SOC Essentials: Investigating and Threat Hunting (SEITH)

ID SEITH **Preis** 1.000,– € (exkl. MwSt.) **Dauer** 9 Stunden

Kursüberblick

This course is part of the Defense Analyst learning path and is intended for learners who want to begin or advance a career as a Security Analyst within a SOC, as well as defense engineers and Splunk Enterprise Security or Splunk SOAR administrators who provide support to these roles.

In this course you will learn and practice how to conduct investigations using Splunk Enterprise Security features through best practices shared by our security champions, as well as practice some common analyst automation tasks using Splunk SOAR. You will also learn about the PEAK Threat Hunting framework and will apply its basic concepts in hypothesis-driven and baseline threat-hunting exercises.

Zielgruppe

- SOC Analysts
- Defense Engineers
- Splunk Admins who support these roles

Voraussetzungen

To be successful students should have a basic understanding of common cyber technologies and concepts including:

- OSI Model
- Networking concepts and common security tools
- Common Operative Systems like Windows and Linux

The following Splunk courses are also highly recommended:

- Intro to Splunk
- Using Fields (SUF)
- Previous courses in the Defense Analyst learning path

Kursziele

At the end of this course you should be able to:

- Describe SIEM best practices and basic operation concepts of Splunk Enterprise Security, including the interaction between CIM, Data Models, and acceleration, and common CIM fields that may be used in investigations
- Carry out a typical triage and investigation process using Splunk Enterprise Security
- Describe the purpose of the Asset and Identity, and Threat Intelligence frameworks in ES
- Define Splunk ES elements like Notable Event, Risk Notable, Adaptive Response Action, Risk Object, Contributing Events.
- Identify common built-in dashboards in Enterprise Security and the basic information they contain.
- Explain the use of SOAR playbooks and list the basic ways they can be triggered from Enterprise Security
- Explain the essentials of Risk-based Alerting and the Risk framework
- List the common high-level steps of threat hunting using the PEAK framework and practice some common steps of hypothesis hunting with Splunk.

Detaillierter Kursinhalt

Module 1 – Introduction

- The CyberSecurity Defense Analyst
- CIM, Data Models and Correlation Refresh
- Lab 1: Introducing the environment

Module 2 – Splunk Enterprise Security (ES) for Analysts

- Asset & Identity Framework
- Threat Intelligence Framework
- Notable Event Framework
- Adaptive Response Framework
- Incident Investigation Management in Splunk ES
- Lab 2: Pick up an investigation

Module 3 – Risk Analysis Framework

- Lab 3: Continue your investigation with RBA

Module 4 – Working with Splunk SOAR

- Lab 4: Splunk SOAR Practice

Module 5 – Threat Hunting Introduction

- Lab 5: Hunting with Windows Event Codes

Module 6 – Threat Hunting with PEAK: Hypothesis-based Hunt

- Lab 6: Hypothesis-based Threat Hunting Practice

Module 7 – Threat Hunting with PEAK: Baseline Hunt

- Lab 7: Baseline Threat Hunting Practice

This lab experience is using the following Splunk tools:

- Splunk Enterprise Version: 9.1.1
- Enterprise Security (ES) Version: 8.1.0
- Splunk SOAR Version: 6.4.1

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch