SAP Enterprise Threat Detection
L1
05, 2019
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

1. Why did SAP decide to build Enterprise Threat Detection?
2. What is SAP Enterprise Threat Detection?
3. Governance, risk, compliance and security solutions from SAP
4. Securing the Intelligent Enterprise — SAP Enterprise Threat Detection
5. Why is Enterprise Threat Detection needed?
6. SAP Enterprise Threat Detection
7. Overview
8. Architecture
9. Use cases
10. Benefits
Why did SAP decide to build Enterprise Threat Detection?

Customer Feedback

- „SAP systems are seen as a ‘Black Box’ if it comes to security aspects and suspicious behavior in SAP systems“
- There were critical incidents at customers that could have been avoided if the preparation phase would have been discovered (see below)

**SAP invented new technology** (SAP HANA in Memory Database) that provides a unique selling point related to performance and real time alerting

SAP decided to create a new product SAP Enterprise Threat detection

Giving insights into SAP Systems and providing a very high performance
What is SAP Enterprise Threat Detection?

• SAP ETD is a real-time Security Event Management and – Monitoring solution
• It supports the customer to detect, analyze and neutralize cyber attacks as they are happening, and before serious damage occurs
• Core Capability: Secure your SAP Systems
• Key questions answered:

1. How can I keep track on who is attacking me?
2. What actions can I take to neutralize attacks?
3. How do you know what end-to-end action took place?
4. How do I find anomalies in my landscape systems?
5. How do I know what damage has been made?
Governance, risk, compliance and security solutions from SAP
Solution mapping to key themes

Enterprise risk and compliance

- SAP Process Control
- SAP Risk Management
- SAP Audit Management
- SAP Regulation Management by Greenlight
- SAP Business Integrity Screening

Access governance

- SAP Access Control
- SAP Cloud Identity Access Governance offering
- SAP Dynamic Authorization Management by NextLabs
- SAP Access Violation Management by Greenlight
- SAP Identity Management
- SAP Single Sign-On

Cybersecurity and data protection

- **SAP Enterprise Threat Detection**
- SAP Enterprise Digital Rights Management by NextLabs
- SAP Data Custodian
- Field masking and UI logging for SAP S/4HANA
- SAP NetWeaver AS Code Vulnerability Analysis
- SAP Fortify by Micro Focus

International trade and tax management

- SAP Global Trade Services
- SAP S/4HANA for international trade
- SAP Watch List Screening
- SAP Tax Compliance
- SAP S/4HANA for advanced compliance reporting
Securing the Intelligent Enterprise — SAP Enterprise Threat Detection
Refine algorithms to better detect threats

Leverage machine learning to refine anomaly detection methods such as statistical methods, one-time behavior, and potential malicious sites

Keep systems secure in a continuously changing cybersecurity threat environment
Leverage powerful and flexible monitoring, detection, and response capabilities
Receive actionable alerts in time to neutralize threats to your business-critical asset
Help prevent damage to your business and reputation
Why is Enterprise Threat Detection needed?

**External and internal Attacks**
- Attacks by Cyber-Criminals (Hackers will find ways!)
- Automated Attacks
- New Attack Vectors and Risks

**Attacks against SAP Systems**
- Missing Transparency (e.g. in SAP systems)
- Big Data issue (millions/billions of logs/day)

**Compliance**
- New Data Privacy Regulations
- New Data Breach Regulations

**New Threat Situations and new behaviors seen**

**New Challenges**
- Intellectual Property
- Reputation
- Sensitive Data

**New controls needed**
- Severe Penalties
Why is Enterprise Threat Detection needed?

Risk of being attacked and hacked is omnipresent!

- Interconnected environments!
- Internal and external hackers will find vulnerabilities to get into the system!
- Large organisations are behind attacks!
- Sophisticated Attack Vectors with long preparation and execution times

SAP Systems are subject to Hackers!
Companies' 'Crown Jewels' are in SAP systems!

