TechEd 2021: IIS161
Protect the Intelligent Enterprise with SAP Enterprise Threat Detection

Arndt Lingscheid, Michael Schmitt
11, 2021

PUBLIC

THE BEST RUN SAP

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

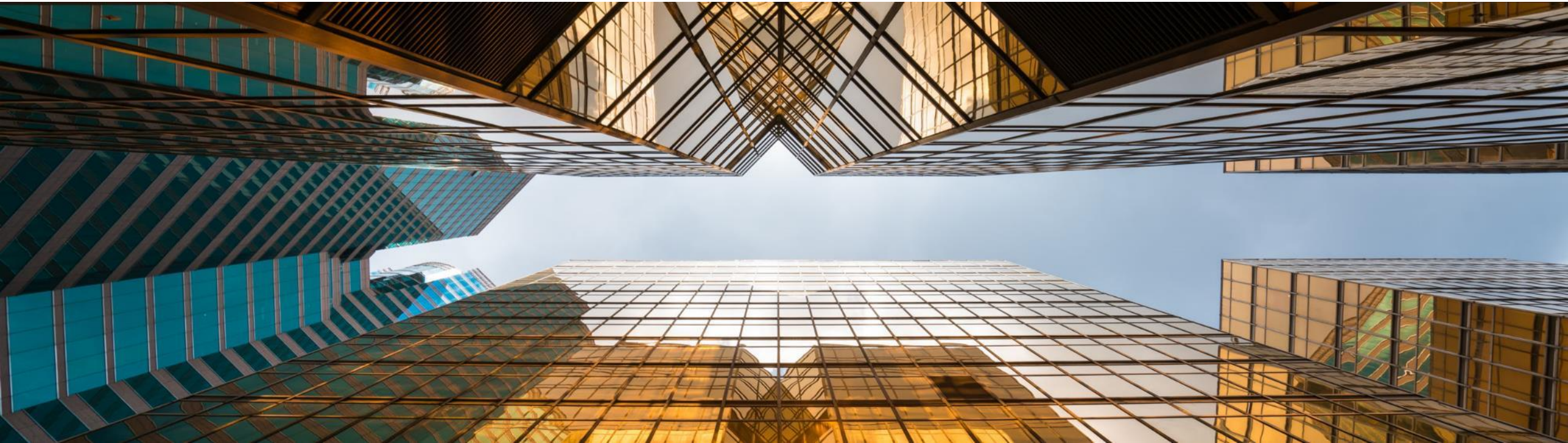
- Attack scenarios in an S4H system
- Detection in ETD

