High-performance threat analytics protecting SAP S/4 HANA applications

Arndt Lingscheid
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.

SAP cyber security and data protection solutions

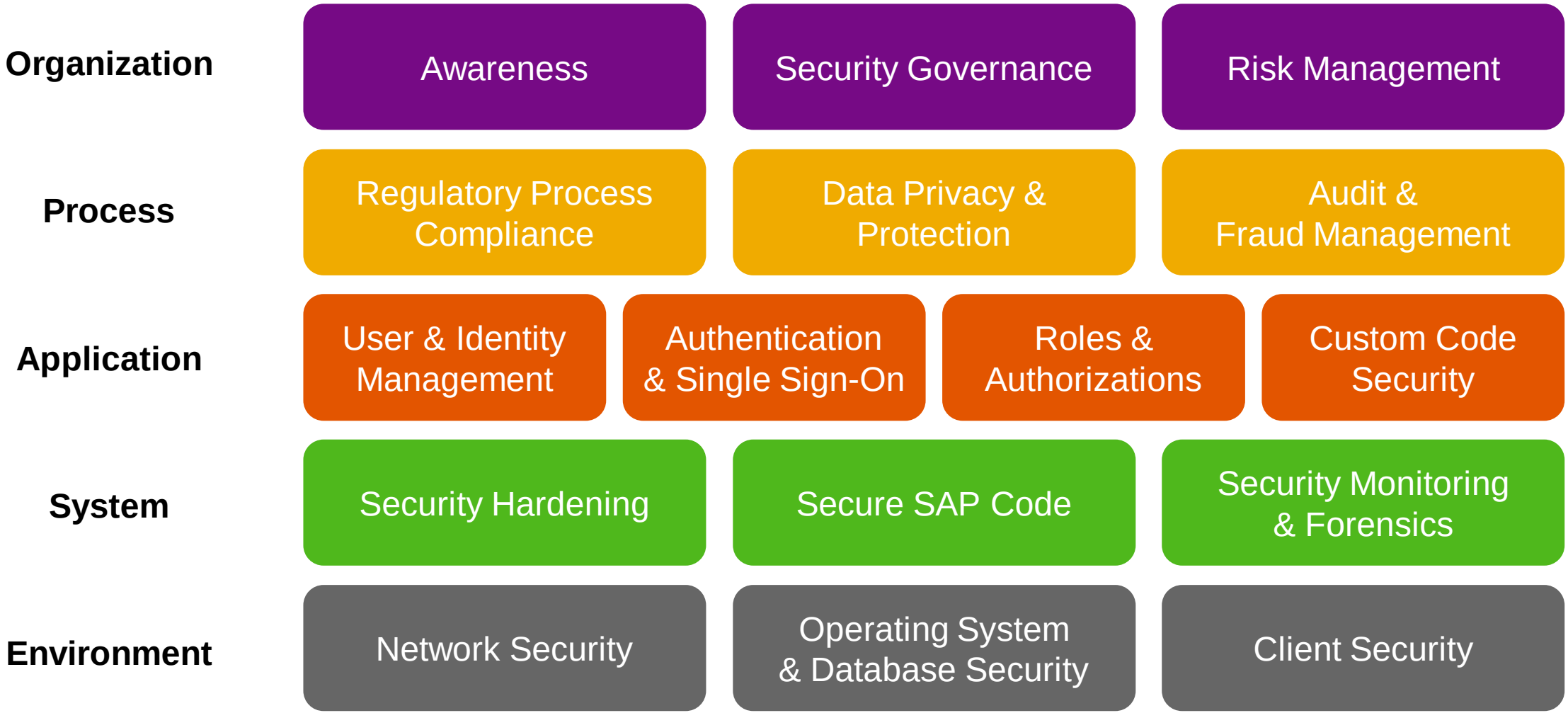

Systems are under attack

Sobering Statistics

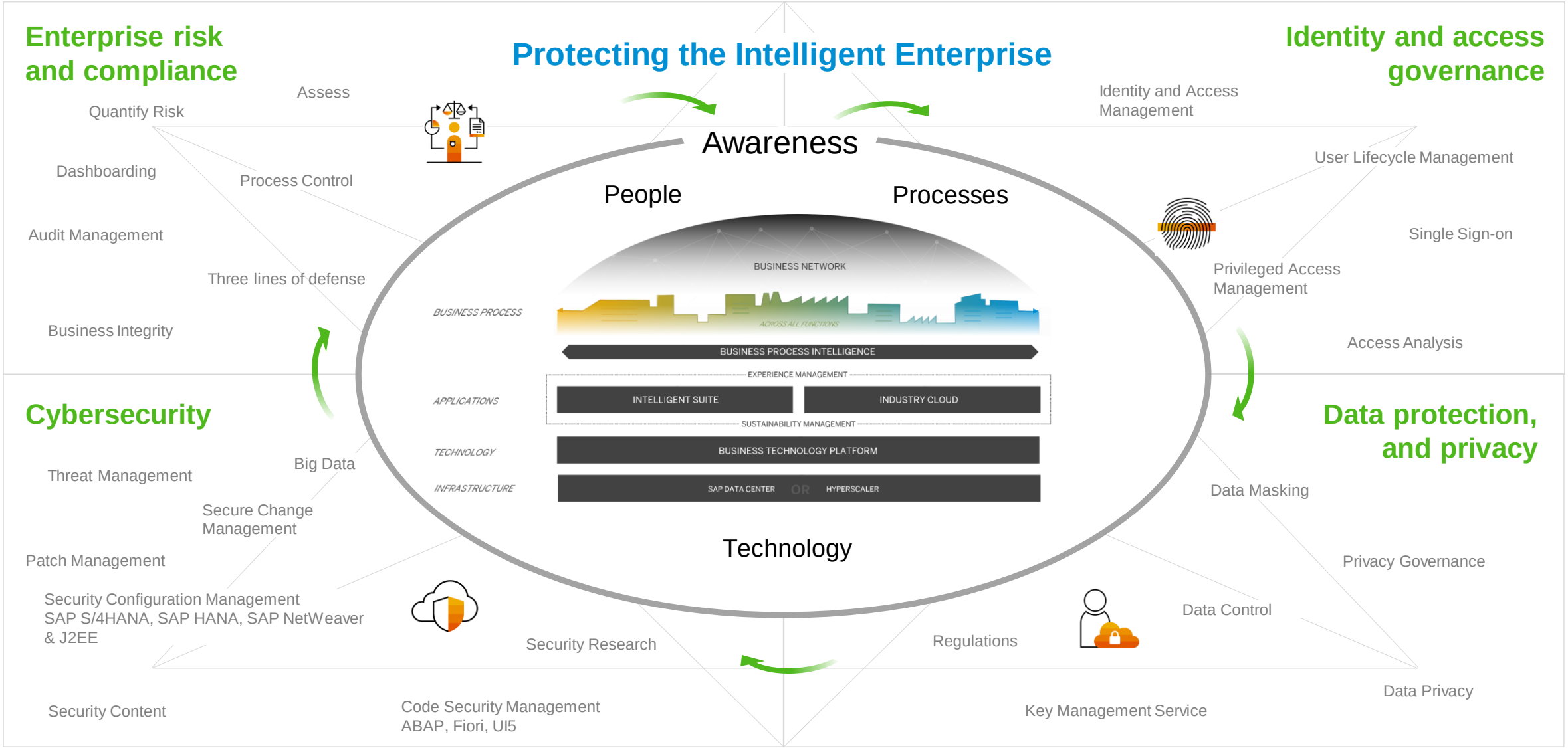
- Businesses that had not deployed security automation saw an average total cost of **$6.03 million**, more than double the average cost of a data breach of **$2.45 million** for businesses that had fully deployed security automation.
- **$5.52** million average total cost of a breach at enterprises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

