecting SAP S/4 HANA applications

Arndt Lingscheid, Michael Schmitt
11, 2021

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.

Agenda

Introduction to SAP Enterprise Threat Detection

- What is it?
- How does it help securing your SAP landscapes?
- Typical Use Cases
- Information on SAP Enterprise Threat Detection, cloud edition

SAP Enterprise Threat Detection Basic Demo

- Navigate within SAP Enterprise Threat Detection

Demo of an Attack/Defend Scenario

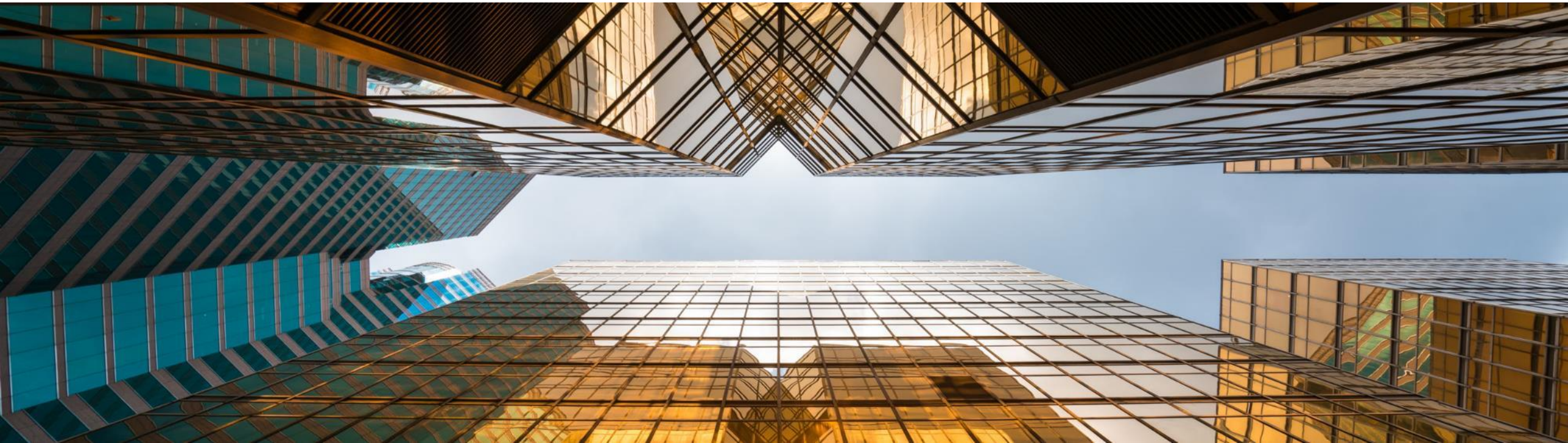
- Attack scenarios in an S4H system
- Detection in ETD

