

## Certified SOC-Analyst (CSA) Schulung

www.kebel.de  
0231.5191986



Seminarpreis ab:  
2950,00 € zzgl. MwSt.  
(3510,50 € inkl. 19% MwSt.)

Kurs-ID: CMK52

Live Online Seminarpreis ab:  
2950,00 € zzgl. MwSt.  
(3510,50 € inkl. 19% MwSt.)

Dauer: 3 Tage  
Standardzeiten:  
09:00 bis 16:00 Uhr

IT Trainings Kebel  
Europaplatz 11  
44269 Dortmund  
T: 0231.5191986  
F: 0231.5191988  
training@kebel.de

## Aktuelle Terminübersicht und Anmeldung zum Kurs

⇒ Certified SOC-Analyst (CSA) Schulung

### Seminarziel

Der Certified SOC-Analyst (CSA) ist ein Aus- und Weiterbildungsprogramm, welches die Teilnehmer dabei unterstützt, gefragte technische Kompetenzen zu entwickeln, die von einigen der branchenweit erfahrensten Ausbilder vermittelt werden. Dieses Programm zielt darauf ab, neue Berufschancen durch tiefgreifendes und detailliertes Wissen zu schaffen, gepaart mit erweiterten Fähigkeiten, die einen signifikanten Beitrag zu einem SOC-Team leisten können. In einem intensiven 3-Tages-Kurs deckt es die Grundlagen des SOC-Betriebs ab und vertieft das Wissen in Bereichen wie Log-Management und Korrelation, SIEM-Implementation, erweiterte Vorfallerkennung und Incident Response. Darüber hinaus erwerben die Teilnehmer Kenntnisse in der Verwaltung verschiedener SOC-Prozesse und der Zusammenarbeit mit dem CSIRT bei Bedarf. Dieser Kurs wird von einem zertifizierten und erfahrenen EC-Council-Trainer geleitet. Die Prüfungsgebühr ist bereits im Kurspreis enthalten. Der Kurs findet in Kooperation mit der EDC Business GmbH statt. EDC Business GmbH ist ein autorisierter Trainings-Partner von EC-Council. Die Firma IT Trainings Kebel ist kein autorisierter Trainings-Partner und bewirbt und vertreibt nur die Kurse der EDC Business GmbH.

### Kursvoraussetzungen

Erfahrung im Bereich Netzwerk- und IT-Sicherheit

### Kursinhalt

SOC Essential Concepts

-Computer Network Fundamentals

-TCP/IP Protocol Suite

-Application Layer Protocols

-Transport Layer Protocols

-Internet Layer Protocols

-Link Layer Protocol

-IP Addressing and Port Numbers

-Network Security Controls

-Network Security Devices

-Windows Security

-Unix und Linux Security

Dipl.Ing. Thorsten Kebel  
USt.ID: DE175560970  
DE 5244 0501 9901  
7100 5728  
BIC: DORTDE33

Alle genannten Marken und Produkte  
sind Warenzeichen oder eingetragene  
Markenzeichen der entsprechenden  
Unternehmen.



- Web Application Fundamentals
- Information Security Standards, Laws and Acts
- Security Operations and Management
- Security Management
- Security Operations
- Security Operations Center (SOC)
- Need of SOC
- SOC Capabilities
- SOC Operations
- SOC Workflow
- Components of SOC: People, Process and Technology
- Types of SOC Models
- SOC Maturity Models
- SOC Generations
- SOC Implementation
- SOC Key Performance Indicators (KPI) and Metrics
- Challenges in Implementation of SOC
- Best Practices for Running SOC
- SOC vs NOC
- Understanding Cyber Threats, IoCs, and Attack Methodology
- Cyber Threats
- Intent-Motive-Goal
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness
- Network Level Attacks
- Host Level Attacks
- Application Level Attacks
- Email Security Threats
- Understanding Indicators of Compromise (IoCs)
- Understanding Attacker's Hacking Methodology

www.kebel.de  
0231.5191986



Incidents, Events, and Logging

-Incident

-Event

-Log

-Typical Log Sources

-Need of Log

-Logging Requirements

-Typical Log Format

-Logging Approaches

-Local Logging

-Centralized Logging

Incident Detection with Security Information and Event Management (SIEM)

Security Information and Event Management(SIEM)

Security Analytics

Need of SIEM

Typical SIEM Capabilities

SIEM Architecture and Its Components

SIEM Solutions

SIEM Deployment

Incident Detection with SIEM

Examples of commonly Used Use Cases Across all SIEM deployments

Handling Alert Triaging and Analysis

Enhanced Incident Detection with Threat Intelligence

Understanding Cyber Threat Intelligence

Why Threat Intelligence-driven SOC?