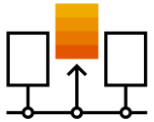


Cybersecurity- and Compliance Solutions from SAP based on NIST

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.

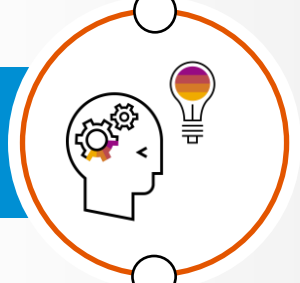
Security Audit Log compliance

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

Processing all SAP log events in a non-SAP SIEM solution

Challenge

- Tremendous costs since other SIEM solutions are licensed based on the log volume.
- Log implementation projects since the semantic understanding must be implemented in SIEM solution.

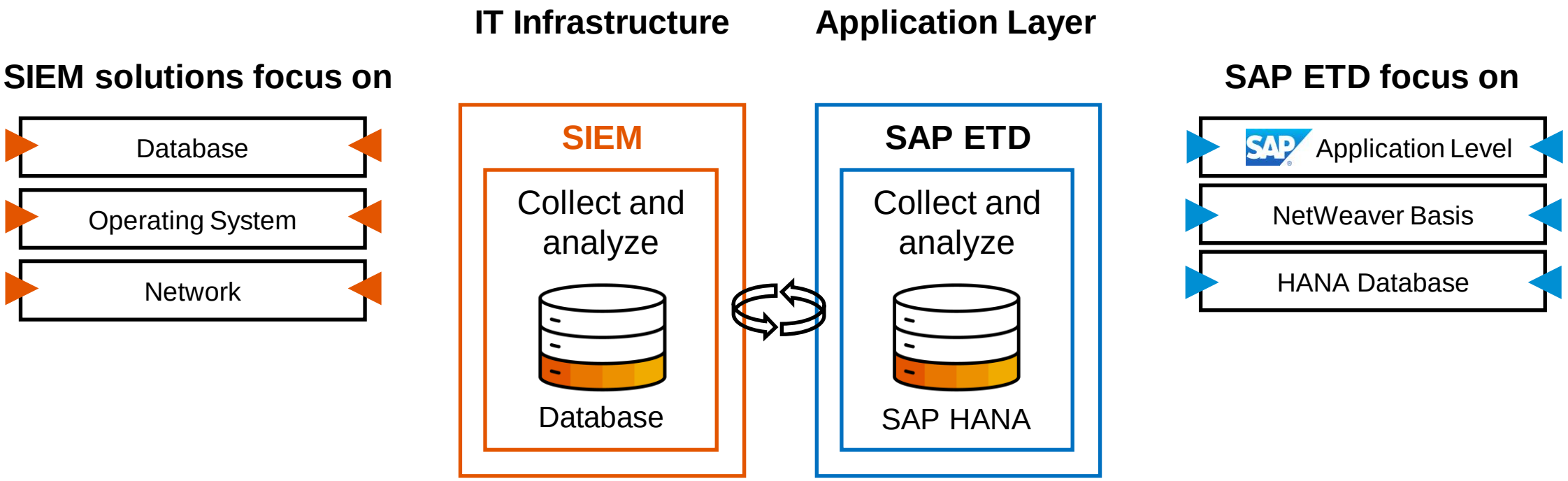
Solution

- Use SAP Enterprise Threat Detection.
- License is based on monitored users.
- SAP delivers the semantic understanding as pre-defined patterns.

Benefits

- SAP Enterprise Threat Detection gives transparency to the inside of the application layer out of the box.
- SAP Enterprise Threat Detection saves costs analyzing a huge amount of log data.
- SAP Enterprise Threat Detection bridges the gap between IT infrastructure monitoring an in application monitoring of the SAP applications.

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

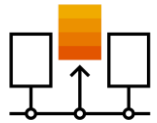
Protective Technology

Detect

Anomalies and Events

Continuous Security Monitoring

Detection Processes



Respond

Response Planning

Communications

Analysis

Mitigation

Improvements

Recover

Recovery Planning

Improvements

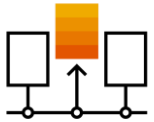
Communications

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			

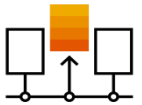
- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

Solutions for Control & Insight | Process Control | Risk Management | SAC Cybersecurity Dashboard | SAP Privacy Governance

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
- Authorizations
- Encryption
- HANA Data Masking
- HANA Data Anonymization