Organization for later Hands-On Sessions

- Details for Subscription

Q&A

Introduction to **SAP Enterprise Threat Detection**





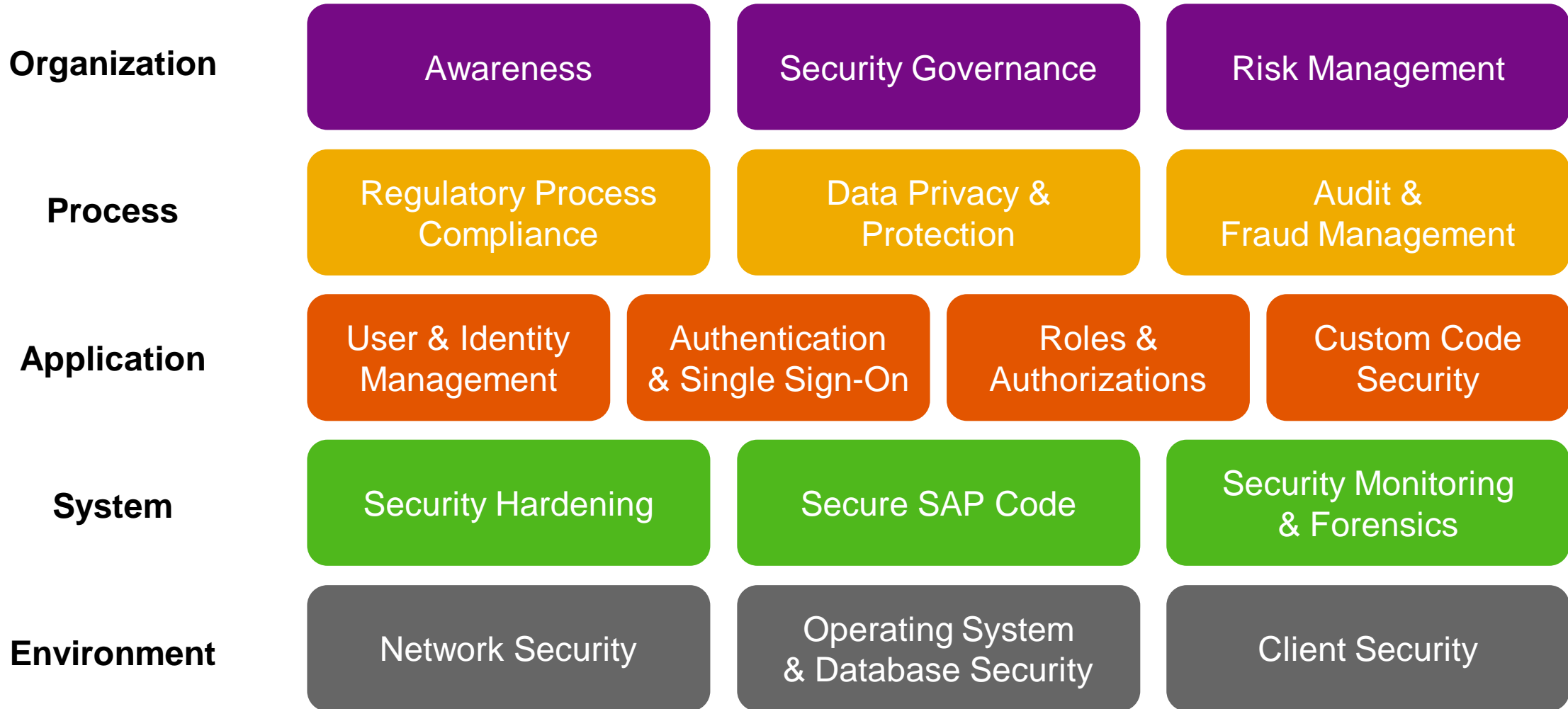
Systems are under attack

Sobering Statistics

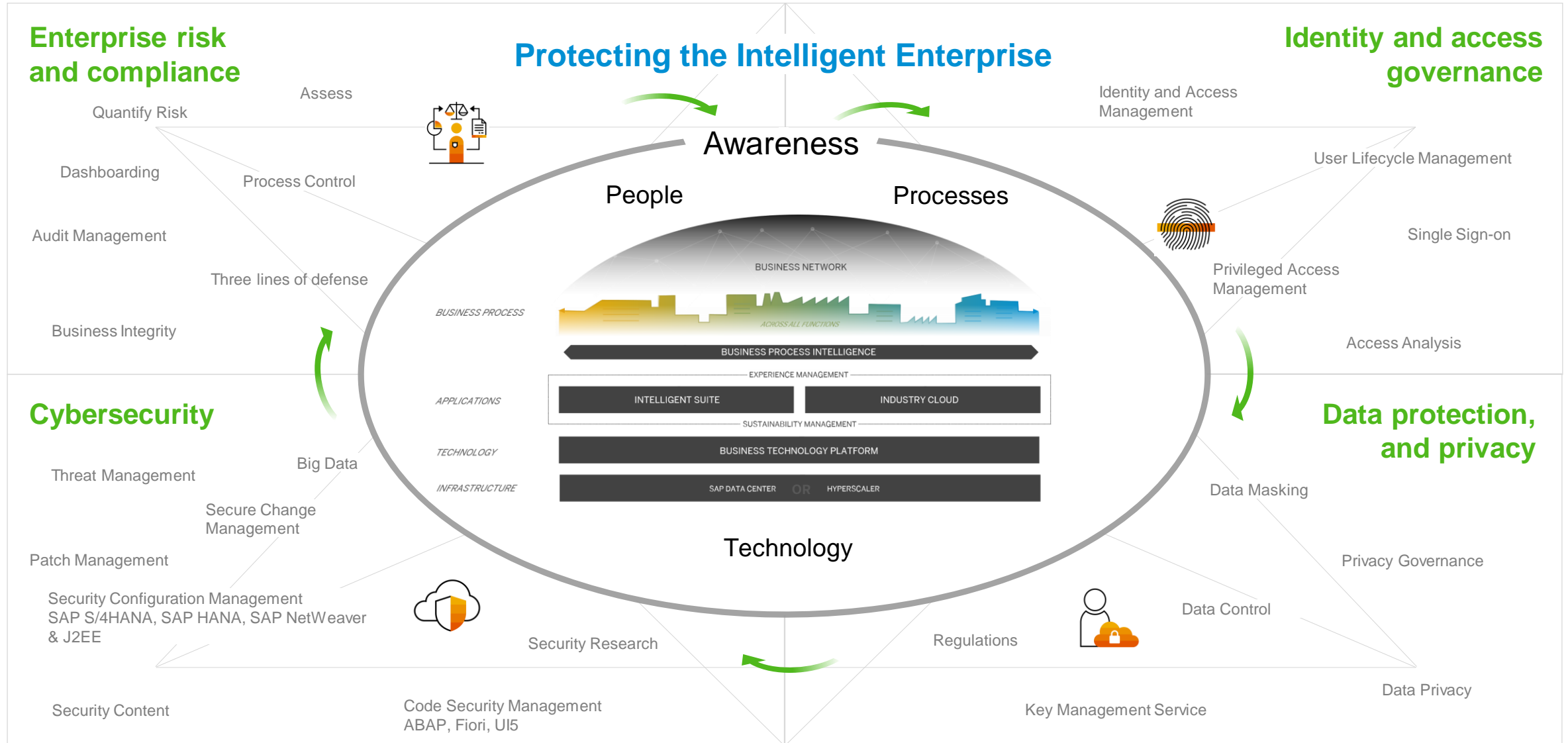
- Businesses that had not deployed security automation saw an average total cost of **\$6.03 million**, more than double the average cost of a data breach of **\$2.45 million** for businesses that had fully deployed security automation.
- **\$5.52 million average total cost of a breach** at enterprises of more than 25,000 employees
- **Mega Breaches**: In breaches of more than 50 million records, the average cost was **\$392 million**, more than 100 times the average.
- The time to contain a security breach on average is **280 days**.
- Lost business costs **\$1.52 million** accounted for nearly **40%** of the average total cost of a data breach.
- It's not a question of experiencing a data breach. It's only a question WHEN!
(The percentage chance of experiencing a data breach within two years was **~30%** percent in 2019.)

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

SAP Secure Operations Map



SAP Depth and Breadth, supporting the Intelligent Enterprise



Cybersecurity- and Compliance Solutions from SAP based on NIST



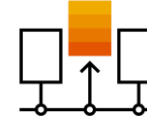
Identify



Protect



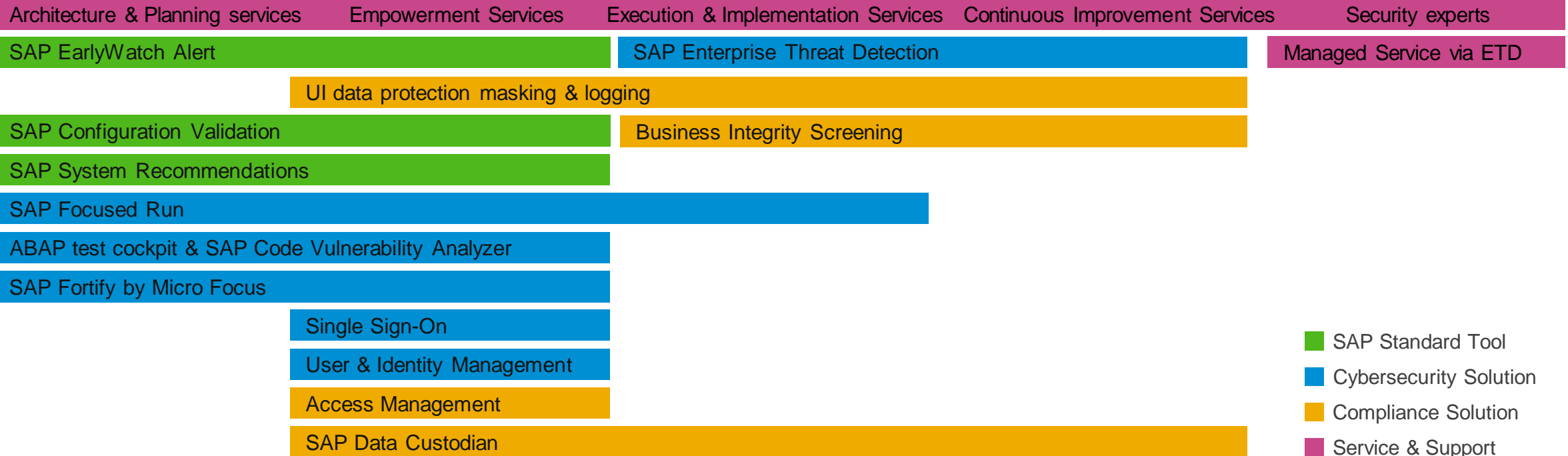
Detect



Respond



Recover



- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

SAP Enterprise Threat Detection



Stop security breaches in today's SAP S/4HANA business applications.

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

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.

Challenge



- Increasing number of hacker attacks
- Regulatory requirements for security and compliance controls.
- Roles and Authorizations only will not protect an SAP S/4HANA environment.
- Perimeter and IT infrastructure security is not sufficient to protect the SAP S/4HANA business core.
- Analyzing the huge amount of events coming from the SAP S/4HANA Business Applications.

Solution



- Stop security breaches in today's SAP S/4HANA business applications.
- SAP system Transparency with respect to Security- and Compliance-Events.
- Correlate the complete picture of a hacker attack, not only a few small puzzle pieces.
- Perform forensic investigations, search for threats and detect anomalies in SAP S/4HANA applications.
- All audit logs available in a central instance (manipulation safe, unfiltered, normalized, readable).

Benefits



- **Detect** threats in your most valuable assets of SAP S/4HANA applications to avoid financial loss, legal and reputational damage.
- **Safeguard** the operation of your SAP S/4HANA and ensure the continuity of your business.
- **Reduce** effort for conducting audits, managing compliance to regulatory requirements and company policies.
- **Gain transparency and simplify** the analysis of suspicious activities, identify security gaps, and understand the impact on your business.
- **Analyze** huge amounts of information quickly and to take the right decision in time.

Security Audit Log compliance

Challenge



Solution



Benefits



- Complex configuration
- Causes performance problems
- Must be filtered
- Cannot be read by humans
- Cannot be searched in an efficient way
- Cannot be stored for Audit purpose

