SAP Enterprise Threat Detection
Overview
October 2015
Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document 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. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Agenda

The challenge
The solution
Ad hoc analysis in action
Real-time security analysis in action
Additional topics
Summary
The challenge
What sort of attack do companies fear the most?

- Reputation
- Intellectual Property
- Operations
The threat environment is changing and becoming more dangerous

Traditional defenses no longer provide sufficient protection for business-critical software

More exposure to risk:
- Interconnected systems, mobile applications, …
- Increased interest in SAP software by cybercriminals
- Threats from inside nullify technical precautions

Attackers will penetrate to your critical systems
- What will you do then?
IT security organizations have serious blind spots

Cybercriminals are working in the dark areas of the IT landscape

What’s going on?
- Are there unexpected activities in the landscape?
- Are there ongoing attacks?
- Who is involved?
- What end-to-end attack actions took place?
- What was the damage?

If you cannot look, you cannot see
- If you cannot see, you cannot react effectively
What are the current threats? – A big-data solution is needed

Vast quantity of security-relevant data
• A tiny fraction is indicative of a particular threat

You must react in real-time to neutralize some attacks

To react in real-time you must:
• Analyze in real-time
• Understand in real-time
• Get actionable information in real-time
The solution
Protect your business
Effectively identify and analyze threats

Leverage the power of the real-time data platform
Efficiently analyze and correlate logs
Integrate custom log providers

Perform forensic investigations and discover new patterns

Automatic evaluation of attack detection patterns
Find threats focused on SAP software

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
SAP Enterprise Threat Detection
Main use cases

**Real-time security monitoring**
- Gather events from the landscape
- Evaluate attack detection patterns
- React on critical alerts
- Gain an overview of the threat situation

**Ad hoc analysis**
- Analyze existing suspicions
- Perform forensic investigation
- Support compliance processes
Architecture of SAP Enterprise Threat Detection

SAP Enterprise Threat Detection

- **Systems provide log data**
  - Java
  - ABAP
  - SAP HANA
  - Non-SAP

- **Monitored Landscape**

- **ESP (Event Stream Processor)**
  - Push

- **Normalize & enrich log data**

- **Evaluate & analyze, Generate Alerts**
  - SAP HANA

- **SAP HANA**
Example scenario
Assignment of SAP_ALL and following actions

An admin user increases the authorization of another user with SAP_ALL.

The hacker now uses the enhanced user to debug a financial report to divert money to his account.

Automated attack detection patterns would alert the security operations center at several stages and determine:

- Users
- Terminals
- Key events
- Values that were altered
Ad hoc analysis in action
Launch pad

The launch pad is the main entry point to the tools in SAP Enterprise Threat Detection.

The Forensic Lab tile takes you to the tool where you do ad hoc analysis and create attack detection patterns.
Browsing events in the Forensic Lab

When you browse events you are essentially applying filters to the normalized log data that exists in the SAP HANA database

- A series of filters is referred to as a path
- Visualize the filtered data to look for standout values
- Generate attack detection patterns from paths
Example of browsing events

Filter the events of the last 30 minutes for debugging activity
- There are 4 events where values have been changed
- There is 1 event where the program flow has been changed

Drill down to see the values that have been changed

Select a user for further investigation over a longer time period
- What has he been doing?
Real-time security analysis in action
Example of real-time analysis

- An operator looks at recent activity in the landscape and determines that there is abnormal activity in a particular system.

- He groups significant alerts into an investigation and sets the severity to very high for follow up by an analyst.

- The analyst uses the forensic tools to determine the impact of the attack and decide on what countermeasures need to be taken.
Patterns generate alerts when an attack is detected

The threat situation can be visualized in terms of alerts and their corresponding information

- Patterns
- Users
- Systems
- Terminals
Working with alerts and events
Monitor and Forensic Lab

Alerts → Initial analysis → Further analysis and derive new patterns
Additional topics
Pushing log data to SAP Enterprise Threat Detection

**Monitored systems:**
- Push their log data
- Schedule the data transfer
- ABAP and JAVA systems have a log extractor to support the transfer of data

**Event Stream Processor (ESP):**
- Exposes a REST service to receive log data from ABAP and JAVA systems
- Provides other ways of getting data into SAP Enterprise Threat Detection – for example, via UDP or file upload
Data model of SAP Enterprise Threat Detection

Normalization of log data
- Information content of the source is not reduced
- Unified representation of time stamps, user identities, …
- Maintenance of additional information

Data model is generic enough to cover customer-specific scenarios
- Use the log learning and knowledge base tools to integrate your own logs
Pseudonymization
Data protection for the individual
Summary
SAP Enterprise Threat Detection
A big-data solution to a serious security challenge

Protect the integrity of business processes and prevent theft or manipulation of business data

BIG DATA
Vast amount of log data scattered across the landscape.

ACQUIRE
Bring data together in one place with a common format.

ANALYZE
Evaluate attack detection patterns. Browse & analyze.

ACT
Lock user account, cut off connection, …

REAL RESULTS
Detect attacks early and prevent harm.

REAL TIME
Further information

Get more information and updates

SAP Enterprise Threat Detection
http://scn.sap.com/docs/DOC-58501

Security Community
http://scn.sap.com/community/security

Documentation on SAP Help Portal
http://help.sap.com/sapetd