Organization for later self-paced hands-on

- Details for Subscription

Q&A

Introduction to
SAP Enterprise Threat Detection



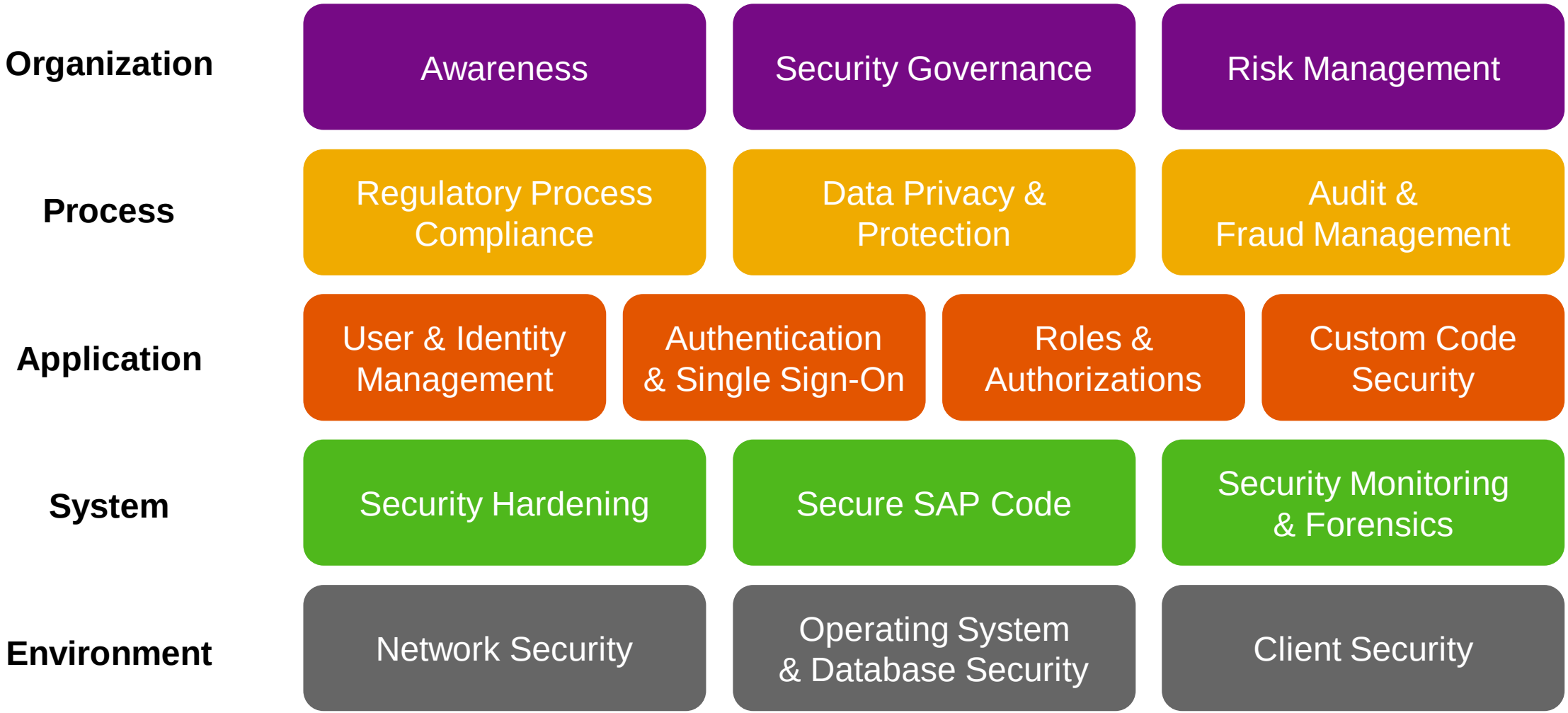

Systems are under attack

Sobering Statistics

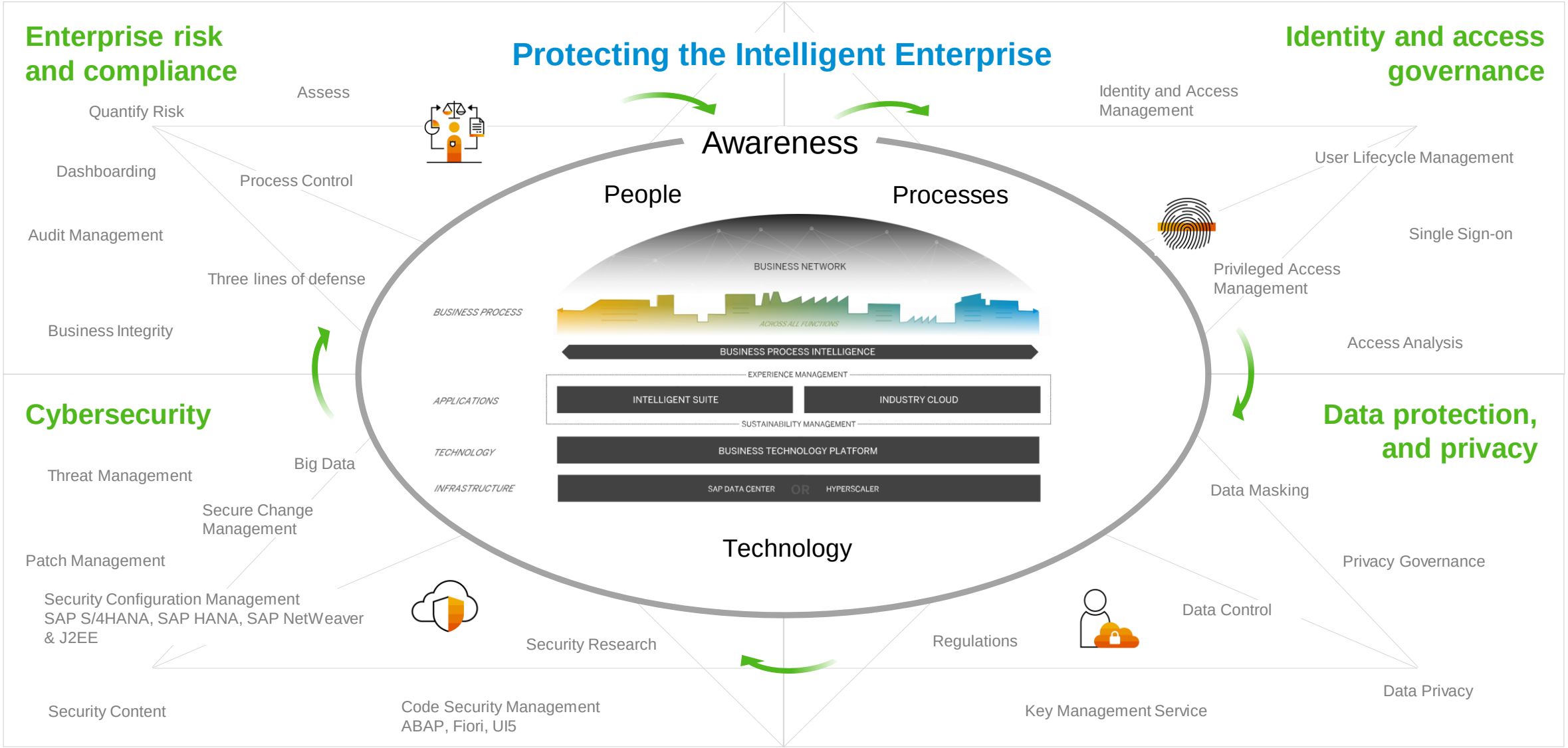
- Businesses that had not deployed security automation saw an average total cost of **$6.03 million**, more than double the average cost of a data breach of **$2.45 million** for businesses that had fully deployed security automation.
- **$5.52** million average total cost of a breach at enterprises 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

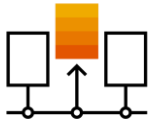


Cybersecurity- and Compliance Solutions from SAP based on NIST

Identify

Protect

Detect



Respond

Recover

Identify	Protect	Detect	Respond	Recover
Architecture & Planning services	Empowerment Services	Execution & Implementation Services	Continuous Improvement Services	Security experts
SAP EarlyWatch Alert		SAP Enterprise Threat Detection		Managed Service via ETD
	UI data protection masking & logging			
SAP Configuration Validation		Business Integrity Screening		
SAP System Recommendations				
SAP Focused Run				
ABAP test cockpit & SAP Code Vulnerability Analyzer				
SAP Fortify by Micro Focus				
	Single Sign-On			
	User & Identity Management			
	Access Management			
	SAP Data Custodian			

- 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 an hacker attack, not only a few small puzzle peace's.
- Perform forensic investigations, search for threats and detect anomalies in SAP S/4HANA applications.
- All audit logs available in a central instance (manipulation save, 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.

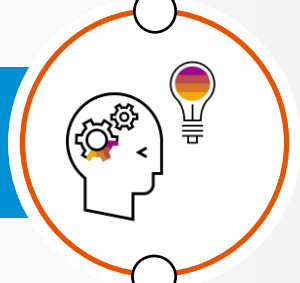
Security Audit Log compliance

Challenge

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

Incompliant

Solution



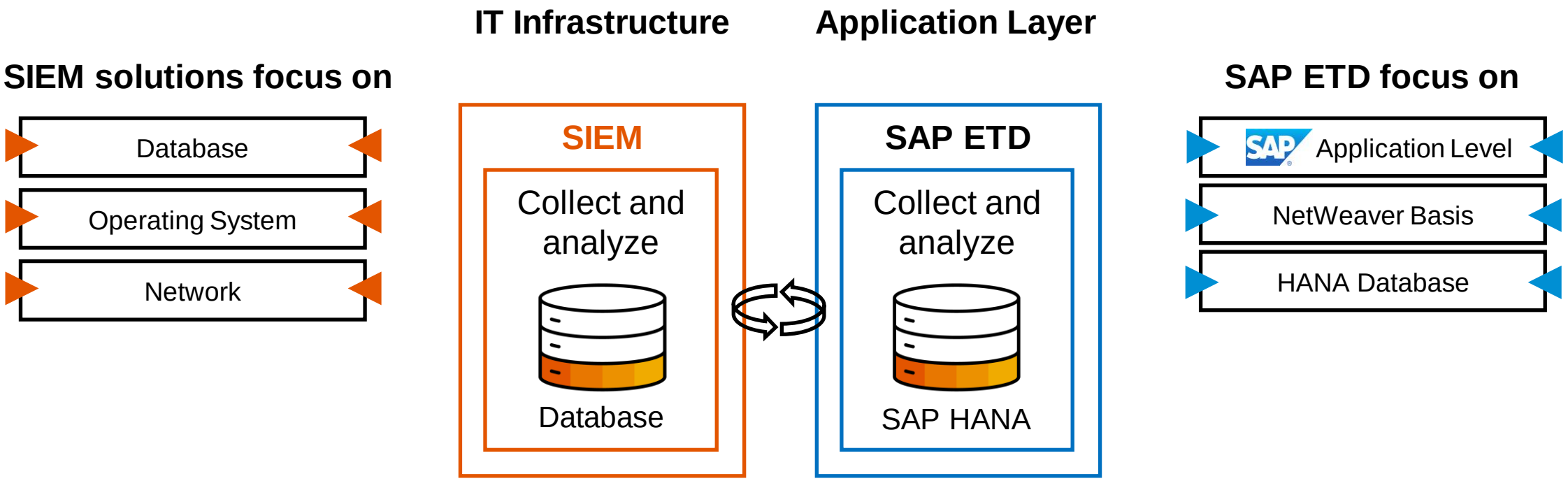
- Direct transfer of all information belonging to the Security Audit log to SAP Enterprise Threat Detection

