IIS 267

Hands-On Session SAP Enterprise Threat Detection Exercises

Michael Schmitt, Arndt Lingscheid, SAP

Agenda

- EX 1: Working with the Forensic Lab (15 min)
- EX 2: Browse and Model (10 min)
- EX 3: Processing alerts and investigations (15 min)
- EX 4: Pseudonymization of User Data (5 min)
- EX 5: Monitoring Dashboards (10 min)
- EX 6: Log Learning – How to learn a new log source (20 min)

EX 1: SECURITY EXPERT - WORKING WITH THE FORENSIC LAB INTRODUCTION

Security Aspect:

- The Security Expert sometimes needs to do an ad-hoc analysis about things that happen in the landscape, or he gets a hint about certain suspicious behavior of an IP Address, within an SAP System, of certain program calls etc.
- He might need to create own charts to easier interpret the data and the suspicious behavior within, and even he might need to create an own detection patterns to get future alerts about the suspicious actions he found during his analysis.

Tool Aspect:

- The forensic lab is one the most important application in SAP Enterprise Threat Detection and helps you to gain insight about what is going on at present in your system landscape.
- Forensic lab supports workspaces for identifying and analyzing weaknesses or attacks and supports the modelling of charts or attack detection patterns. For attack detection patterns, you create the configurations, which you want SAP Enterprise Threat Detection to use to scan for events that match the pattern. No coding or complex regex/SQL queries are needed, instead SAP Enterprise Threat Detection takes care of transforming your attack detection pattern model to SAP HANA optimized queries.
- In this exercise you will learn how to work with the forensic lab, how to analyze log events and how to create charts and attack detection patterns are created.

EX 1: SECURITY EXPERT - WORKING WITH THE FORENSIC LAB SUMMARY

Security Aspect:

- As a Security Expert you are now able to do forensic analysis and find suspicious behaviors and evidences in big amounts of data.
- Now you can visualize this data as to your needs and create own Attack Detection Patterns in case you need to get Alerts on future occurrences of this situation.

Tool Aspect:

- You learned how to use the Forensic Lab to look into data, create Charts and Patterns and how to save them and to make them available to others.

EX 2: BROWSE AND MODEL INTRODUCTION

Security Aspect:

- As a Security Expert you very much have a feeling about anomalies and suspicious behavior within your systems and landscapes, by that if just looking at the data you would already find some presumably critical aspects that you want to explore. The invention of new Patterns based on this knowledge and these findings is the next important step to put your knowledge into automated action. In order to see if your pattern runs in the defined way, you may need to simulate the attack on a Test application, and presumably do a penetration test with Alert Checks.

Tool Aspect:

- You will use the Forensic Lab to model a Pattern of your choice, and then simulate the attack within an SAP S/4H system to verify that your first and/or your second Pattern works.

EX 2: BROWSE AND MODEL SUMMARY

Security Aspect:

- In the role of a Security Expert you have found suspicious behavior by Browsing through the data and you created/invented a Pattern based on these new findings. Then you did a hacking scenario/simulation to check whether your alert was raised.

Tool Aspect:

- You got familiar with forensic lab, how to find very different kinds of data within the logs, and how to use the tools to build patterns and charts, and how to test the working of these patterns.

EX 3: PROCESSING ALERTS AND INVESTIGATIONS INTRODUCTION

Security Aspect:

- As a Security Analyst in Level 1, 2 or 3 one of your main tasks is to check for raised Alerts and to process them. You need to answer questions like
  – Was this a real Alert or a false positive?
  – What are evidences which need to be collected to proof the attack or misuse?
  – Are there additional Alerts related to this Alert?
- Then you may need to collect the evidences and to follow a Standard Operation Procedure for the further actions.

Tool Aspect:

- SAP Enterprise Threat Detection raises alerts as notification for potential attacks as they are happening. An alert includes references to the log events and the attack detection patterns or the anomaly detection patterns that led to its creation.
- Alerts are processed and analyzed by making use of various applications provided by SAP Enterprise Threat Detection. After your analysis of an alert, you can mark it as an attack or a suspected attack and you can add it to an investigation.
- Investigations are collections of related material such as alerts, related events, case files, and snapshots. They are the central item with which more than one person might work with (e.g. monitoring agents and/or security experts).

EX 3: PROCESSING ALERTS AND INVESTIGATIONS SUMMARY

Security Aspect: As a Security Analyst you should be able to

- Save the collected evidences to an investigation
- Analyze the alert to avoid the false positives with several tools provided by ETD
- Print the investigation in PFD format as a hard copy

Tool Aspect:

- You know now how to view the Alerts and how to create an Investigation and assign alerts to it.
- The User behind this alert can be shown using Threat Situation
- You can view the Events triggered the current alert
- Add different objects to investigation
- You get to know the advanced tools, such as Case Files

EX 4: PSEUDONYMIZATION OF USER DATA INTRODUCTION

Security Aspect:

- All the person-related data must be protected before the collected evidences indicating a real attack.
- SAP Enterprise Threat Detection replaces the real user ID with User Pseudonym so that no user can be identified during all phases of analysis.
- Only with very restrictive access right the User Pseudonym can be resolved to real user.