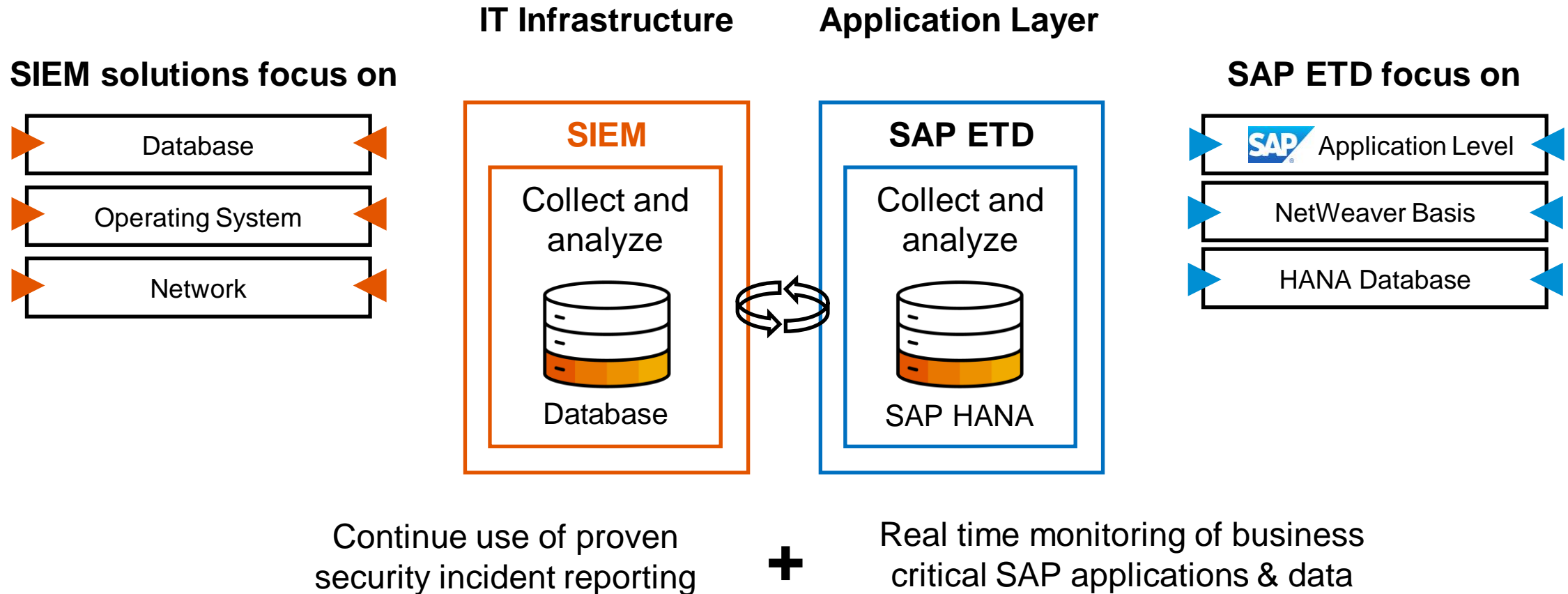
Incompliant

- Direct transfer of all information belonging to the Security Audit log to SAP Enterprise Threat Detection

- Manipulation safe Audit Log
- No additional configuration
- All Security Audit Log entries are available
- Continuous automated analysis
- Manual human analysis possible
- Audit proof at any time

Compliant

SAP Enterprise Threat Detection (ETD) and generic SIEM systems



Integration of SAP ETD with all leading SIEM solutions (HP Arcsight, IBM Q-Radar, Splunk) available

NIST Framework



Identify

Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Supply Chain Risk Management



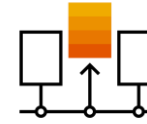
Protect

Access Control
Awareness and Training
Data Security
Information
Maintenance
Protective Technology