Benefits

- 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



Continue use of proven security incident reporting

+

Real time monitoring of business critical SAP applications & data

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

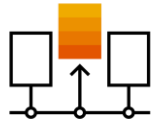
Protective Technology

Detect

Anomalies and Events

Continuous Security Monitoring

Detection Processes



Respond

Response Planning

Communications

Analysis

Mitigation

Improvements

Recover

Recovery Planning

Improvements

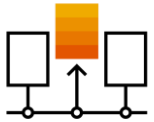
Communications

Cybersecurity- and Compliance Solutions from SAP based on NIST

Identify

Protect

Detect



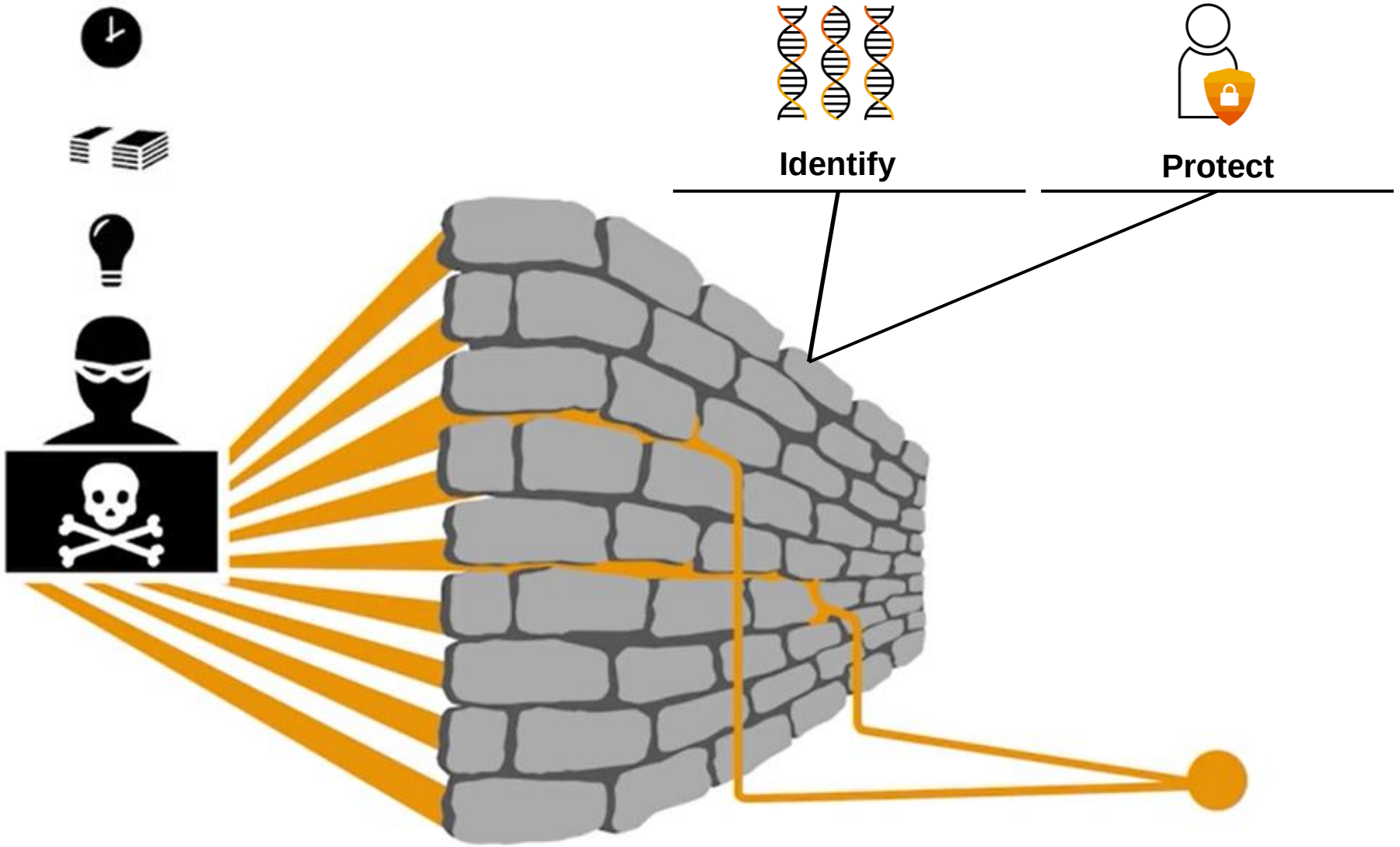
Respond

Recover

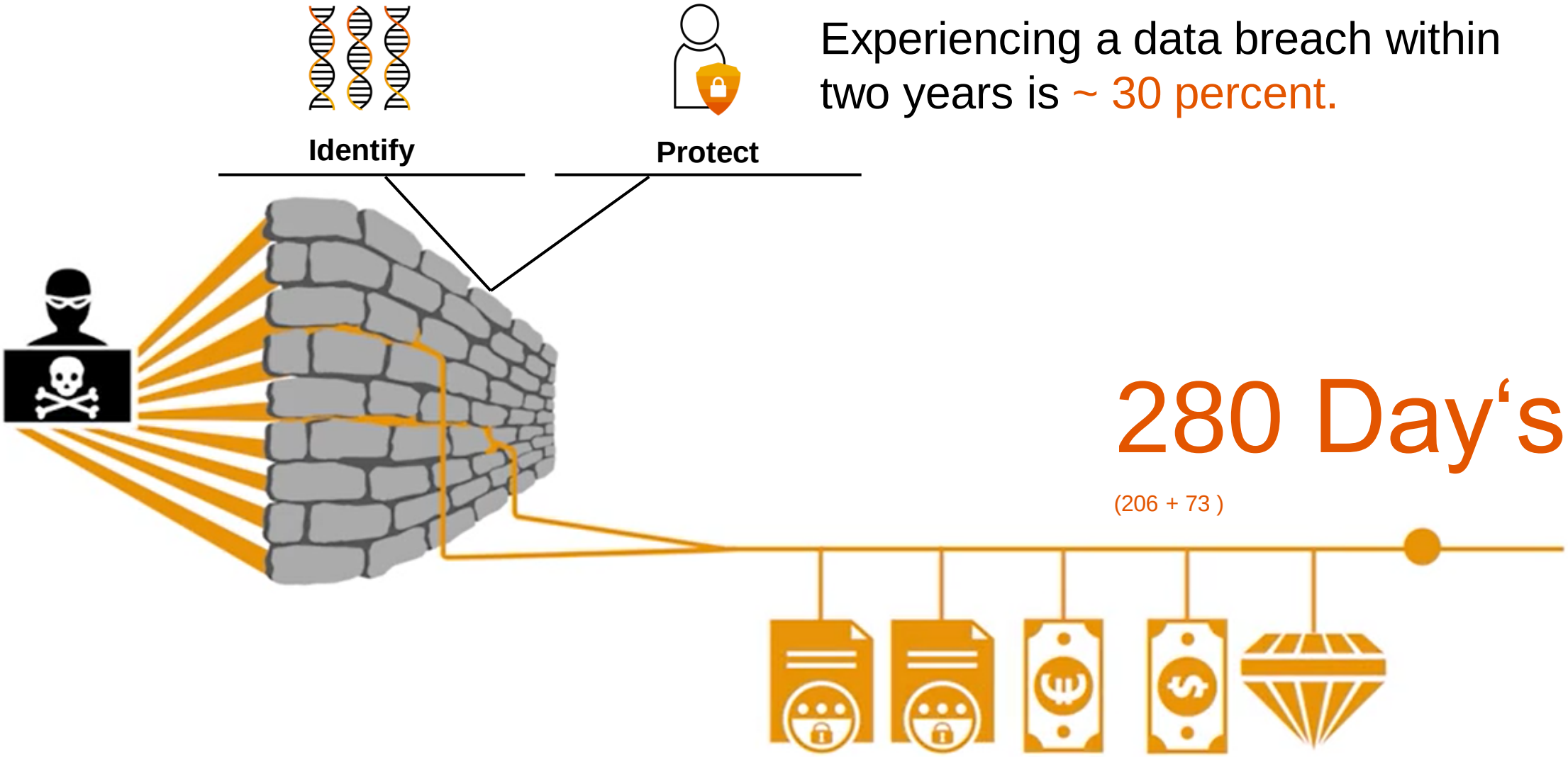
Identify	Protect	Detect	Respond	Recover
Architecture & Planning services	Empowerment Services	Execution & Implementation Services	Continuous Improvement Services	Security experts
SAP EarlyWatch Alert		SAP Enterprise Threat Detection		Managed Service via ETD
	UI data protection masking & logging			
SAP Configuration Validation		Business Integrity Screening		
SAP System Recommendations				
SAP Focused Run				
ABAP test cockpit & SAP Code Vulnerability Analyzer				
SAP Fortify by Micro Focus				
	Single Sign-On			
	User & Identity Management			
	Access Management			
	SAP Data Custodian			

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

SAP Enterprise Threat Detection



SAP Enterprise Threat Detection

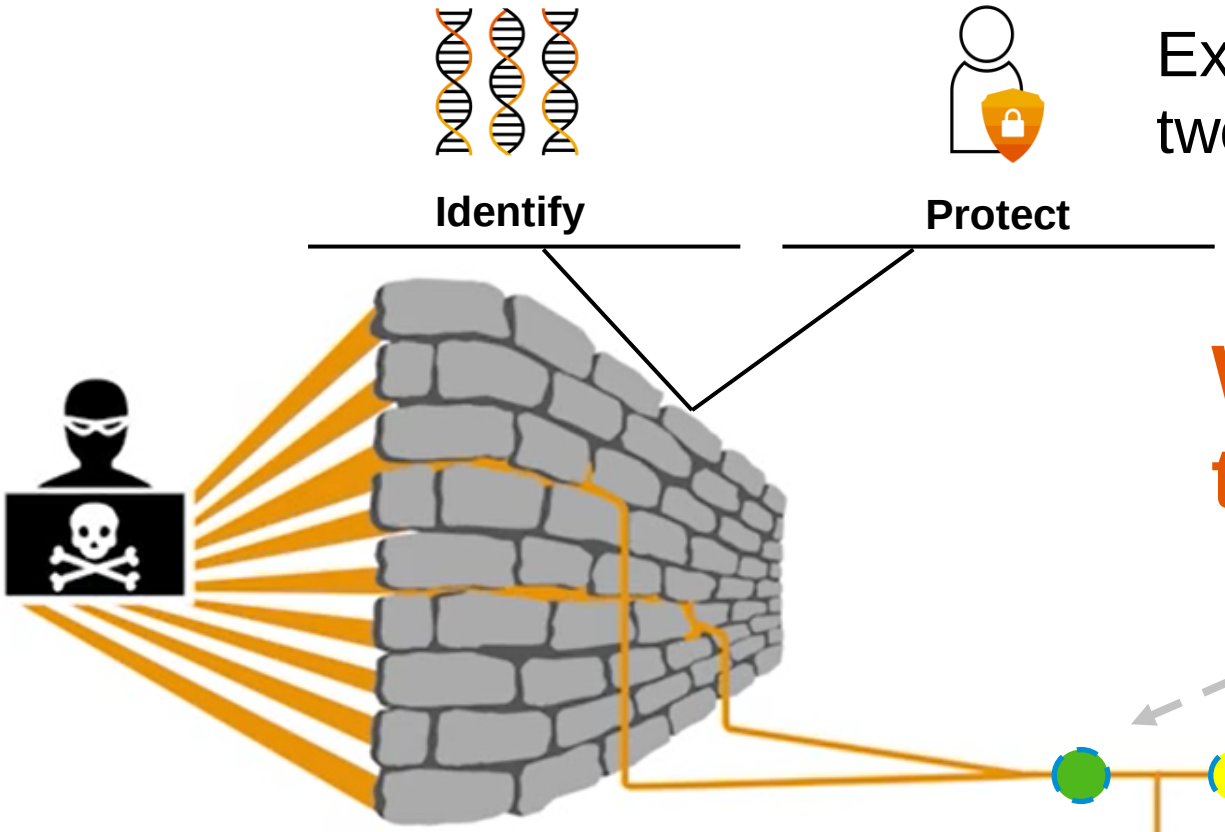


Experiencing a data breach within two years is ~ 30 percent.

280 Day‘s

(206 + 73)

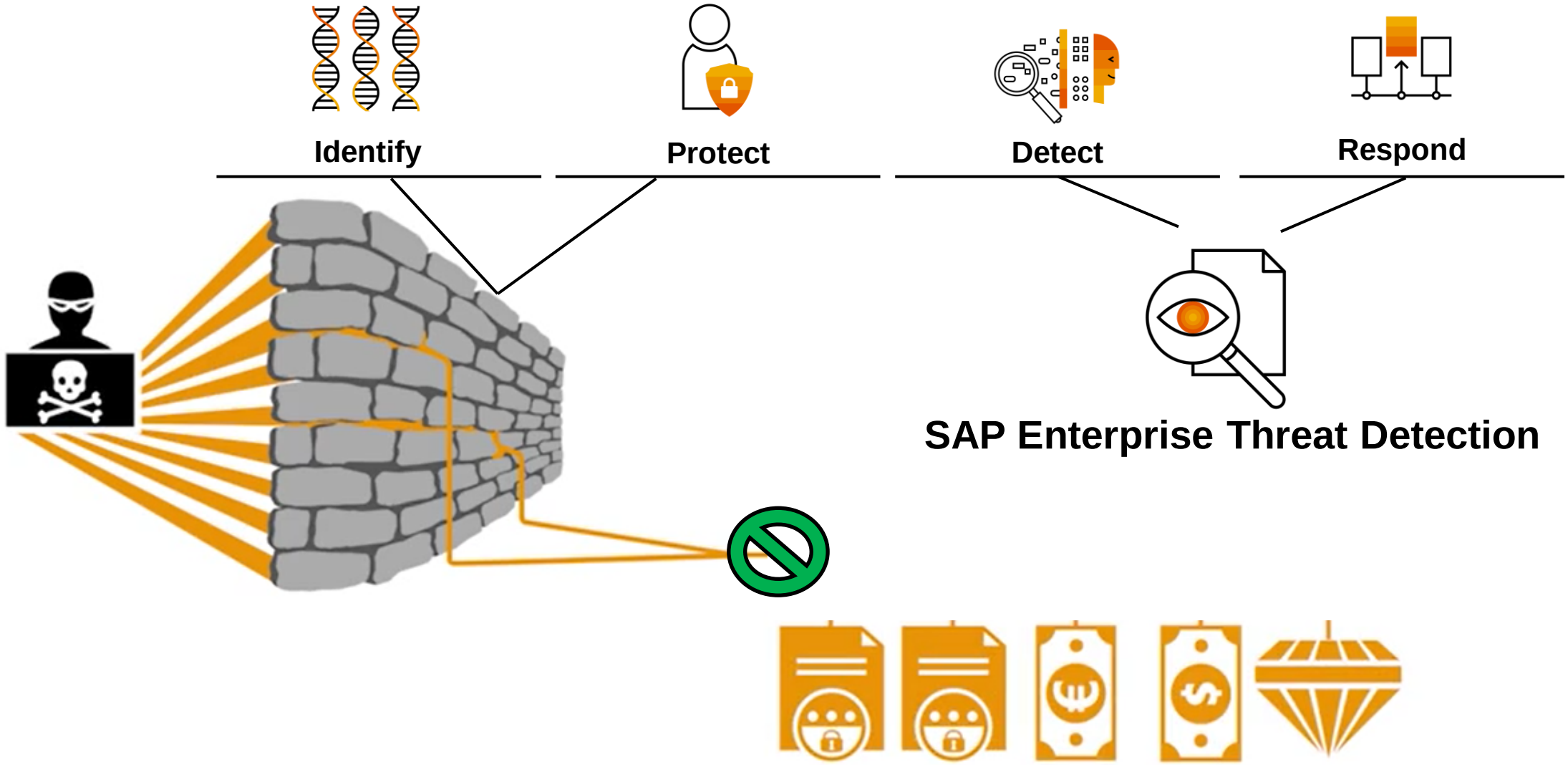
SAP Enterprise Threat Detection



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

When are you able to stop a breach ?