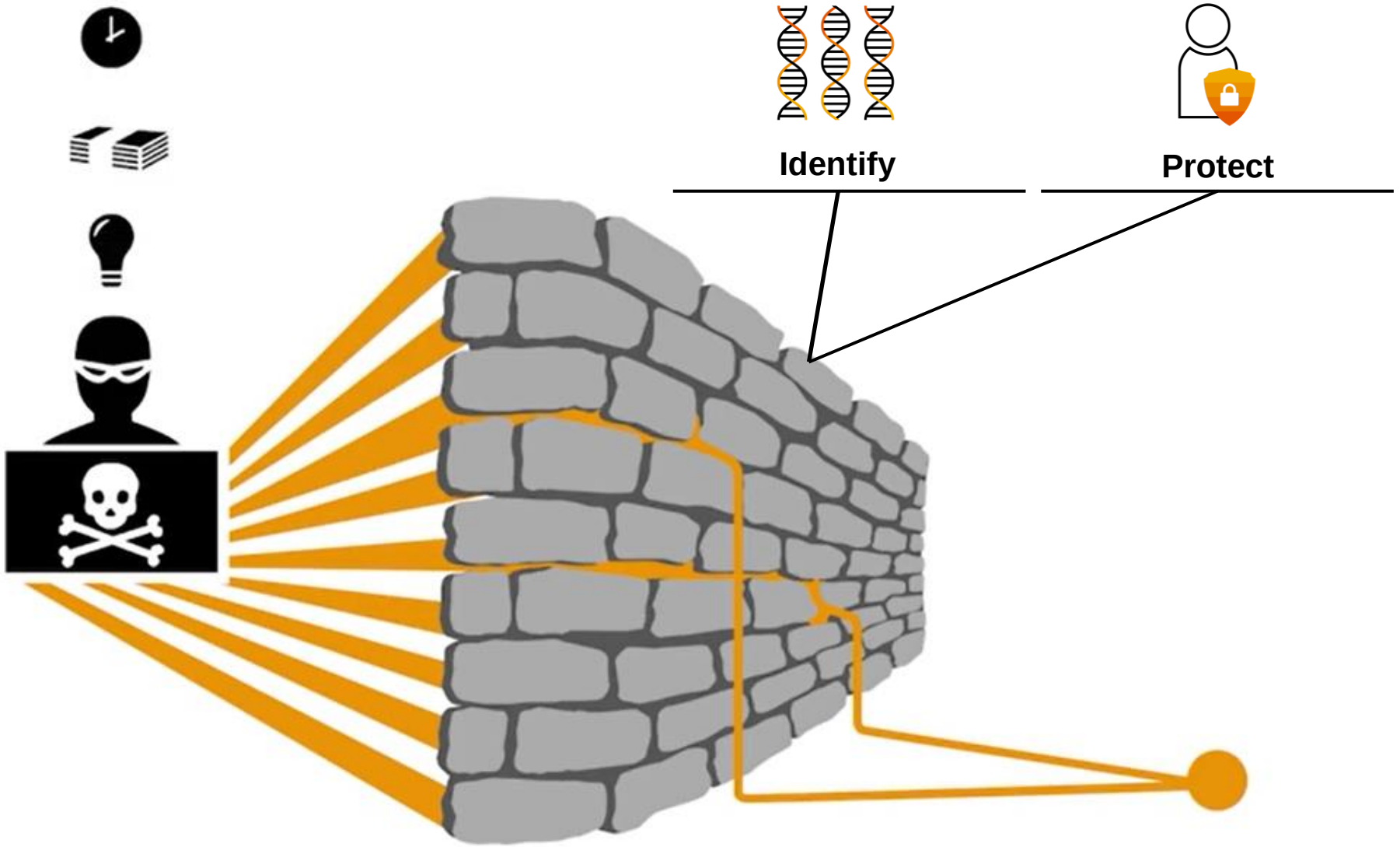
HANA Data Privacy Option

SAP Application layer

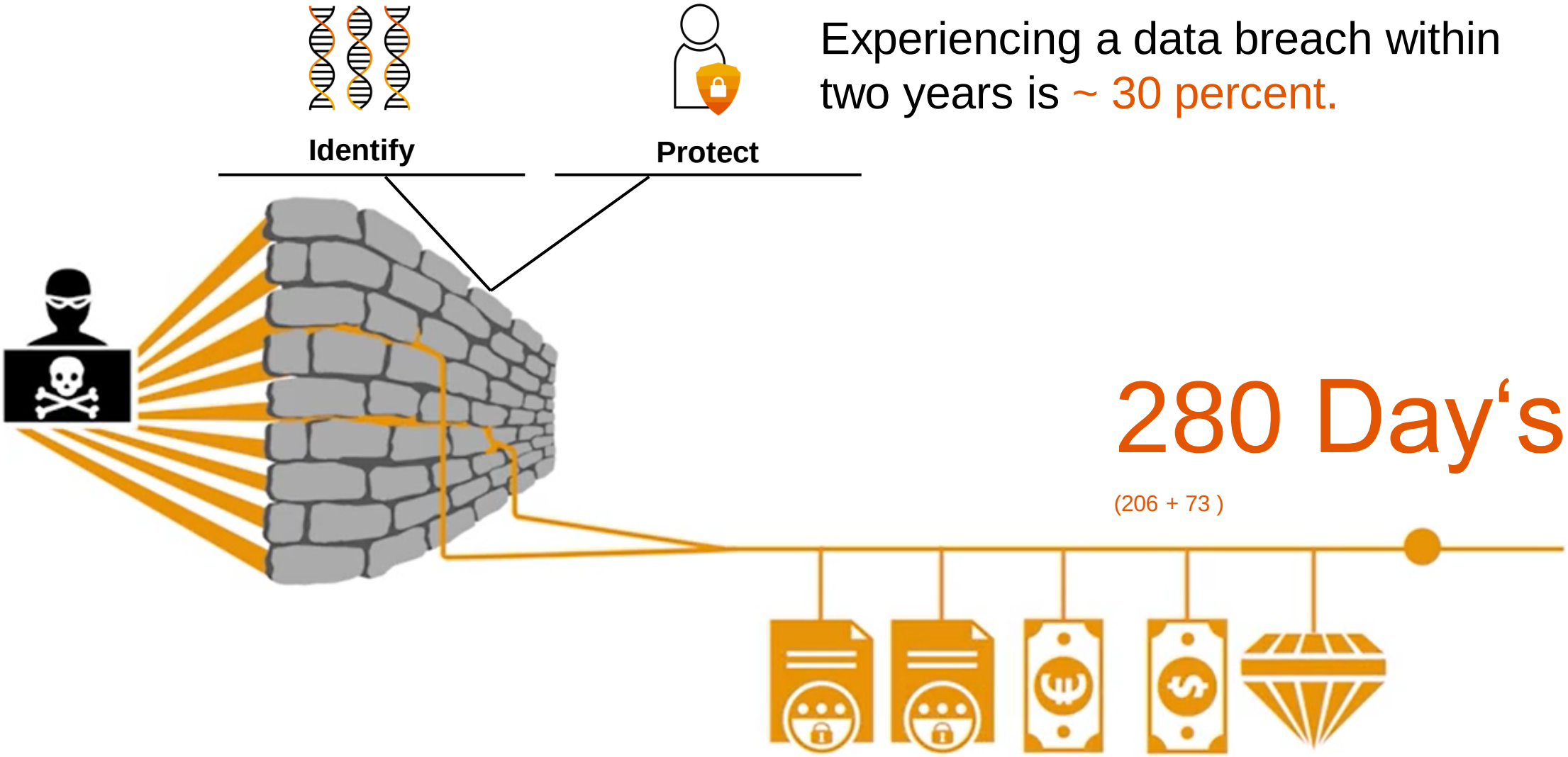
SAP HANA Platform

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

SAP Enterprise Threat Detection



SAP Enterprise Threat Detection

