SECETD

SAP Enterprise Threat Detection

COURSE OUTLINE

Course Version: 02
Course Duration:

SAP Copyrights, Trademarks and Disclaimers

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials may have been machine translated and may contain grammatical errors or inaccuracies.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. 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.

Typographic Conventions

American English is the standard used in this handbook.

The following typographic conventions are also used.

This information is displayed in the instructor's presentation	🖥
Demonstration	➤
Procedure	1 2 3
Warning or Caution	⚠
Hint	💡
Related or Additional Information	»
Facilitated Discussion	💬
User interface control	*Example text*
Window title	*Example text*

Contents

Course Overview

TARGET AUDIENCE

This course is intended for the following audiences:

- Data Manager
- Industry / Business Analyst Consultant
- Developer IT Adminstrator IT Support
- Business User
- Business Analyst

UNIT 1 Introduction to SAP Enterprise Threat Detection

Lesson 1: Introducing SAP Enterprise Threat Detection

Lesson Objectives

After completing this lesson, you will be able to:

- Identify the basic features of SAP Enterprise Threat Detection

UNIT 2 Technical Overview of SAP Enterprise Threat Detection

Lesson 1: Identifying Solution Architecture Features

Lesson Objectives

After completing this lesson, you will be able to:

- Identify solution architecture features
- Detail the solution components

Lesson 2: Identifying Features of the System Landscape, Sizing, and High Availability

Lesson Objectives

After completing this lesson, you will be able to:

- Identify features of high availability

Lesson 3: Identifying High Availability and Log-Loss Prevention

Lesson Objectives

After completing this lesson, you will be able to:

- Identify log-loss prevention
- Recognize pattern replay

Lesson 4: Managing Log Sources

Lesson Objectives

After completing this lesson, you will be able to:

- Identify semantic data attributes and log events
- Identify context information and pseudonymization

Lesson 5: Installation and Configuration

Lesson Objectives

After completing this lesson, you will be able to:

- Describing Basic Components

Lesson 6: Readiness Checks and Troubleshooting

Lesson Objectives

After completing this lesson, you will be able to:

- Perform readiness checks and troubleshoot issues

Lesson 7: Identifying Features of Pattern Creation

Lesson Objectives

After completing this lesson, you will be able to:

- Identify features of pattern creation
- Model and attack

UNIT 3 Monitoring and Reporting

Lesson 1: Processing Alerts

Lesson Objectives

After completing this lesson, you will be able to:

- Process alerts

Lesson 2: Monitoring the System Health

Lesson Objectives

After completing this lesson, you will be able to:

- Monitor the system health
- Use monitoring dashboards

Lesson 3: Pseudonymizing User Data

Lesson Objectives

After completing this lesson, you will be able to:

- Pseudonymize user data
- Ensure compliance

UNIT 4 Onboarding Lifecycle Overview

Lesson 1: Incorporating Standard Operating Procedures

Lesson Objectives

After completing this lesson, you will be able to:

- Incorporate Standard Operating Procedures

Lesson 2: Connecting Log Sources via Log Learning

Lesson Objectives

After completing this lesson, you will be able to:

- Connect log sources via log learning

Lesson 3: Business Process Threat Patterns

Lesson Objectives

After completing this lesson, you will be able to:

- Identify business process threat patterns
- Create and change business partners
- Identify threats in invoice payments

UNIT 5

Good Practices Onboarding Lifecycle

Lesson 1: Following Best Practices

Lesson Objectives

After completing this lesson, you will be able to:

- Follow best practices

UNIT 6

Read Access Logging and UI Logging

Lesson 1: Identifying Log Sources

Lesson Objectives

After completing this lesson, you will be able to:

- Identify special and important log sources

UNIT 7 Custom Extensions

Lesson 1: Customizing Extensions

Lesson Objectives

After completing this lesson, you will be able to:

- Customize SAP Enterprise Threat Detection

UNIT 8 Appendix

Lesson 1: Installing and Configuring SAP Enterprise Threat Detection

Lesson Objectives

After completing this lesson, you will be able to:

- Install and configure