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

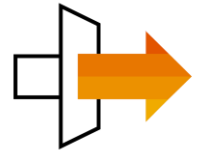
Debugging DEV System

Discover SM59 connections

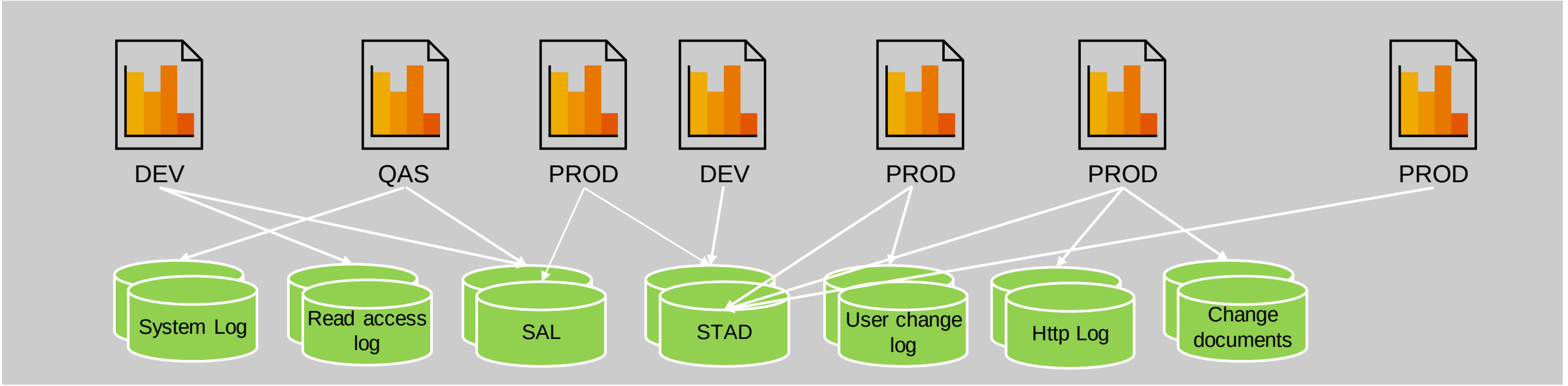
RFC to change passwd

Change vendor

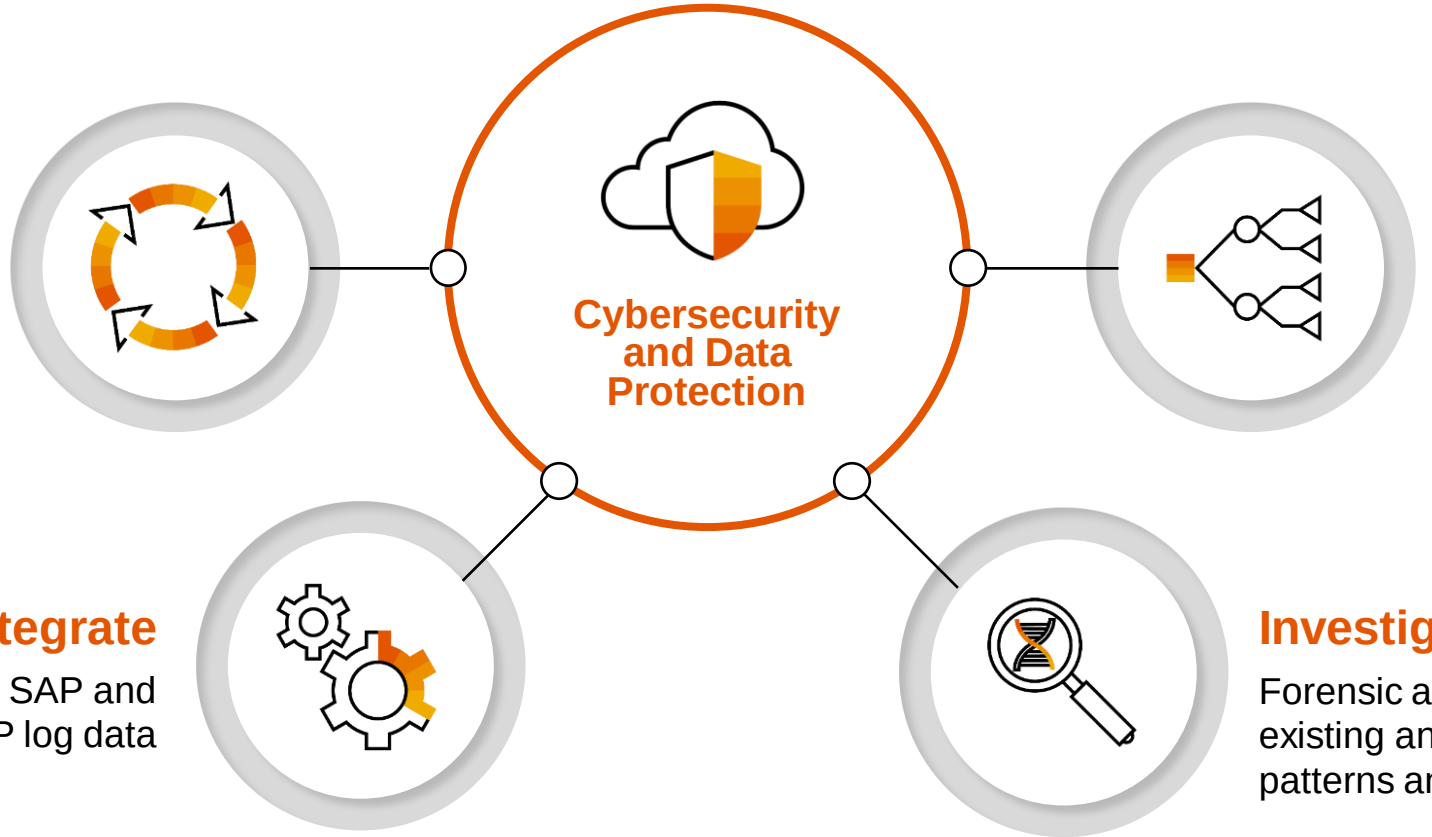
Outgoing payments



01.2020 | 06.2020 | 03.2021



How does SAP Enterprise Threat Detection work



Analyze

Efficiently enrich, analyze, and correlate logs

Evaluate

Automatically evaluate attack detection patterns with real-time alerting

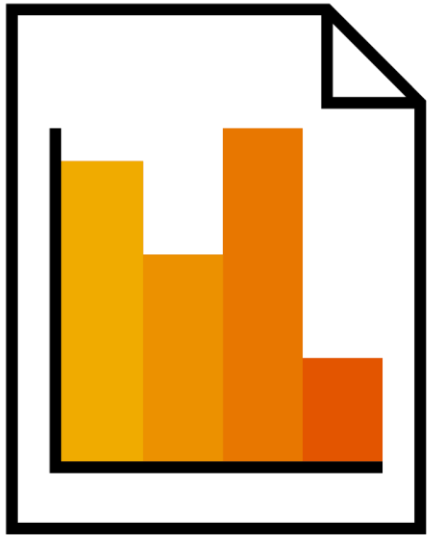
Integrate

Integration of SAP and non-SAP log data

Investigate

Forensic analysis and modeling of existing and new attack detection patterns and dashboards