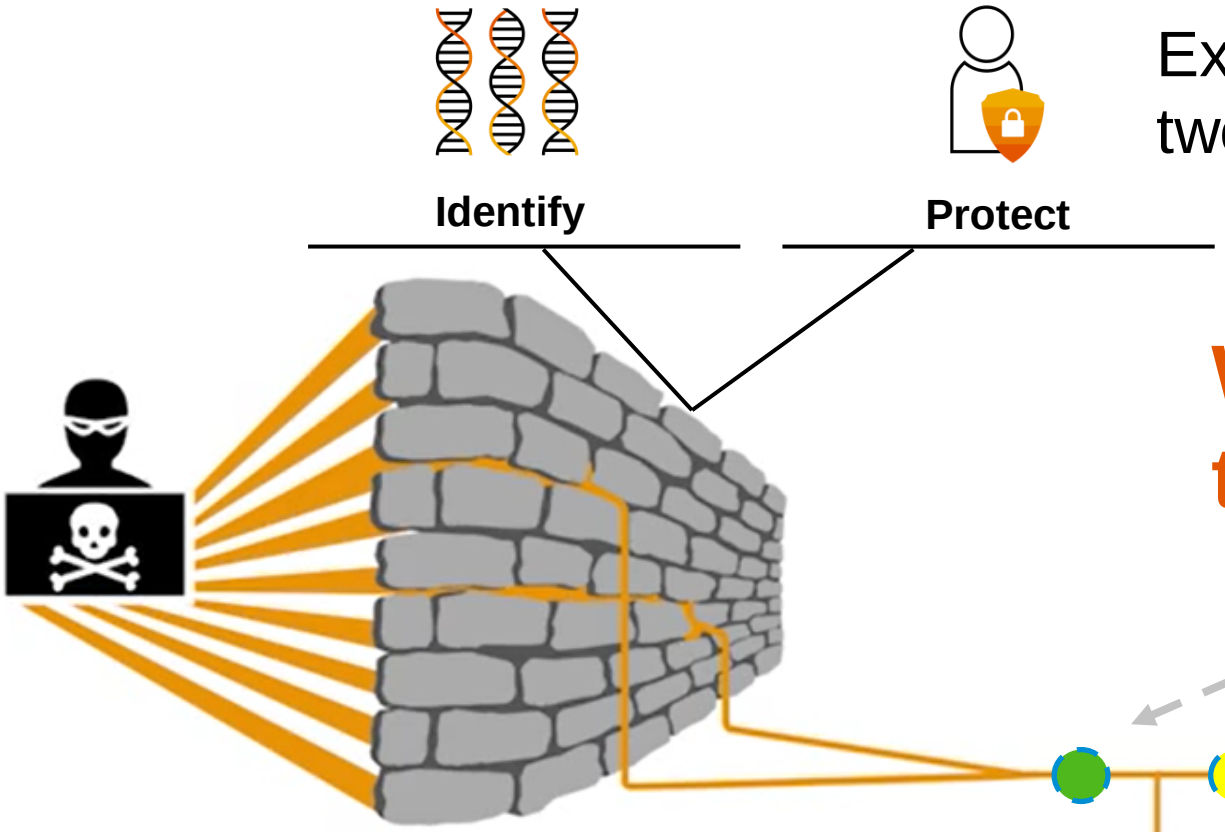


Experiencing a data breach within two years is ~ 30 percent.

280 Day‘s

(206 + 73)

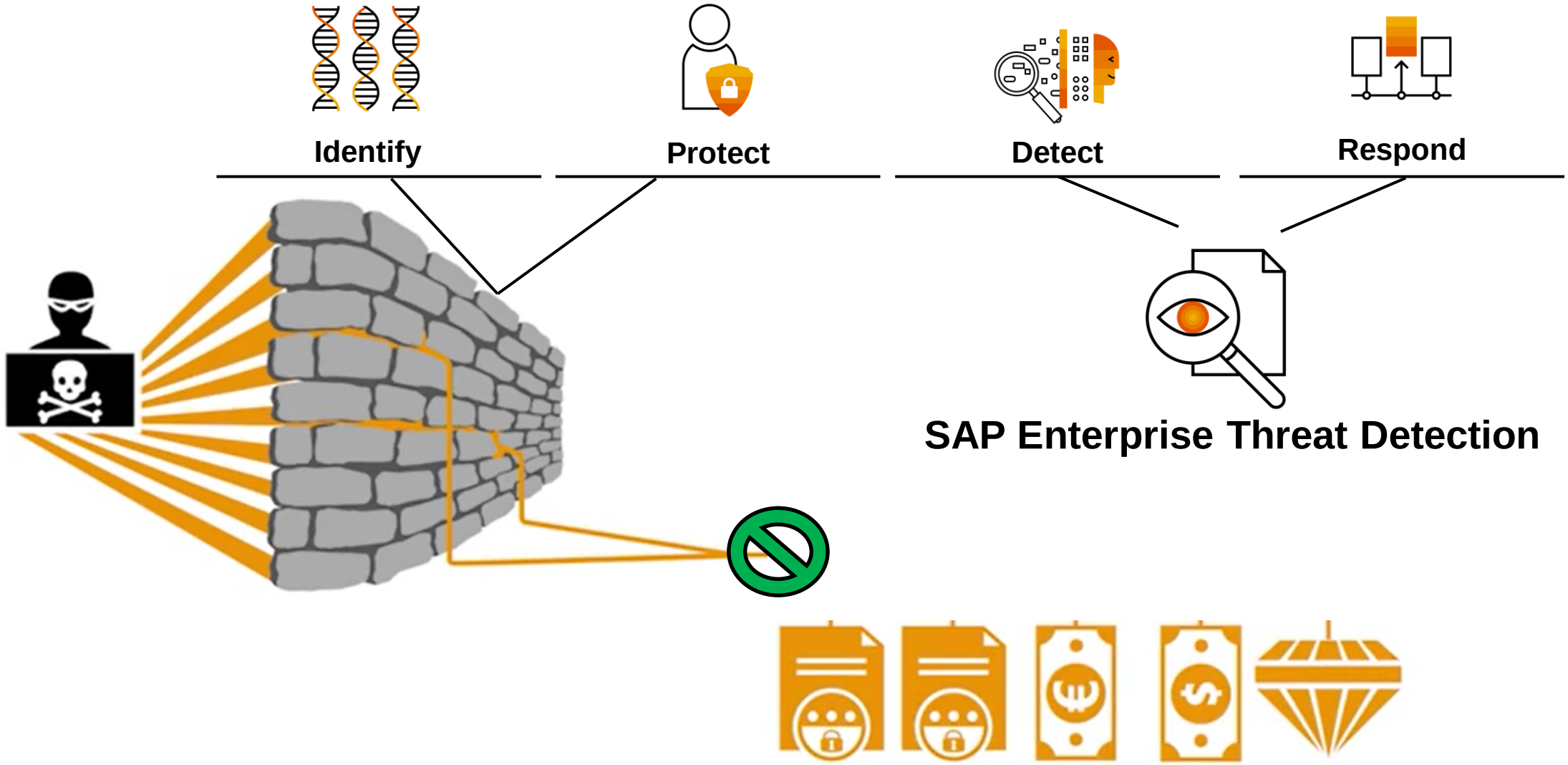
SAP Enterprise Threat Detection



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

When are you able to stop a breach ?