SAP Enterprise Threat Detection helps detecting these Threats as early as possible
SAP Enterprise Threat Detection detects issues already in the attack preparation phase, by that preventing even more serious damage

New Threat Situations and new behaviors seen

New Challenges

New controls needed

- Intellectual Property
- Reputation
- Sensitive Data
- Severe Penalties
SAP Enterprise Threat Detection
Unique Selling Points and Features

SAP system transparency with respect to security

SAP related content, ready to use further content delivered on a regular basis

Reduce false positives with context information (users/systems)

Correlation of any data (e.g. no data preparation/indexation required) – end to end analysis

Compliance

High manipulation safety: data collection insurance (by Kernel API)

Very high performance, alert detection in real time

User pseudonymization included

Data volume independent pricing
SAP Enterprise Threat Detection
Unique Selling Points and Features

Automated attack detection patterns

SAP system transparency with respect to security

Forensic analysis, modelling of attack detection patterns, charts

SAP related content, ready to use further content delivered on a regular basis

Freely customizable monitoring dashboards

Reduce false positives with context information (users/systems)

Easy ingestion of any non SAP log data

Correlation of any data (e.g. no data preparation/indexation required) – end to end analysis

System monitoring + risk evaluation

Compliance

Alert forwarding to other SIEM systems

High manipulation safety: data collection insurance (by Kernel API)

Alert and investigation handling included

Very high performance, alert detection in real time

Log management within ETD normalized data, original data, unrecognized data

User pseudonymization included

Anomaly detection and related patterns

User/system behavioral analysis

Data volume independent pricing
SAP Enterprise Threat Detection — Architecture

SAP Landscape
SAP NW JAVA
SAP NW ABAP
SAP HANA
Log Collector

Non-SAP log data
SAP Data Centers
Non SAP Data Centers
IT Network Devices
Log Collector

Systems provide log data and context information
Evaluation in real time only with ETD

SAP Enterprise Threat Detection

SAP HANA
Streaming Analytics

Normalization and pseudonymization of log data

Analyst tool

threat situation, lab forensic, patterns, log learning, etc.

SAP HANA
Log Collector

Normalize and pseudonymize, of log data
Overview

Architecture

Use cases

Enterprise Threat Detection
Use cases included with SAP Enterprise Threat Detection

Authorization Management
Make sure that assignments of critical roles or profiles to users are conform with policies

System Configurations
Make sure that system security settings are not changed

Information Disclosure
Make sure that no extraction of confidential information takes place

Login Attempts
Make sure that no logins of expired, deleted or locked users take place and that there is no miss-use of standard users

Data Manipulation
Make sure that content of critical database tables are not changed/deleted

Remote calls of a productive System
Make sure that communication from non-productive to productive systems does not takes place

Access to Critical Resources
Make sure that forbidden/ blacklisted transactions, reports or function modules are not executed

Debugging and Error-Analysis
Make sure that no miss-use of debuggers (e.g. change values at runtime to change application flow) takes place in productive systems
Use cases included with SAP Enterprise Threat Detection

**Denial of Service**
Make sure that denial of service attacks are recognized timely to avoid complete system outages or unresponsiveness of a system.

**Web-APIs**
Make sure that no miss-use of web-APIs takes place.

**SQL Functions**
Make sure that suspicious SQL functions calls of are recognized.

**User Behaviour**
Make sure that unusual behaviour of technical and dialog users are recognized.

**Passwords and Administrative Roles**
Make sure that passwords of administrative users are not being manipulated.

**Special Patterns related to attacks related to SAP Security Notes**

Read Access Logging as additional source for specialized Patterns
Ensure that your Intellectual Property is not stolen/downloaded/viewed.
Demo
Brute Force Attack and Sensitive Data Download

User failed Logon → Frequency Increases → Sensitive data accessed

Forgotten passwords lead to User Failed Logons → Suddenly there is a spike in User Failed Logons beyond a set threshold → Automated attack detection patterns would alert the security operations center and identify → Users Terminals Key events Sensitive data accessed Data downloaded
Demo
Call for a Critical Transaction

Logon of unauthorized User Group

Call critical Action

Unauthorized Data view

Logon

Unauthorized access beyond a set threshold

Automated attack detection patterns would alert the security operations center and identify

Users
Terminals
Key events
Sensitive data accessed
Data downloaded
SAP Enterprise Threat Detection – Starter Pack Alarm System

Who viewed and downloaded which data?

Challenges

• The most important data of a company (financial data, engineering data,…) must be protected separately
• Who viewed or even downloaded this data without authorization?
• Valuable Know-how (engineering plans, recipes,…) is stolen
• How can customer information be protected from hacking?