Detect

Anomalies and Events
Continuous Security Monitoring
Detection Processes



Respond

Response Planning
Communications
Analysis
Mitigation
Improvements



Recover

Recovery Planning
Improvements
Communications

Cybersecurity- and Compliance Solutions from SAP based on NIST



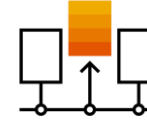
Identify



Protect



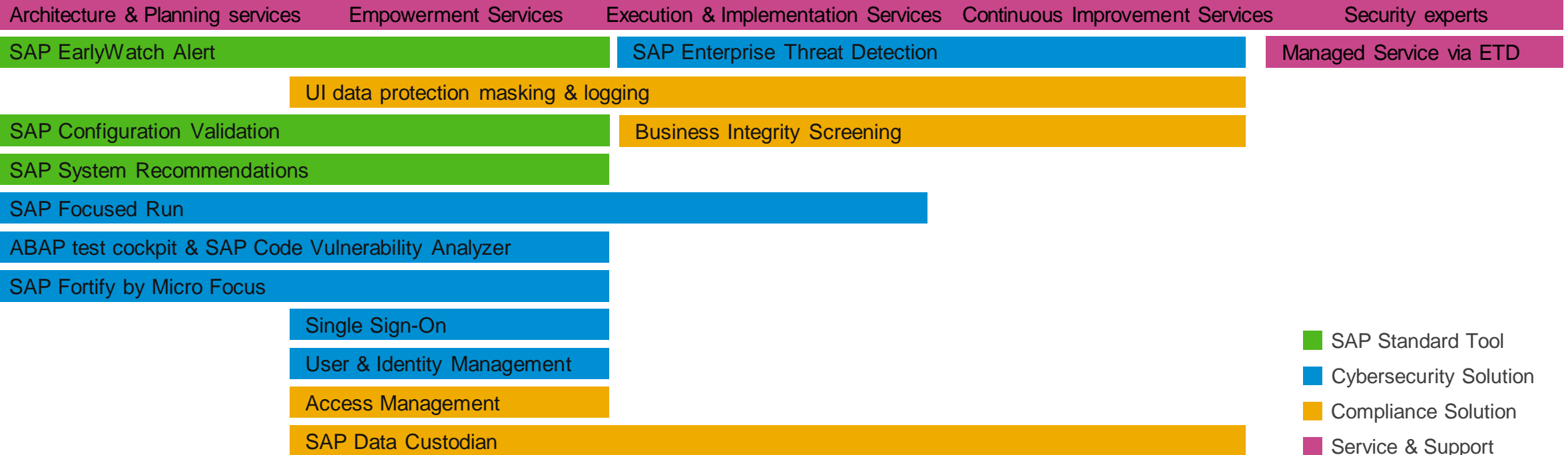
Detect



Respond

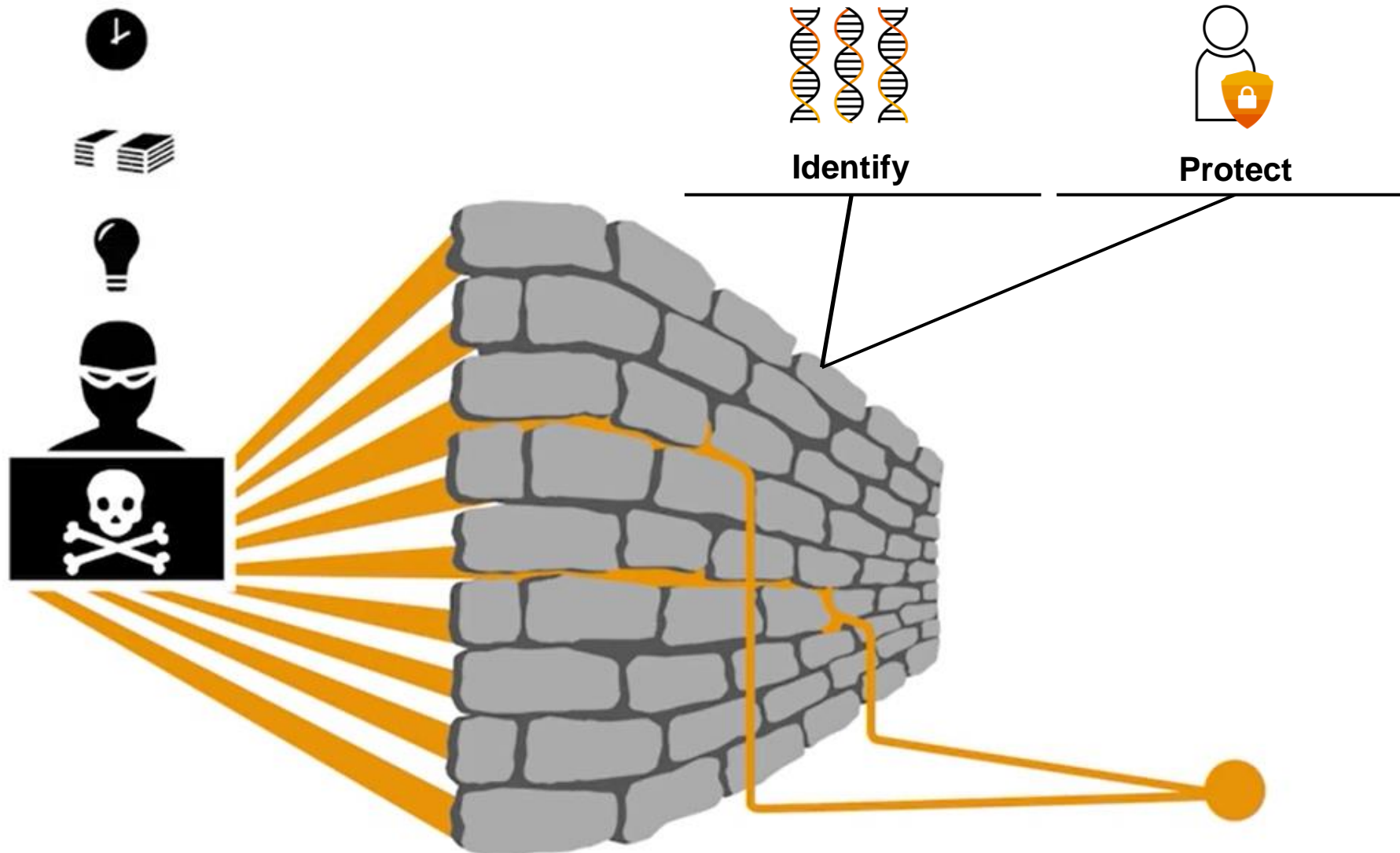


Recover



- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

SAP Enterprise Threat Detection



SAP Enterprise Threat Detection

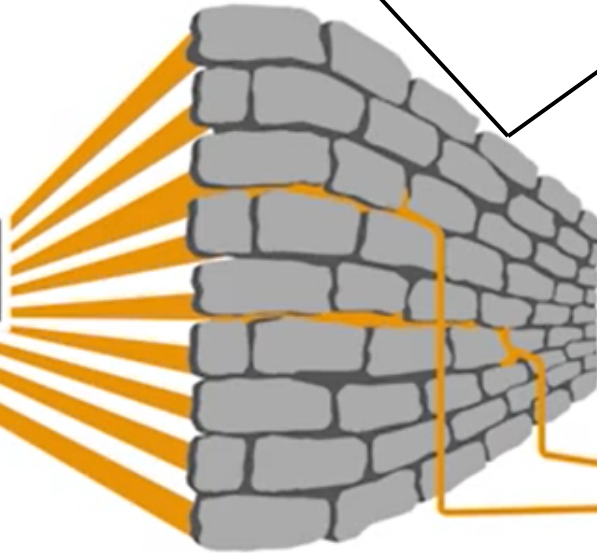


Identify



Protect

Experiencing a data breach within two years is ~ 30 percent.

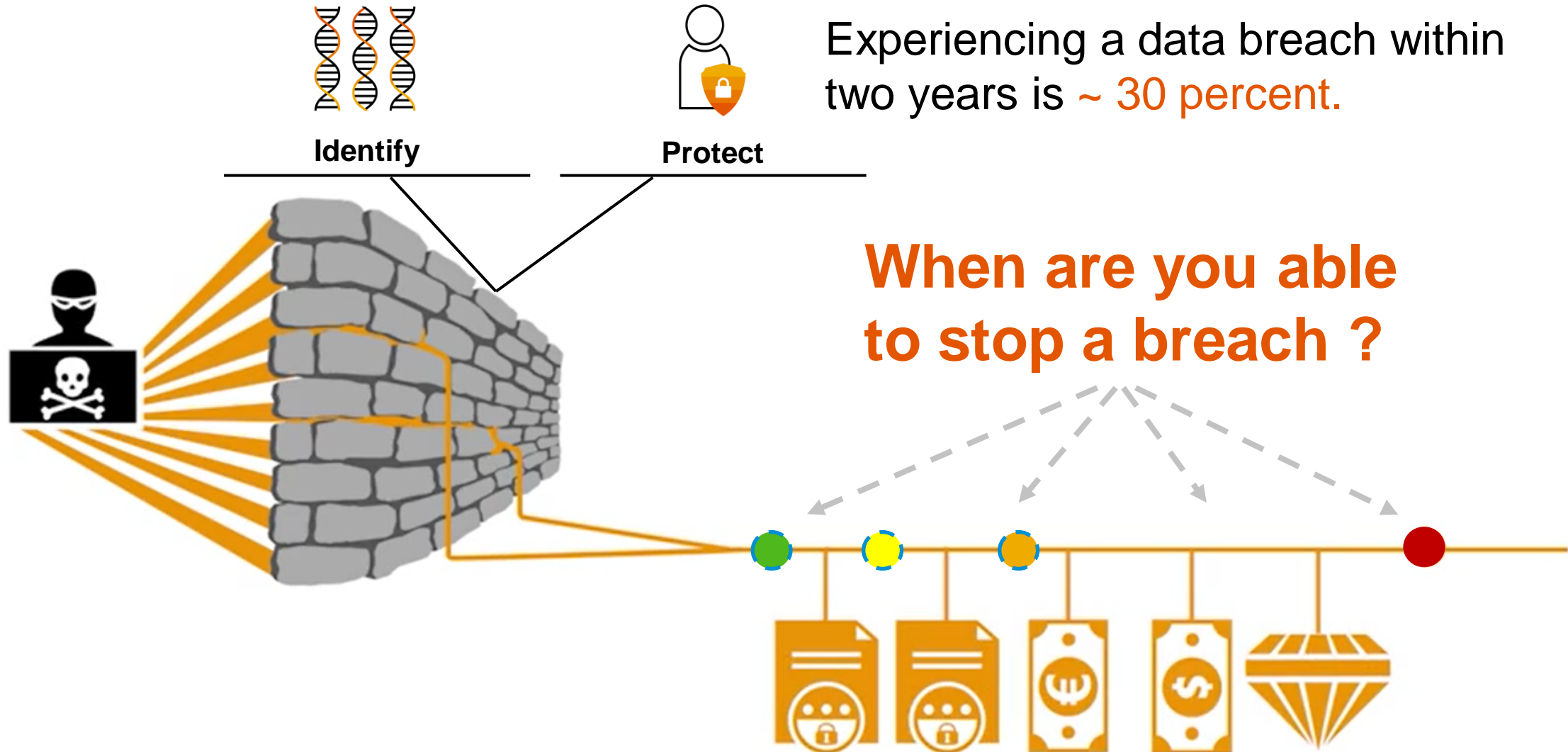


280 Day's

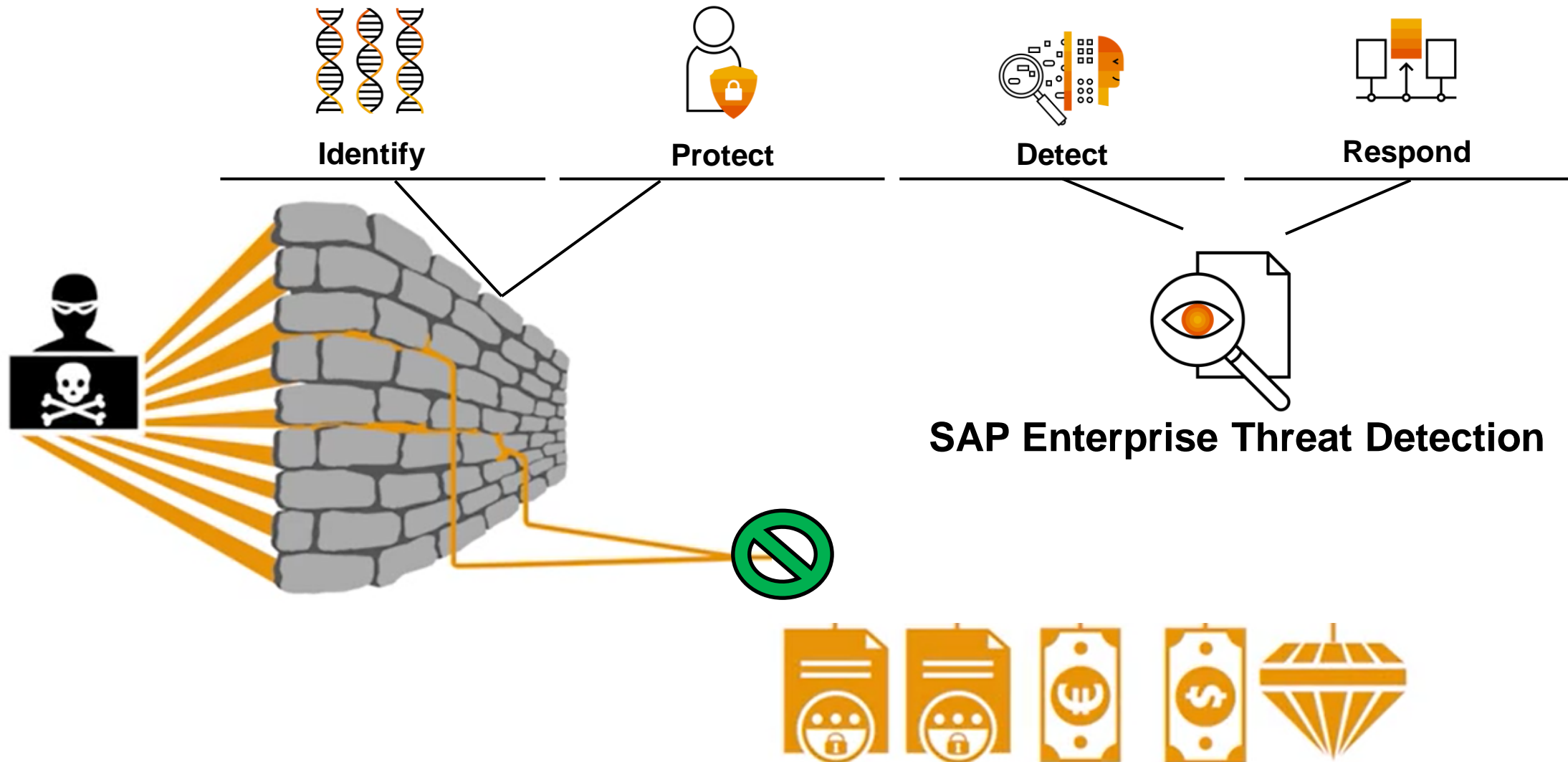
(206 + 73)



SAP Enterprise Threat Detection



SAP Enterprise Threat Detection

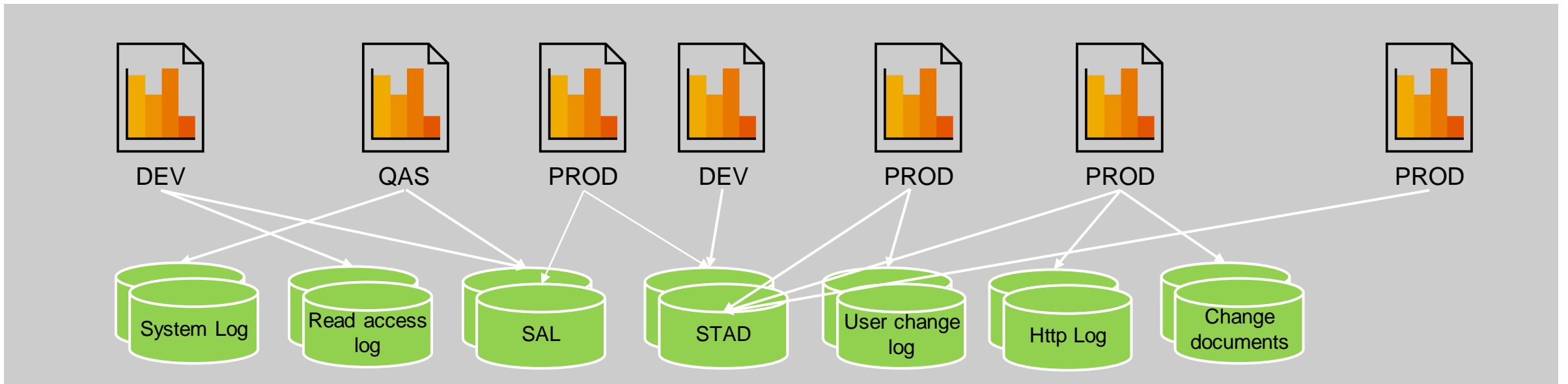
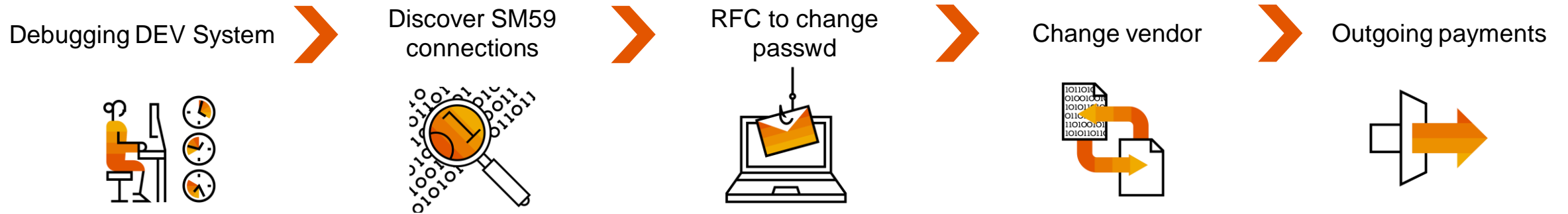


Examples of real life security incidents

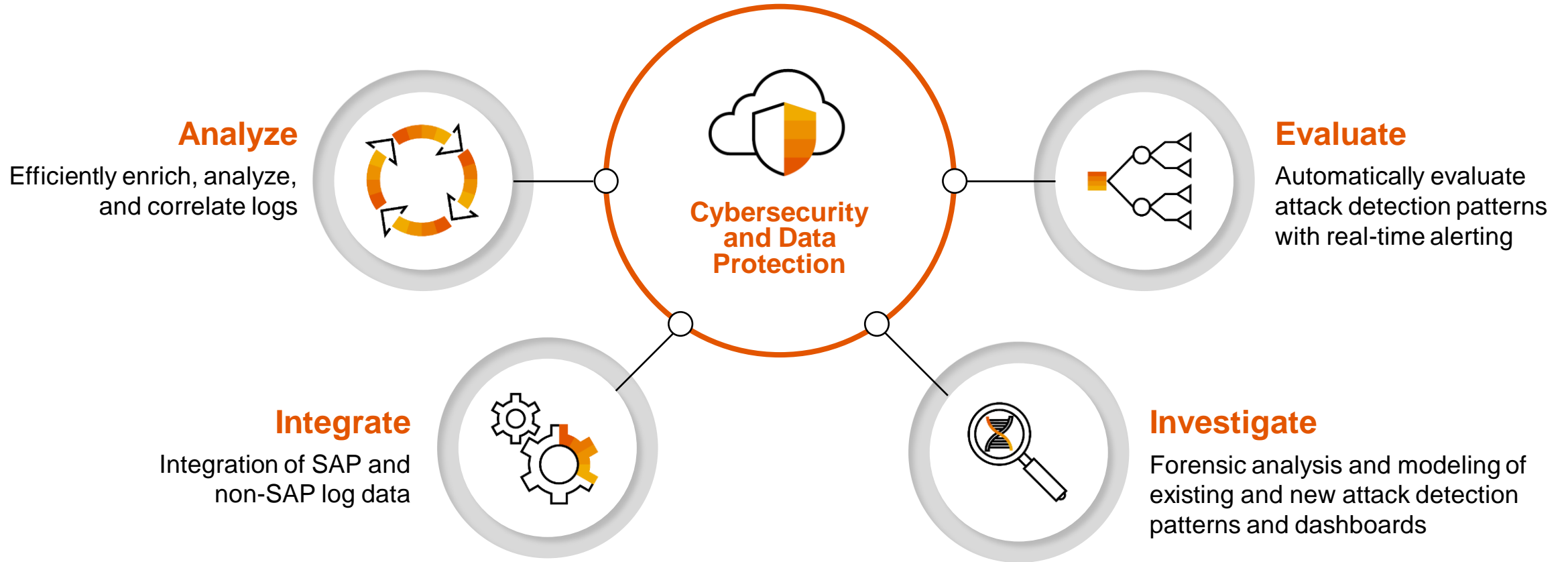
- 1) Information about new products stored in SAP applications appeared in the internet before product launch
- 2) New published SAP Security vulnerability was used two days after SAP's security patch day to access critical data
- 3) User data tables with weak password hashes were downloaded on file system
- 4) Brute force attack was used to access SAP with superuser permissions
- 5) User tried to log on to (all) companies SAP systems using the SAP standard users
- 6) Download of chemical compositions in the ERP test environment via developer rights. The employee left the company and started at a competitor
- 7) Identity theft: user login in the same timeframe from different locations
- 8) External consultants disregard security policies and work as developer in a productive system
- 9) Business interruption for several days because an external partner deleted an SAP business table
- 10) A user's password was decrypted. The hacked user was suspected of stealing company data. Fortunately, he did not have access to the system at the time because it was a holiday in his country.
- 11) Privileged user manipulated his/her salary (many)