SAP Enterprise Threat Detection



Preventing Fraud & Cyber Attacks

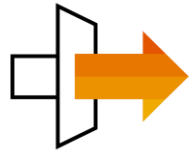
Debugging DEV System

Discover SM59 connections

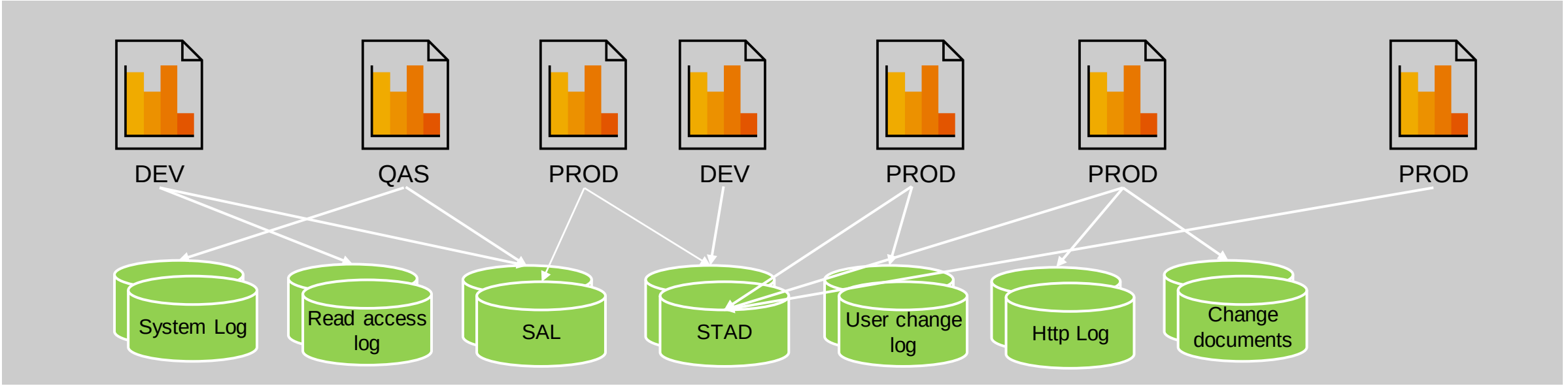
RFC to change passwd

Change vendor

Outgoing payments



01.2020 | 06.2020 | 03.2021



SAP Enterprise Threat Detection

More than ~400 SAP customers worldwide in all industries protect their SAP landscape with SAP Enterprise Threat Detection.

Most of those companies are listed within the DAX 30, DOW 30, or come e.g. from the defense sector. Please address the authors or your SAP account manager for more details about our reference customers.

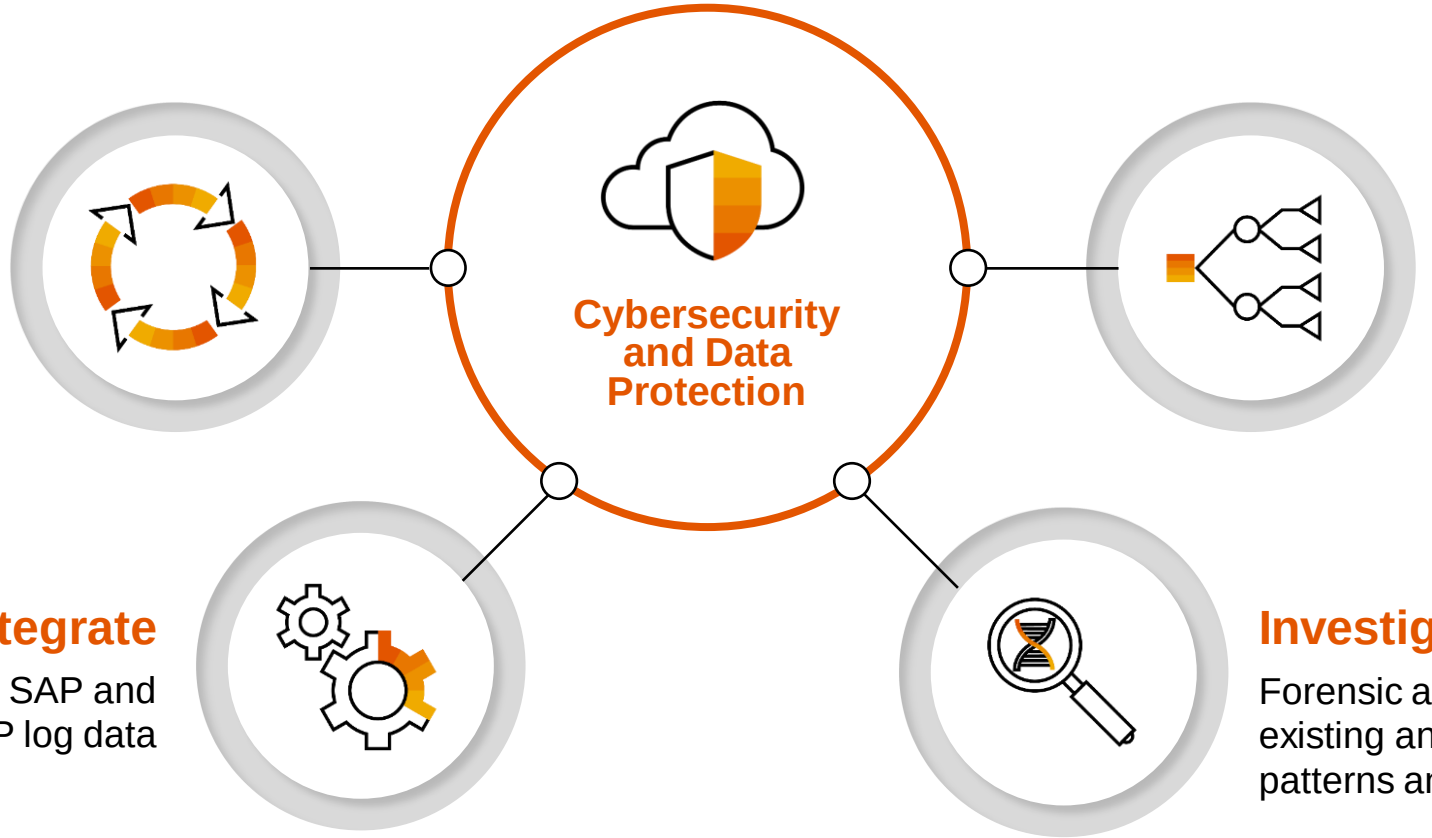
SAP Enterprise Threat Detection is supported by the world leading auditing companies.

We have implementation partners in many regions of the world.