SAP-Functionality

• SAP-manager receives notification when critical data has been read or downloaded
• Adaption of authorized user via “white list”
• Unauthorized download of data is detected
• Evaluation of Read Access Log (RAL) via SAP Pattern possible

Benefits

• Protection of the crown jewel of my company
• Transparency – Who has access to my data?
• Monitoring of existing Security Policies
• Simple scenario are adapted to the customer
• Small selection of industry-specific patterns
• Alerting by e.g. e-mail to responsible person
• Valuable development-know-how (e.g. engineering data) is protected at low cost
SAP Enterprise Threat Detection Service
Introduction of a basic “alarm system” based on SAP ETD

Introduction of SAP Enterprise Threat Detection as an „alarm system“

Initial situation

- Operation of a complex SAP environment with AS ABAP Systems
- Need for a solution that inform about severe, security relevant events within SAP landscape and beyond (e.g. network)
- The need for a significant reduction in the number of false alarms

Price
29,000 €

Feature
Service number: 50109981
SAP Enterprise Threat Detection Service
Introduction of a basic “alarm system” based on SAP ETD

Description of services
• **Kickoff Workshop** with presentation of the SAP ETD solution, the delivery approach and the coordination to the project as well as the system to be analyzed
• **Installation and Configuration** SAP Smart Data Streaming (SAP SDS, required for SAP ETD, max. 2 SAP systems) and SAP Enterprise Threat Detection (The SAP ETD required for SAP HANA system must be available)
• **Configuration** from SAP SDS and SAP ETD to record log events, detect attack patterns and alert ABAP-based security events
• **Basic-Workshop** about SAP ETD Functions and basic configuration of SAP Standard Threat Pattern
• **Basic Configuration** Threat Pattern delivered by 10 SAP, by default
• **ETD Roadmap** For the Preparation of a comprehensive implementation of SAP ETD

<table>
<thead>
<tr>
<th>Price</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>29,000 €</td>
<td>Service number: 50109981</td>
</tr>
</tbody>
</table>

SAP Enterprise Threat Detection — Architecture

![Architecture Diagram](image)
SAP Enterprise Threat Detection Service
Introduction of a basic “alarm system” based on SAP ETD

Your benefit
• Quick analysis results based on SAP Best Practice knowledge
• Very good introduction which offers added value SAP Enterprise Threat Detection
• Clear Roadmap for a optimized security incident/ response process based on SAP Enterprise Threat Detection

Price
29,000 €

Feature
Service number: 50109981
SAP Enterprise Threat Detection operational capabilities

What are the options for operating ETD?

The customer is free to choose which operating mode he wants to use:

- Independent operation by customers themselves (on Premise)
- Infrastructure hosting possible via SAP (SAP HANA Enterprise Cloud) or partner
- Variations of different managed service scenarios available (via SAP or Partner)
What advantages does Enterprise Threat Detection offers from a strategic point of view?

Arguments for a SAP solution

- SAP understands SAP log files best
- SAP content
  - Customers give us feedback and expand our patterns
  - Regular expansion of available content
  - Planned integration of the SAP Cloud Application
- Cooperation with security-relevant organizations
- Cooperation with security partners like Atos, FireEye, HPE, IBM, IBS Schreiber, NTT, Schönhöfer, Secude, Trend Micro, Xiting…
- Reduction of risks through non-recorded SAP Security Patches
- Evaluation in real time only through Enterprise Threat Detection
SAP Enterprise Threat Detection
Further Information

- Product Description

- Help SAP

- Enterprise Threat Detection Community Topic Page
  https://www.sap.com/community/topics/enterprise-threat-detection.html

- YouTube, e.g.
  https://www.youtube.com/watch?v=EiypEITilgY
Thank you.

Questions

Contact information
Preventing Fraud from a Multi Vector Attack

Debugging DEV System ➔ Discover SM59 connections ➔ RFC to change passwd ➔ Change vendor ➔ Outgoing payments

get access

STAD

Http Log

documents

System Log

READ access log

STAD

User change log

Http Log

Change documents

SAP Enterprise Threat Detection

Structured, standardized security data across the landscape

Patterns and correlation engine

Alerts and forensic lab
SAP Enterprise Threat Detection

Real Time Threat Visibility in Complex SAP Scenarios

Centrally Audited SAP Security Controls

Leveraging HANA Big Data, Machine Learning, Correlation, Analytics

Real Time Correlation of SAP, Non-SAP Logs w/ Log Learning

SAP User Behavior Monitoring

Efficient Investigations – Less False Positives

Compliance Support

Proactive Threat Monitoring, Early Interception of Threats