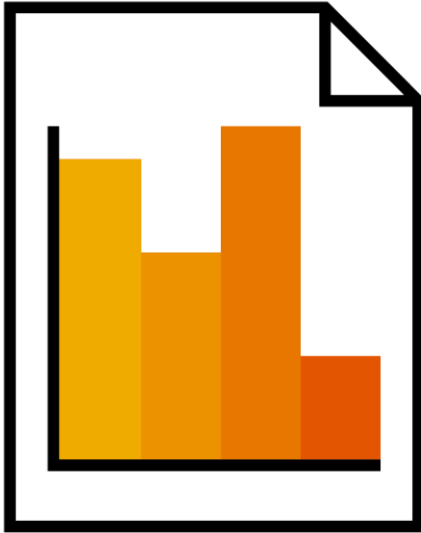
Preventing Fraud & Cyber Attacks



How does SAP Enterprise Threat Detection work



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

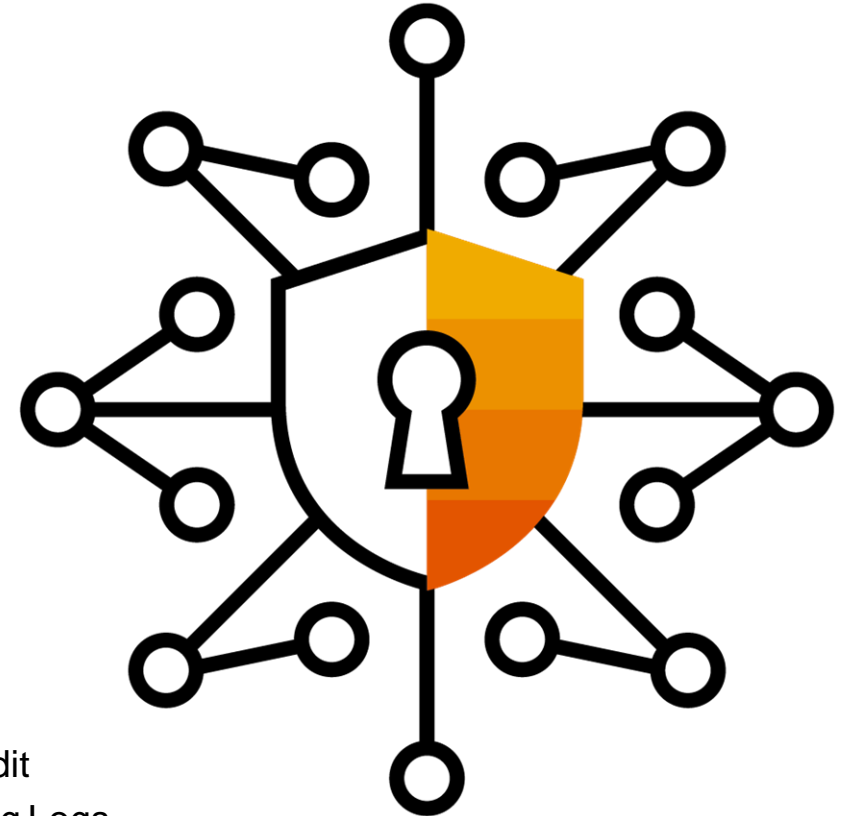
In Planning:

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

Table Change Log
SAP Analytics Cloud
SAP Cloud Solutions

Unique benefits of Enterprise Threat Detection

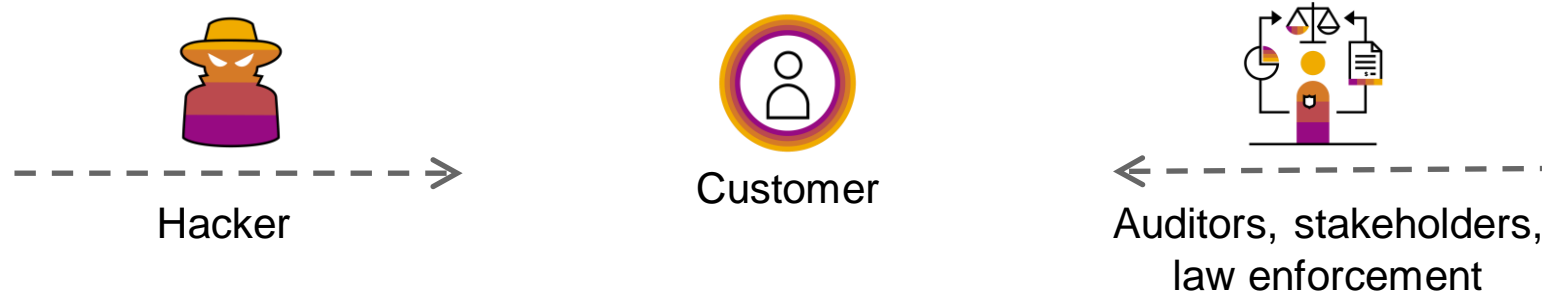
- SAP understands SAP log files best
 - Forensic analyses over months
 - as well as Threat Hunting
 - and Anomaly detection
 - Generic approach (not based on fix test cases)
- SAP-specific content
 - Customers give us feedback and extend our patterns
 - Regular expansion of available content (every 2 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?



SAP Enterprise Threat Detection, cloud edition

Protecting the crown jewels

Product arrives with included Managed Security Service!



- Baseline Service
- ✓ 7x24 alert generation for your SAP environment
 - ✓ Active alert monitoring ***
 - ✓ Checking for ~50 standard attack path patterns
 - ✓ Risk based & prioritized alerting **
 - ✓ Monthly reporting of incidents and log data

Alert processing and
investigation at best efforts

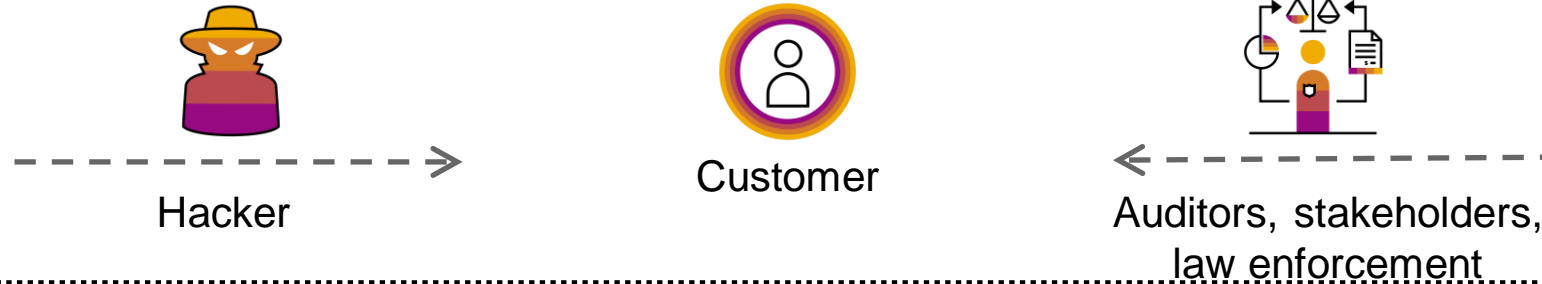
Different datacenters*

Local Service provision*

Language: English

SAP Enterprise Threat Detection, cloud edition

Protecting the crown jewels



Extended Service

- Committed response times
- Security consulting (T&M)
- Customized service level agreements

Customized/Enhanced SLAs
on additional costs

Baseline Service

- ✓ 7x24 alert generation for your SAP environment
- ✓ Active alert monitoring ***
- ✓ Checking for ~50 standard attack path patterns
- ✓ Risk based & prioritized alerting **
- ✓ Monthly reporting of incidents and log data