Partners are e.g.:

- Ernst & Young,
- KPMG,
- Turnkey,
- IBS Schreiber,
- Asconsit,
- PWC,
- SAPNS2,
- Deloitte
- Accenture,
- Infosys,
- Xiting…

How does SAP Enterprise Threat Detection work



Analyze

Efficiently enrich, analyze, and correlate logs

Evaluate

Automatically evaluate attack detection patterns with real-time alerting

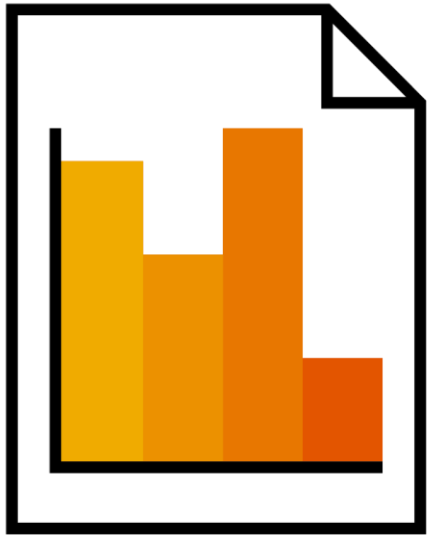
Integrate

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

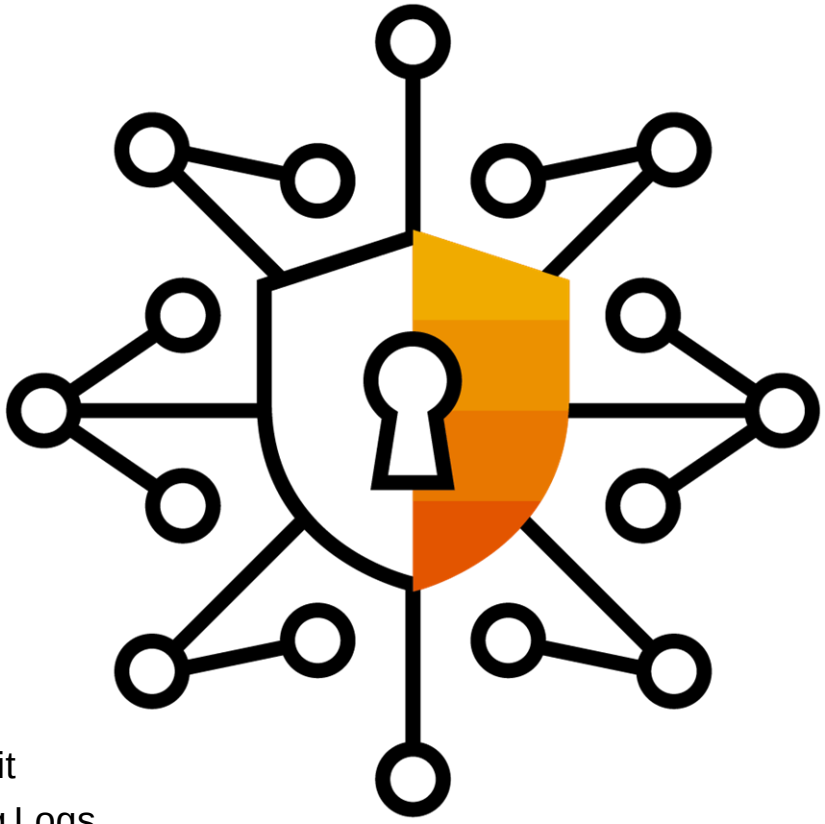
- AuditD

In Planning:

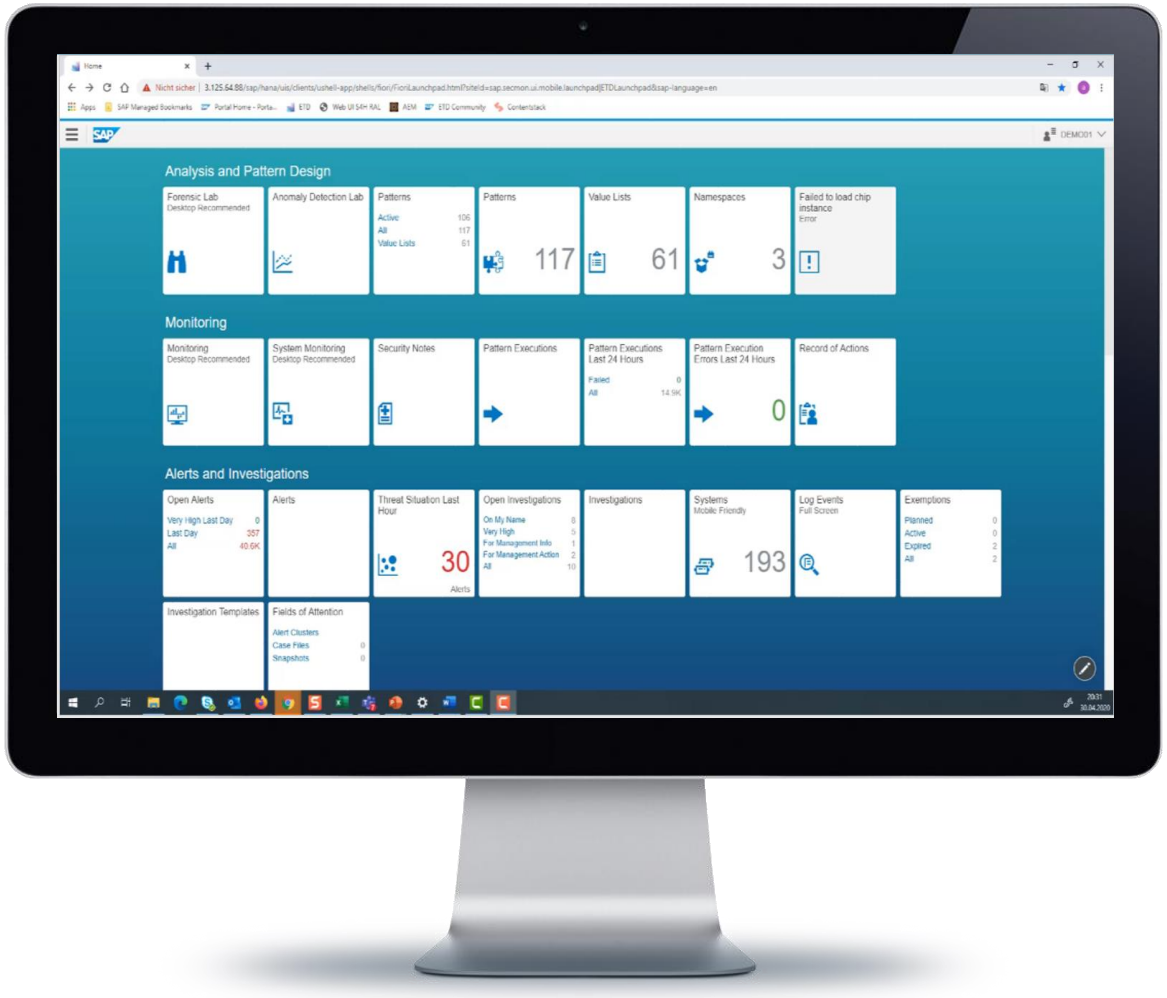
Log Change Reader
Transport File Analyzer
Cloud Connector Logs
Business Objects Log Support
Table Change Log
SAP Analytics Cloud
SAP Cloud Solutions