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

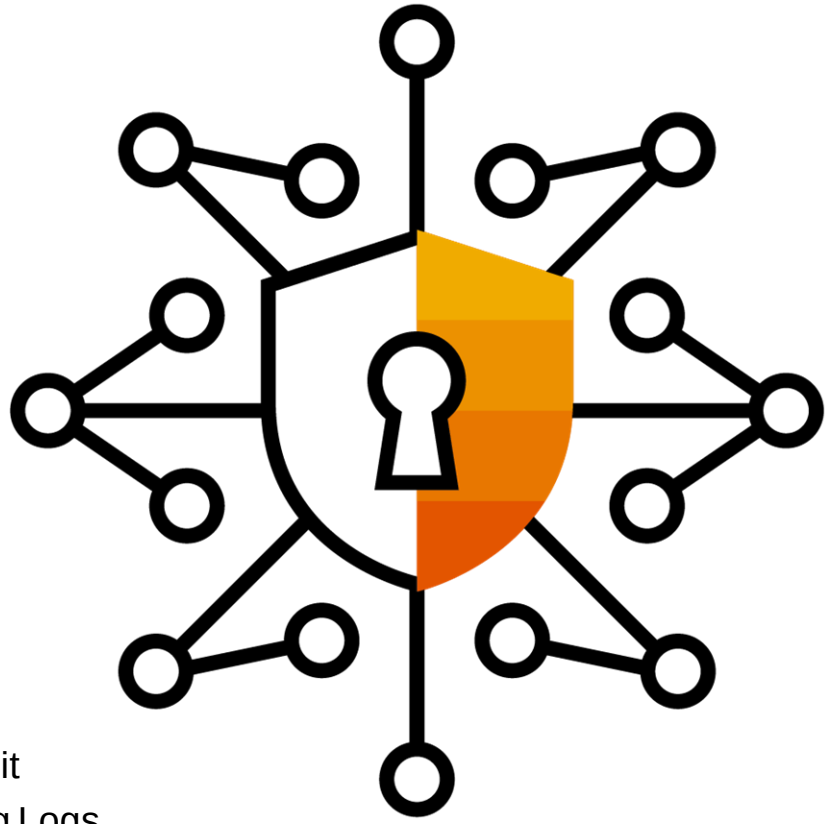
- AuditD

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

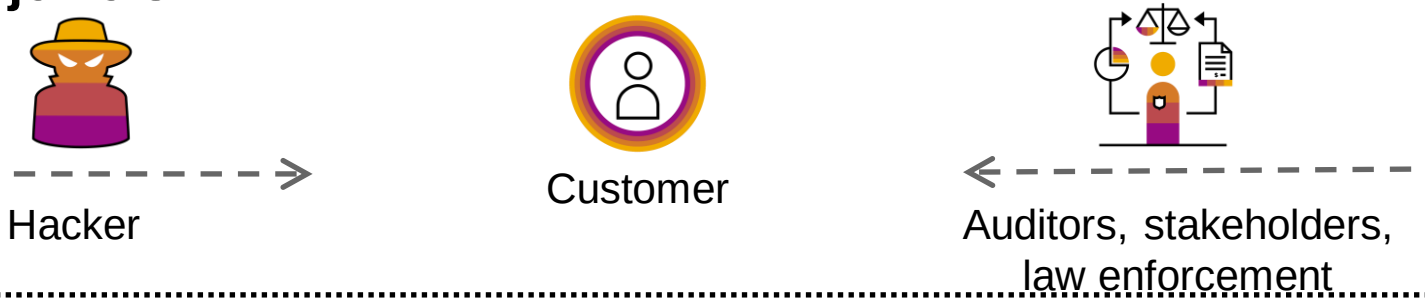
Different datacenters* | Local Service provision* | Language: English

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

** Planned in Q2 2022
*** currently 5x8, 7x24 Planned in Q4 2022

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

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

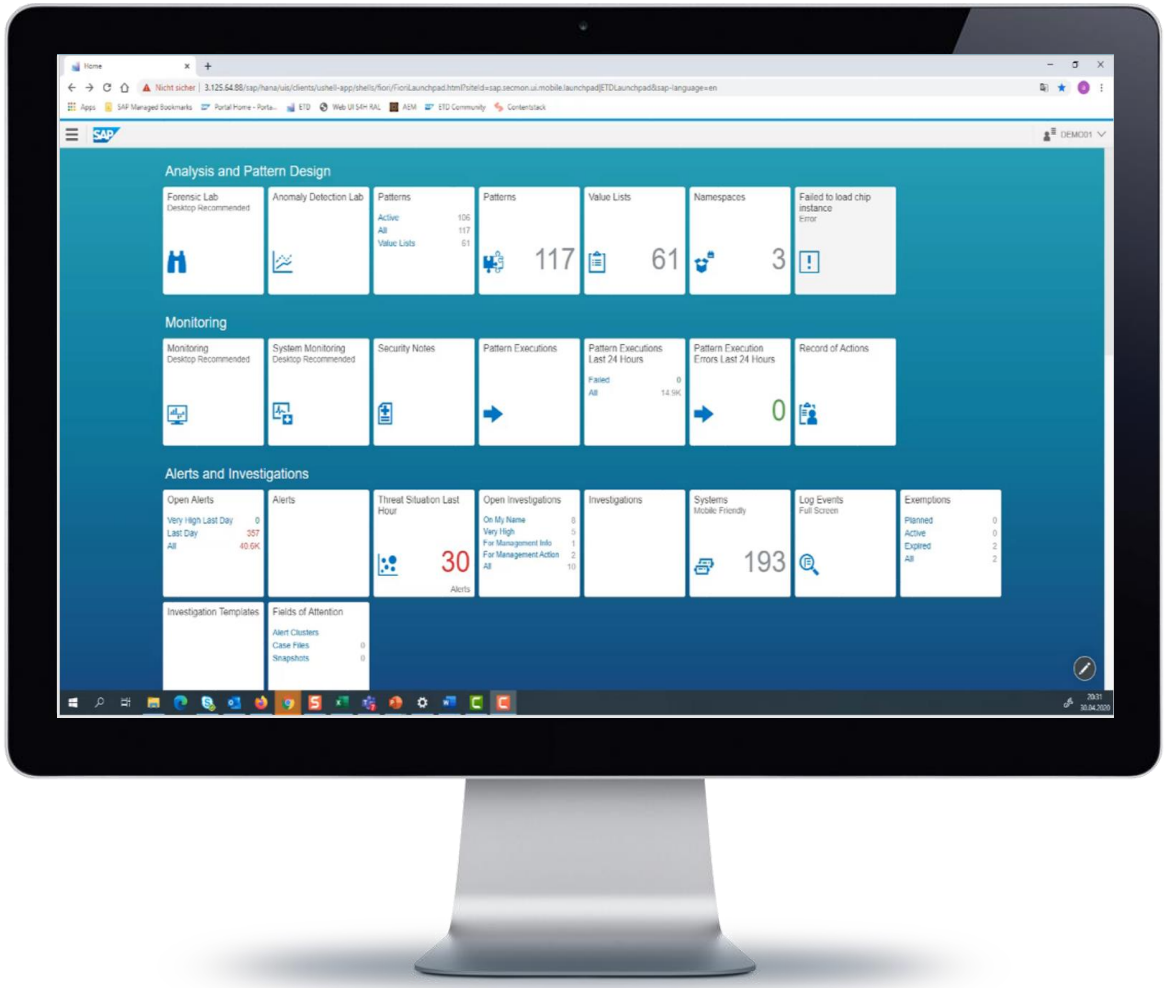
** Planned in Q2 2022
*** currently 5x8, 7x24 Planned in Q4 2022