Alert processing and
investigation at best efforts

Different datacenters*

Local Service provision*

Language: English

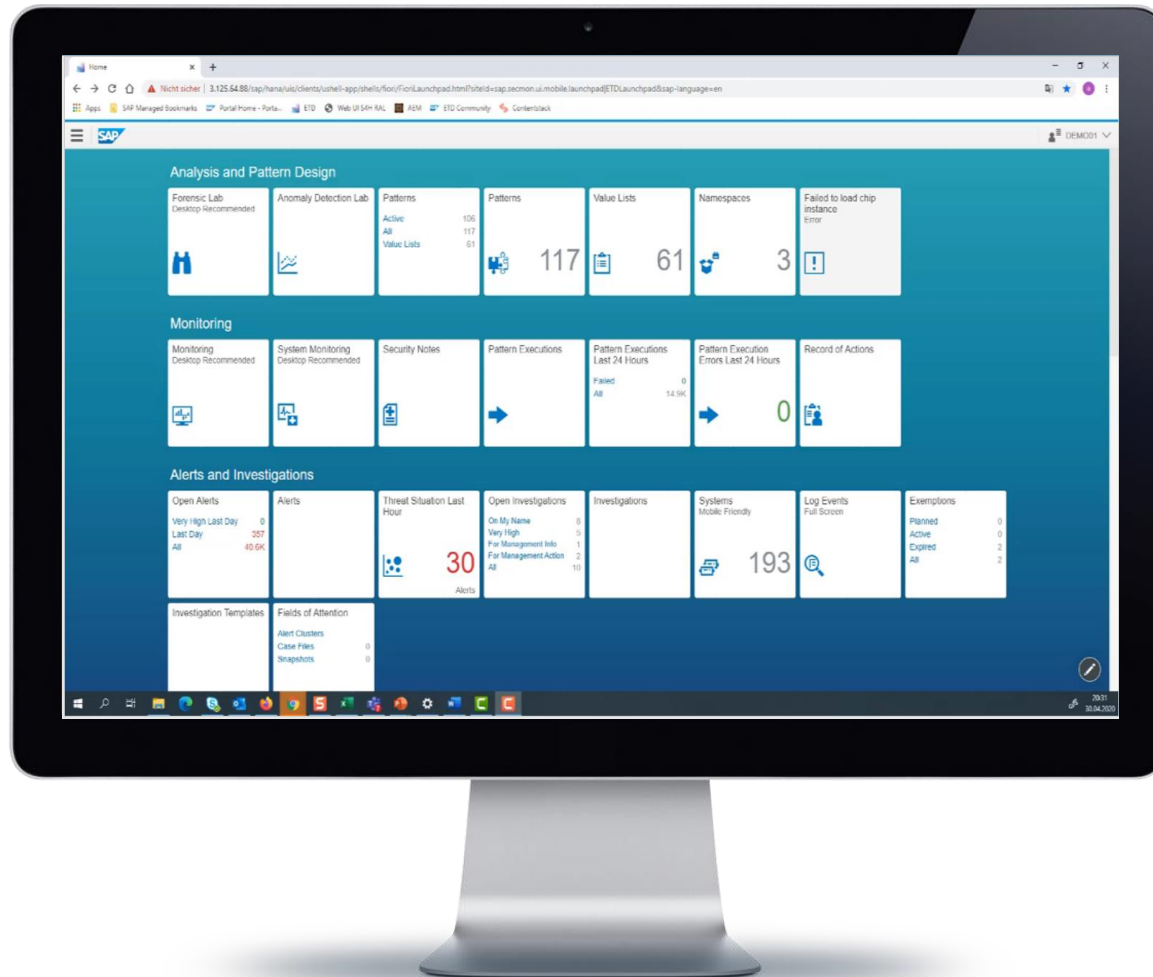
Protecting the crown jewels

Get your security controls under control

- Access to sensitive information
- Critical system configuration changes
- User and privileged access monitoring
- Critical system communication
- User login management



SAP Enterprise Threat Detection



Home

← → ↺ 🏠

Nicht sicher | 3.125.64.88/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteid=sap.secmou.uis.mobile.launchpad|ETDLaunchpad&sap-language=en

Apps SAP Managed Bookmarks Portal Home - Porta... ETD Web UI S4H RAL AEM ETD Community Contentstack

☰ SAP

👤 DEMO01

Analysis and Pattern Design

Forensic Lab
Desktop Recommended

Anomaly Detection Lab

Patterns
Active 106
All 117
Value Lists 61

Patterns
117

Value Lists
61

Namespaces
3

Failed to load chip instance
Error

Monitoring

Monitoring
Desktop Recommended

System Monitoring
Desktop Recommended

Security Notes

Pattern Executions

Pattern Executions Last 24 Hours
Failed 0
All 14.9K

Pattern Execution Errors Last 24 Hours
0

Record of Actions

Alerts and Investigations

Open Alerts
Very High Last Day 0
Last Day 357
All 40.6K

Alerts

Threat Situation Last Hour
30 Alerts

Open Investigations
On My Name 8
Very High 5
For Management Info 1
For Management Action 2
All 10

Investigations

Systems Mobile Friendly
193

Log Events Full Screen

Exemptions
Planned 0
Active 0
Expired 2
All 2

Investigation Templates

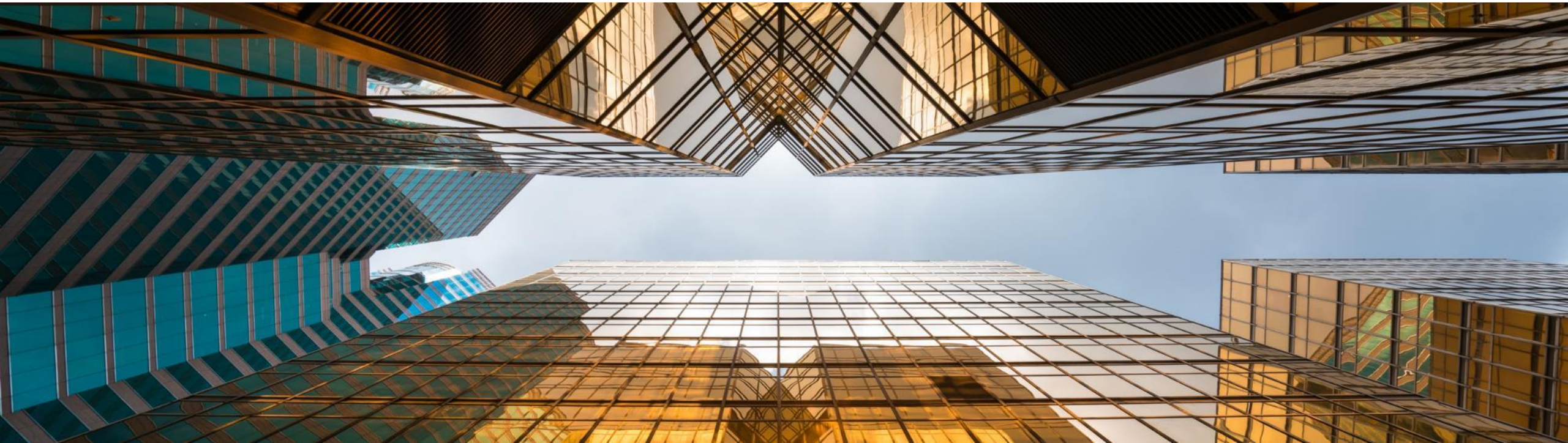
Fields of Attention
Alert Clusters
Case Files 0
Snapshots 0