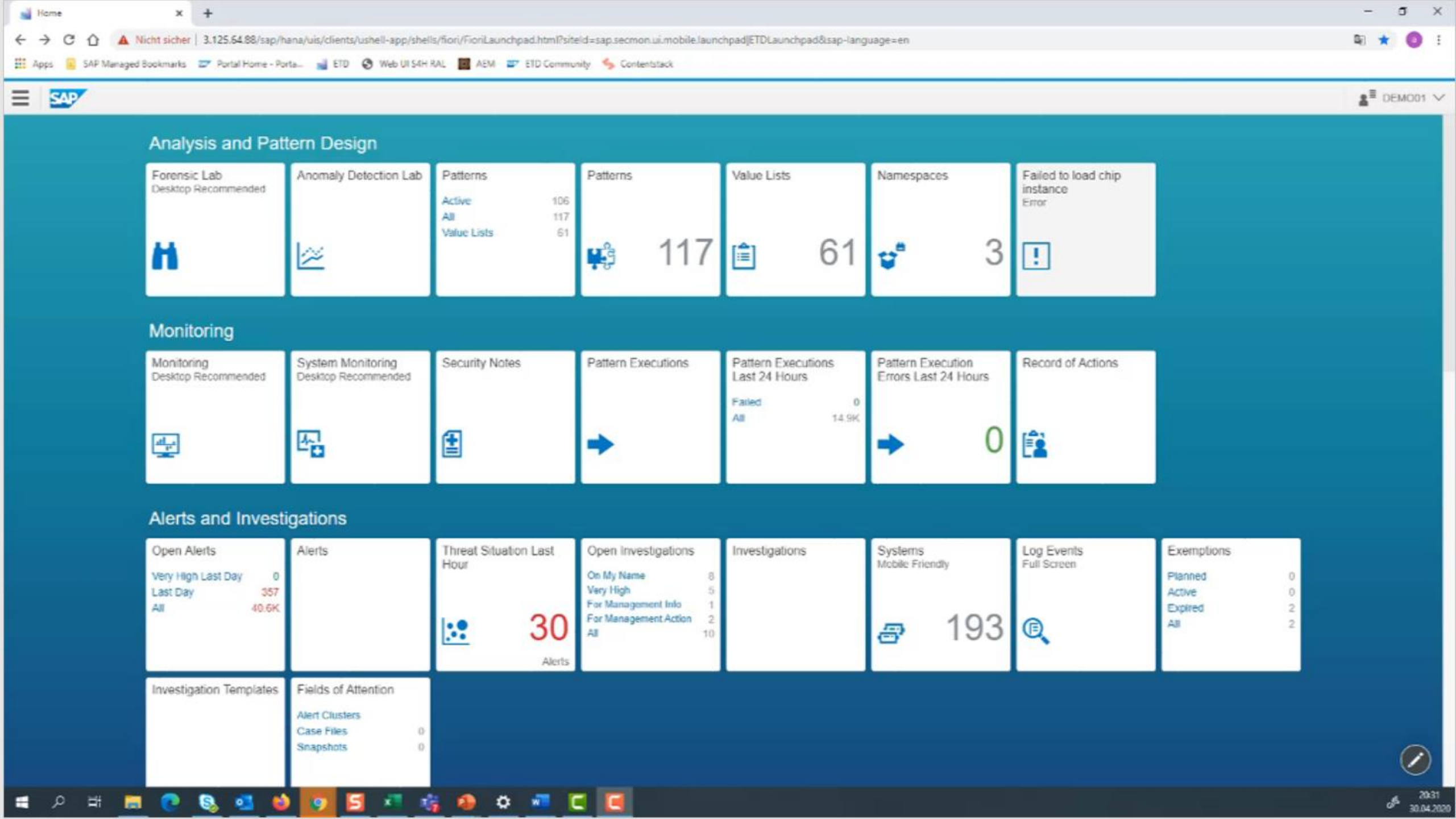
Unique benefits of Enterprise Threat Detection

- 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




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

Reference Use Case: SAP Enterprise Threat Detection @ SAP IT

SAP Cyber Defense and Response Center – Security Event Management

SAP Enterprise Threat Detection used by SAP IT for Security Event Management

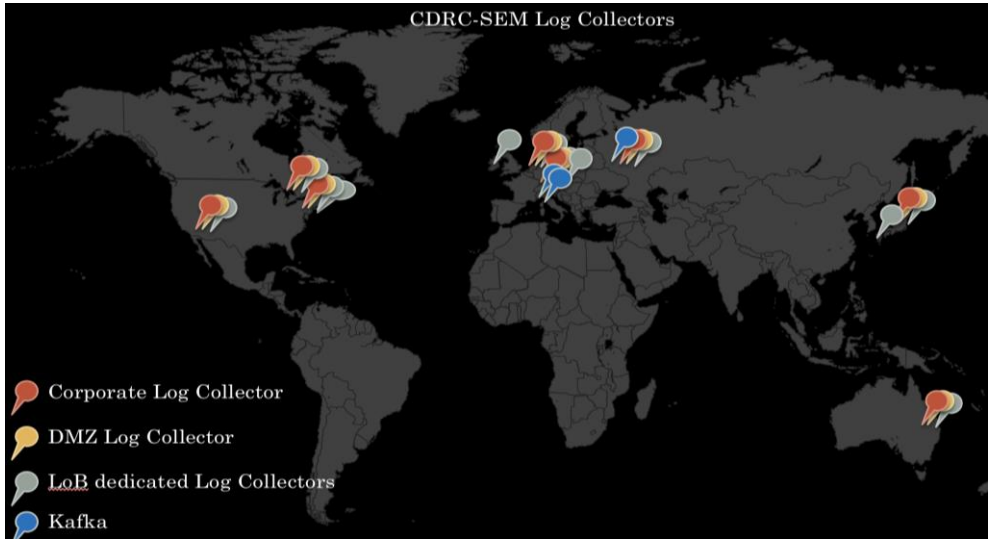
- Monitors, collects and correlates security events, generated within the SAP IT infrastructure, SAP cloud platforms and if applicable within the application layers, to detect security incidents and threats for all SAP lines of business