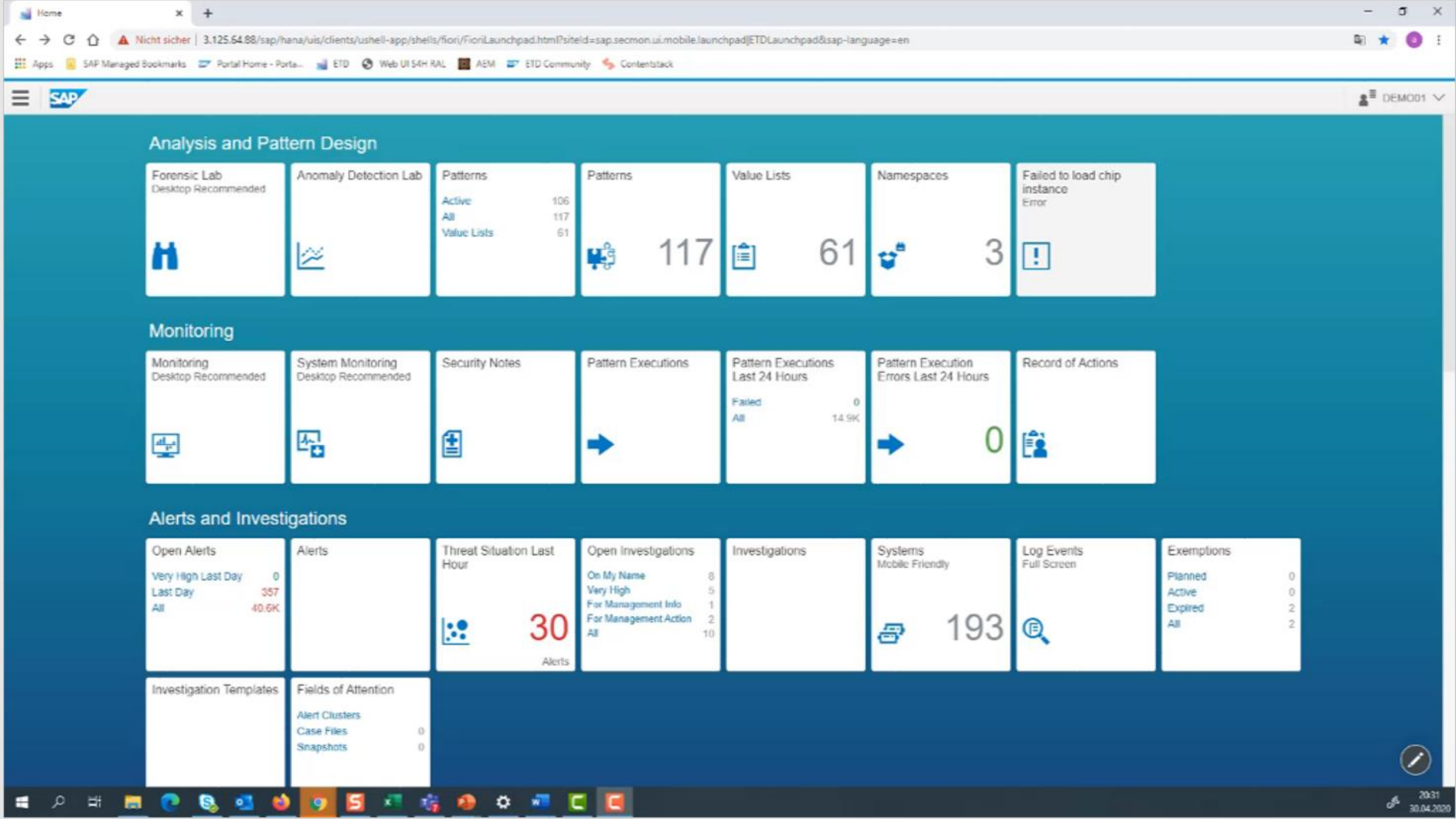
Protecting the crown jewels

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

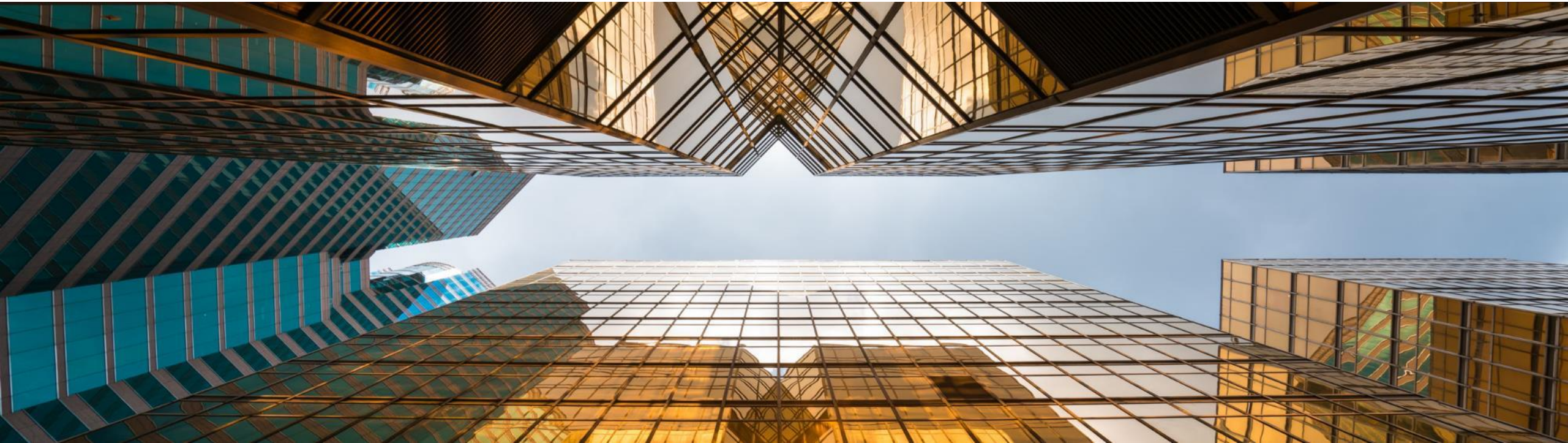
SAP Enterprise Threat Detection




Home
Nicht sicher | 3.125.64.88/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad&sap-language=en
Apps
SAP Managed Bookmarks
Portal Home - Porta...
ETD
Web UI S4H RAL
AEM
ETD Community
Contentstack
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