🔍

20:31
30.04.2020

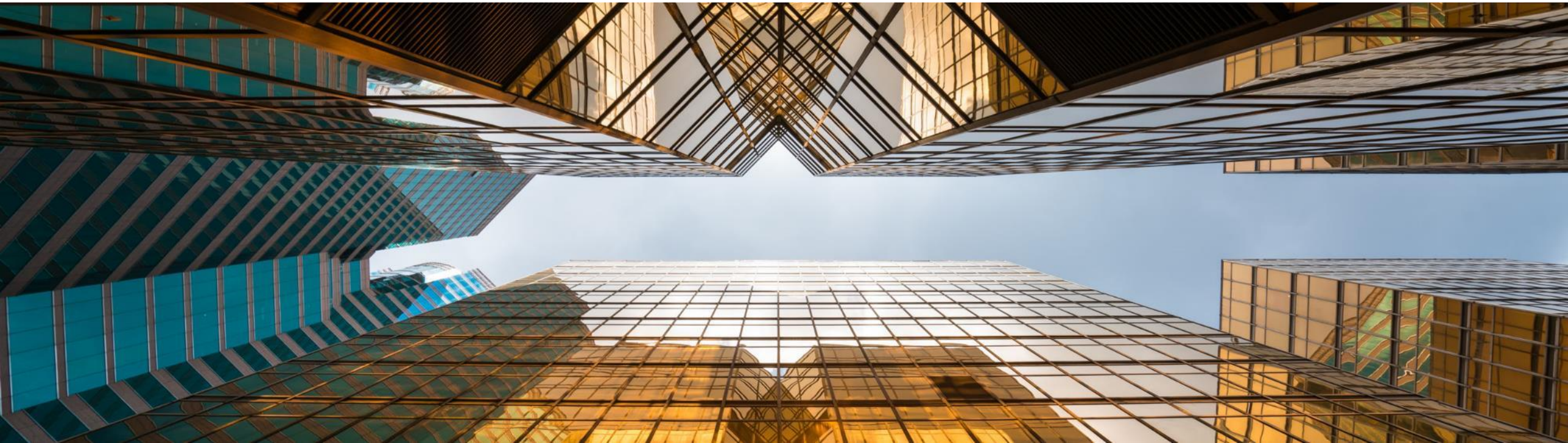
Basic Demo

SAP Enterprise Threat Detection



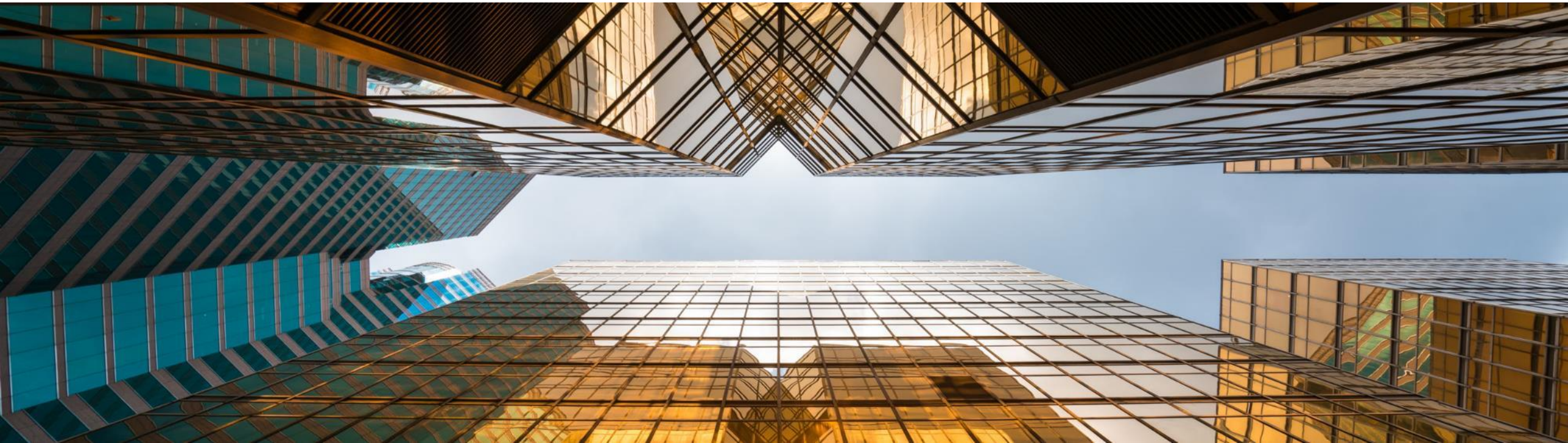
Demo of an Attack/Defend Scenario

SAP Enterprise Threat Detection



Organization for later Hands-On Sessions

SAP Enterprise Threat Detection



Organization for Hands-On Access

We provide several exercise systems with a maximum capacity of 20 participants

- Opening times until Friday, 3rd December, End of Business
- Opening times in your corresponding time zone at Std. working times
- **Interested participants, please send us a mail**
 - **We will then provide you the system connect and a dedicated user-id**

How to access the Exercise document: Later provided Link provides access to the exercises document:



Explore SAP Enterprise Threat Detection

This demo edition enables you to explore SAP Enterprise Threat Detection. You can analyze and monitor suspicious activities in the SAP S/4 HANA system or SAP HANA database, or making use of the log learning application.

- [SAP Enterprise Threat Detection: Exercises](#)
- [SAP Enterprise Threat Detection: Launchpad](#)

Note on browsers:

In case you want to use Google Chrome on the remote desktop, you can install it from [here](#).

When accessing the SAP Enterprise Threat Detection Launchpad on browsers, you will encounter browser messages about untrusted sites, unsecure connections, unknown certificate messages and continue (the messages show up since in this trial environment no trusted connection between browser and backend is configured unless you manually import a certificate).

Organization for Hands-On Access

Exercise Document

Secure the Intelligent Enterprise with SAP Enterprise Threat Detection

Exercise: Working with SAP Enterprise Threat Detection

TechEd Version 2021

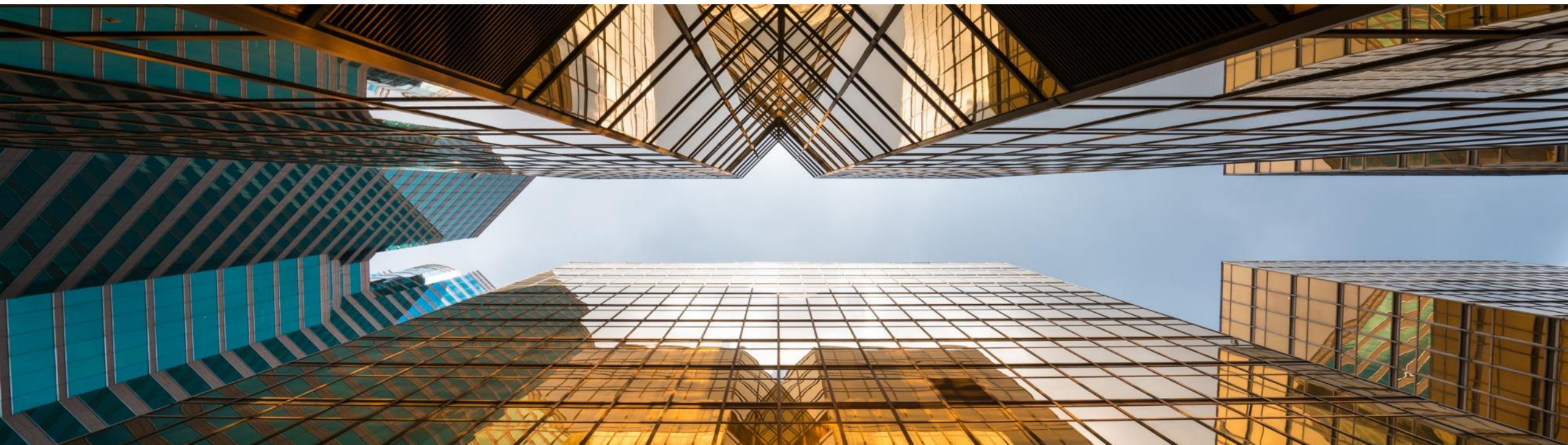
....

TABLE OF CONTENTS

1.	ETD USER – ETD ROUNDTrip AND NAVIGATION	3
1.1.	Start Page and Navigation to different tiles.....	3
1.2.	Summary.....	22
2.	SECURITY EXPERT - WORKING WITH THE FORENSIC LAB	22
2.1.	Filtering Data.....	23
2.2.	Modelling Charts.....	25
2.3.	Browse through the data and model your own individual charts.....	27
2.4.	Working with Value Lists.....	29
2.5.	Modeling Attack Detection Patterns	30
2.1.	Summary.....	35
3.	BROWSE, MODEL, AND ATTACK.....	35
3.1.	Create a Data Download Pattern and simulate the Attack	36
3.1.	Browse through the data and model your own individual Attack Detection Pattern.....	46
3.2.	Summary.....	46
4.	PROCESSING ALERTS AND INVESTIGATIONS.....	47
4.1.	Viewing Alerts.....	47

Q&A

SAP Enterprise Threat Detection



SAP TechEd learning offerings accelerate your career

Upskill to stand out of the crowd



Check learning.sap.com/teched to benefit like other certified experts:

26%

get promotions

+28%

more responsibilities

65%

greater self-confidence



Accelerate your SAP-expert career:



- Prepare for a certification in SAP BTP with **SAP Learning Journeys** and **scheduled live sessions**
- Stand out of the crowd with the **event-exclusive certification offer**



Expand your conference experience:



- Follow **learning recommendations for selected sessions** to help you drive business and career success
- Ask questions in the **SAP-moderated Learning Group for SAP TechEd** – also available after the event



Thank you.

Contact information:

Arndt Lingscheid

Solution Owner Security Products and GRC

SAP SE Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany

Mail: a.lingscheid@sap.com

Contact information:

Dr. Michael Schmitt

Product Manager SAP Enterprise Threat Detection

SAP SE Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany

Mail: m.schmitt@sap.com

Follow us



www.sap.com/contactsap

© 2021 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 for additional trademark information and notices.