Tool Aspect:

- You will learn how to resolve the User Pseudonym

EX 4: PSEUDONYMIZATION OF USER DATA SUMMARY

Security Aspect:

- As a User of a special authorized group you can find the real user behind a User Pseudonym

Tool Aspect:

- You learned how to resolve a User with “Resolve User Identity”

EX 5: MONITORING DASHBOARDS INTRODUCTION

Security Aspect:

- Security Monitoring Agent needs to have an overview of the whole landscape.
  - Active alerts
  - Status of investigations
  - Log events
  - Health Checks
- Content of the monitor must be able to be configured individually.

Tool Aspect:

- Monitoring dashboards provide an overview of the events, alerts, and investigations in the system.
- You can adjust the refresh rate, the number of charts and patterns displayed, and the time span monitored by the indicators of the Monitoring application.
- Monitoring dashboards can be customized the way you need.

EX 5: MONITORING DASHBOARDS SUMMARY

Security Aspect:

- As a Security Monitoring Agent you have learned that the Monitoring Dashboard is the most important tool for you to deal with your daily security monitoring task.

Tool Aspect:

- You should be able to open the default Monitoring Dashboard
- You can now customize Monitoring Dashboard and save it as your favorite

EX 6: LOG LEARNING – HOW TO LEARN A NEW LOG SOURCE INTRODUCTION

Security Aspect:

- In the daily life of a Security Expert you have to monitor a lot of systems, devices and networks. It is pretty possible, that at certain point of time some logs written by an application or device cannot be interpreted by current ETD. ETD Log Learning application fills this gap and allows you to parse any text-based logs and normalize such log data into the semantic data model of SAP ETD with its semantic events and attributes.
- With common semantic model you can correlate newly normalized log with other known logs. In this way, ETD can be extended to monitor potentially any systems which logs are learned by ETD.

Tool Aspect:

- The Log Learning application analyzes each entry in the log to find elements like variables and key-value lists.
- It represents the discovered elements as what are called annotations. For example, a timestamp is represented by the annotation. During analysis each log entry is analyzed into a sequence of annotations, which might be interspersed with fixed text. This sequence is called the markup for the log entry. Entries with the same markup are grouped together and are considered to be instances of the same entry type.
- The entry type is a technical artefact with an ID. As a user, you work with the markup to specify how to normalize the log entry type to the semantic data model of SAP Enterprise Threat Detection.

EX 6: LOG LEARNING – HOW TO LEARN A NEW LOG SOURCE SUMMARY

Security Aspect:

- As a Security Expert you have extended your monitoring boundary to include a new log - SSH log - into the system.
- Based on the data in the SSH log you can monitor the activities of ssh access in your system landscape.
- Patterns can be built to trigger alerts if disallowed ssh login happens.

Tool Aspect:

- You learned how to use the Log Learning application to parse a Unrecognized Log, assign this log to a new Log Type, associate the log to a Semantic Event and link Annotation to Semantic Attributes.
- You can now create a Run, and follow the workflow of activation, testing and productive deployment to finish the Log Learning process.
- The verification is done in Forensic Lab.

More information

Related SAP TechEd sessions

- IIS125 – Round Table: Secure the Intelligent Enterprise

Public SAP Web sites

- SAP Community: https://community.sap.com/topics/enterprise-threat-detection

Continue your learning experience from SAP TechEd in 2020

Your exclusive path to build and maintain SAP solution skills anytime, any place

Get empowered with access to relevant, up-to-date digital learning for SAP TechEd participants through a complete enablement solution that drives adoption and innovation.

Deepen your learning experience from SAP TechEd

Activate your free access to SAP Learning Hub, event edition, for:

- **Learning Journey** illustrations to guide you through **complementary** self-paced learning content
- **Content specific to SAP TechEd** in the online **SAP Learning Room for SAP TechEd**
- Access to SAP experts in **special live sessions**

Deepen and validate your SAP solution skills

Subscribe to SAP Learning Hub, solution editions, for:

- **Solution-specific Learning Journey guides, content, collaborative learning,** and **hands-on practice** for your role and goals
- Drive performance and business success with validated solution expertise from the **SAP Global Certification** program

Your benefits

- Gain insight into the latest innovations, and master software proficiency
- Keep skills up-to-date, and enable performance and business success with help from SAP solution experts
- Achieve competitive advantages and digital transformation success with trusted certifications

500,000+
Learners in SAP Learning Hub

100+
Experts getting certified per day

150+
SAP Global Certifications

Thanks for attending this session.

Contact for further topic inquiries

Dr. Michael Schmitt
Product Manager Sap Enterprise Threat Detection
m.schmitt@sap.com

Arndt Lingscheid
Product Manager Sap Enterprise Threat Detection
a.lingscheid@sap.com

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®