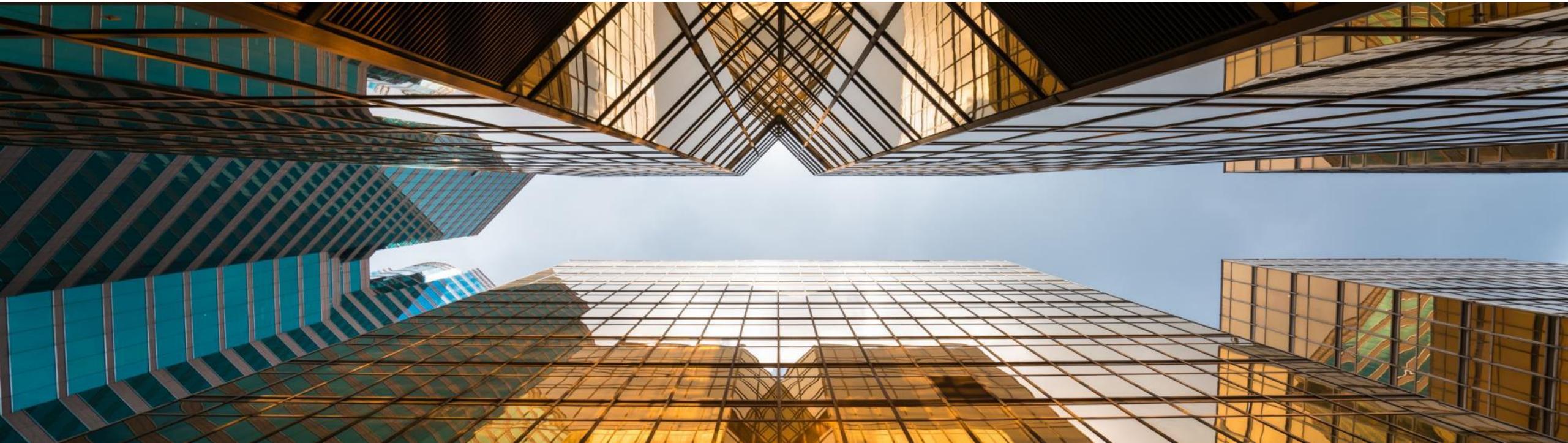
Basic Demo

SAP Enterprise Threat Detection



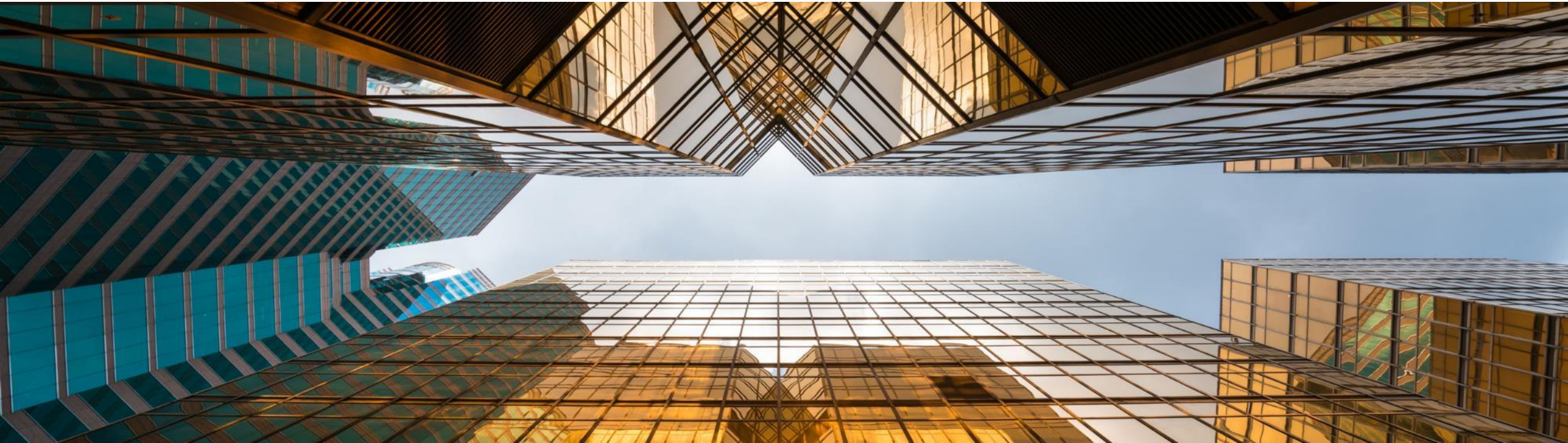
Demo of an Attack/Defend Scenario

SAP Enterprise Threat Detection



Organization for self-paced Hands-On

SAP Enterprise Threat Detection



Organization for self-paced Hands-On Access

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

- Opening times until Friday, 26th November, End of Business
- Opening times in your corresponding time zone at Std. working times

- **Interested participants, please send us a mail with your time zone**
  - **We will then provide you the system connect and a dedicated user-id via mail**

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

Additional information:

- **Please only use your user, don't lock/change other users!**
- **Please don't destroy the system!** You explicitely have high priviledges to simulate attacks, don't miss-use those
- As browser, please use Google, Firefox, or Microsoft Edge on Chromium basis
- The HTTPs connect might lead to a page which tells about a wrong certificate handling and an insecure connect. This is due to missing certificates your End User machine settings, we did not provide. The data exchange is nevertheless encypted. Please ignore the warning and continue to the Web page (goto advanced and continue)

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

....

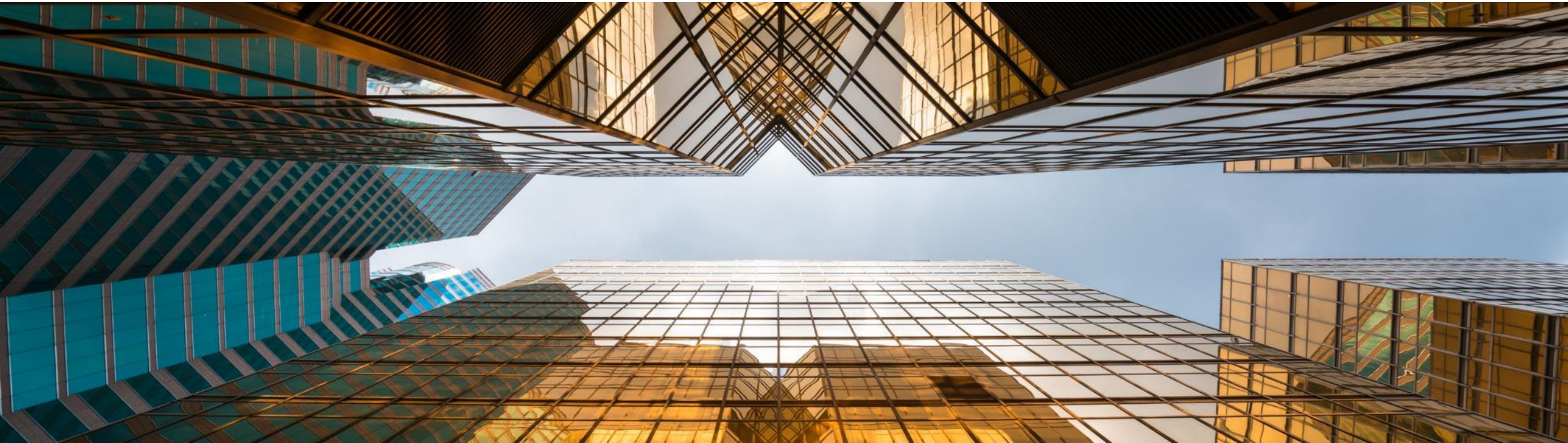
TABLE OF CONTENTS

Organization for self-paced Hands-On Access

In case of issues:

- We cannot guarantee that the connect to the environment works from every place in the world. E.g. your company might not allow ‘insecure’ browser connects, or the call of SAP Logon to a system outside your company. In that case, you cannot execute the exercises. However, you should be able to download the Exercises PDF from github to be able to read through.
- In case of questions related to the exercises, please send a mail.

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

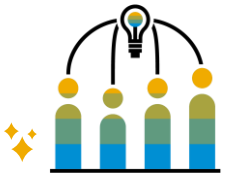
+28%
more responsibilities

65%
greater self-confidence

Accelerate your SAP-expert career:

FREE

- 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:

FREE

- Follow **learning recommendations for selected sessions** to help you drive business and career success

FREE

- Ask questions in the **SAP-moderated Learning Group for SAP TechEd** – also available after the event

** Pearson VUE, Study Reveals the Ever-Advancing Global IT Industry Requires the Backbone of Certification, 2019*

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

THE BEST RUN SAP®