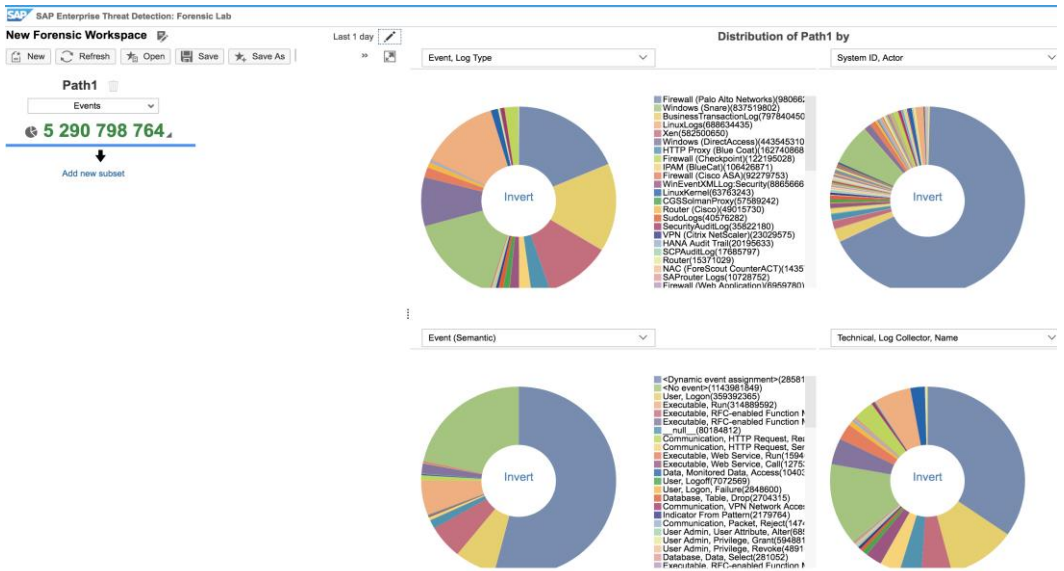
Global deployments of Log Collectors to cover all SAP data centers

24x7 Security Operating Center

Current Figures

- 9.2 billions events per day
- ~120.000 events/sec
- ~200.000 events/sec (peak)
- 160 billions events (total)
- 7.7TB in-memory data





Secure Business with SAP® Solutions

Before: Challenges and Opportunities
- Customer already implemented a SIEM solution, but it did not cover SAP landscape
- Processing SAP events using custom development is too complicated
- Unable to correlate security events from different sources

Why SAP
- Central SIEM for SAP and non-SAP landscape
- Built-in connectors to collect security-relevant events from ABAP AS, Java AS, HANA DB
- Easier and faster customization with the 100+ prepackaged template correlation rules
- Complex integration scenarios made possible because of the SAP HANA basis
- Key unique capabilities like Forensic Lab, Log Learning, Auto-reaction, Retrospective analysis (even when security events are deleted from the source systems)
- SAP ETD can be connect to 3rd party SIEM solutions (push and pull mechanisms)
- SAP Field Services helped to accelerate the implementation and to get fast and reliable results

After: Value-Driven Results
- Improved security events collecting and processing
- Improved credentials secrecy, better monitoring of superusers
- Monitoring of SAP and non-SAP landscape
- General improvements in basis settings (trust relationships, background jobs, technical users, integration scenarios, etc.)

200 mln.
Analyzed events per week

20–30
Incidents resolved per week

THE BEST RUN SAP®

Key project challenges at

- Connecting non-SAP system (3rd party Document Management System) via SAP ETD Log Learning
- Integration with SAP Service Desk (process findings)
- Integration with SIEM based on HP ArcSight (Security Operation Center)
- Automatic value list filtering (update employee vacations data)
- Auto-reaction mechanism based on UI Masking integration (custom development)

SAP Enterprise Threat Detection Success Story

Organization
Anonymous

Location
Germany

Industry
Fuel technology

Products and Services
SAP Enterprise Threat Detection

Employees
3.580

Revenue
circ. 630 Mio. Euro

Objectives

- Support of revision
  - Evaluation of security logs
- Business safety
  - Identification of security lacks
  - Monitoring of critical system activities
- Data privacy
  - Monitoring of critical data usage
  - Monitoring of unauthorized access

Why SAP?

- SAP system transparency with respect to security
- Monitoring of ABAP-systems
- Using analyzed logs e.g. Security Audit Log
- Active patterns e.g. Brute Force, Blacklisted reports, Multiple downloads
- Includes high performance of security analysis
- Usage of anomaly detection lab
- Rather low operational effort

Next Steps

- More SAP standard patterns
- Risks of ‘unsecure’ systems
- Qualified monitoring of downloads
- Evaluation HANA-logs
- Inclusion SAP environment (Windows Logs)
- Archiving/ Housekeeping
- Security notes

150 per day

Alert Peak

10.000 per day

Pattern Executions

3-4 per day

Investigations

10 Mio. per day

Log Events

SAP Enterprise Threat Detection Success Story

Organization
Anonymous

Location
Germany

Industry
Public Sector

Products and Services
SAP Enterprise Threat Detection
ERP SAP System

Employees
100.000

Objectives

- Security analysis of cash flows and related financial system
- ERP-SAP provides central system for the transaction of payments
- Security vulnerabilities in ERP-SAP can have an direct impact on other procedures and end users
- Higher safety requirements for SAP systems due to critical payment and procedure processes

Why SAP?

- Integration of SAP Security into Security Operation Center
- Integration of SAP landscape in SIEM
- Usage of standard and specific patterns
- Risk based mitigation of SAP vulnerabilities
- Security support as Managed service
- Additional security controls for patch management
- Anomaly detection and compliance checks

Next Steps

- Establishment of IT security manager in development teams as multiplicator
- Monitoring of internal solution process
- Regular training to mitigate code and system level vulnerabilities
- Continuous IT security audits in code, system and transport level

25.000 per second

Alert Peak

> 150.000

Monitored user accesses

SAP Enterprise Threat Detection Success Story

Organization
Anonymous

Location
Germany, DAX30 Company

Products and Services
SAP Enterprise Threat Detection

Employees
> 100.000

Objectives

- Monitor of several SAP systems
- Secure It environment

Why SAP?

- Usage of Security Detection Patterns
- Creation of additional own patterns to secure special functions within the SAP systems
- Ingestion of non SAP Log Data on a high amount
- SAP Cloud Platform adapter of ETD to further monitor the whole landscape

Next Steps

- Connect further Cloud Platforms from SAP
- Integrate more non SAP Log Data

100 SAP systems

Monitored with SAP ETD

Protecting the crown jewels

Basis service

- ✓ 24x7 monitoring of your SAP software environment
- ✓ Checking for ~60 standard attack path patterns
- ✓ Risk-based and prioritized alerting
- ✓ Monthly reporting of all incidents and all log data

German data center*

Service provision within the European Union

Language: English

* Other data centers are in discussion.

Protecting the crown jewels

Extended service

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

Basis service

- ✓ 24x7 monitoring of your SAP software environment
- ✓ Checking for ~60 standard attack path patterns
- ✓ Risk-based and prioritized alerting
- ✓ Monthly reporting of all incidents and all log data

German data center*

Service provision within the European Union

Language: English

* Other data centers are in discussion.

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

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®