Incident Response

Incident Response Team (IRT)

Where Does IRT Fits in the Organization?

SOC and IRT Collaboration

www.kebel.de  
0231.5191986



Incident Response (IR) Process Overview

Step 1: Preparation for Incident Response

Step 2: Incident Recording and Assignment

Step 3: Incident Triage

Step 4: Notification

Step 5: Containment

Step 6: Evidence Gathering and Forensic Analysis

Step 7: Eradication

Step 8: Recovery

Step 9: Post-Incident Activities

Responding to Network Security Incidents

Responding to Application Security Incidents

Responding to Email Security Incidents

Responding to an Insider Incidents

Responding to Malware incidents

### **Trainerprofil**

### **Inklusivleistungen offene Seminare**

Kalt- und Warmgetränke

Pausensnacks

warmes Mittagessen

Zertifikat

Seminarunterlage bzw. Seminar-Handout

### **Diese Schulungszentren erwarten Sie:**

Berlin | Bremen | Dortmund | Dresden | Düsseldorf | Erfurt | Essen | Frankfurt a.M. | Hamburg | Hannover  
| Koblenz | Köln | Krefeld | Leipzig | Live-Online-Training | München | Münster | Nürnberg | Regensburg |  
Saarbrücken | Siegen | Stuttgart | ⇒ **Adressen**

oder als Live Online Training

Den Kursteilnehmern steht in allen unseren Schulungszentren ein PC-Arbeitsplatz mit der entsprechenden Software zur Verfügung.

**www.kebel.de**  
**0231.5191986**



## Das Bewertungsportal - eKomi



Lesen Sie unsere [⇒ Bewertungen](#).

Wir haben uns für das unabhängige eKomi-Portal entschieden und nutzen die authentifizierte Software, um unsere Teilnehmer:Innen zu befragen und das eKomi Gütesiegel zu tragen.

Jede abgegebene Bewertung – egal ob positiv oder kritisch – fließt in die Bewertungsstatistik von IT Trainings Kebel ein und ist Teil der eKomi Trust Zertifikate.

Zufriedene Kunden sind uns sehr wichtig.

Alle Kundenrezensionen können Sie auf der Website des Bewertungsportals nachlesen.

[www.kebel.de](http://www.kebel.de)  
0231.5191986



## Offene Kurse gemäß Terminplan

### ⇒ Präsenzkurse

Hierbei handelt es sich um standardisierte Seminare in unseren 21 Trainingszentren. Die Teilnehmer:innen sitzen an einem von uns bereitgestellten PC-Arbeitsplatz. Im Preis enthalten sind ein Seminar-Handout, ein Zertifikat sowie das Catering (Kalt- und Warmgetränke, Obst und Mittagessen).

### ⇒ Live Online Kurse im virtuellen Klassenzimmer

Bei unseren Live Online Kursen erleben Sie interaktive Kommunikation zwischen Trainer:in und Teilnehmer:innen im virtuellen Klassenraum. Die erforderliche Software und der Zugang wird durch unser Haus gestellt. Die Trainer:innen sind in Bild und Ton präsent. Die Teilnehmer:innen haben jederzeit die Möglichkeit, Fragen zu stellen. Gleichzeitig können Sie auf Ihrem (zweiten) Bildschirm selbst die Übungen nachvollziehen und praktisch ausprobieren. Unser Kebel Team steht Ihnen bei Fragen gerne zur Verfügung.

## Seminargarantie

Wir führen nahezu alle Präsenzseminare und Online Kurse bereits ab einer Person durch. Dies gilt für von uns bestätigte Seminare. Auf diese Weise können wir Ihnen eine reiche Terminauswahl anbieten und Sie erhalten Planungssicherheit für Ihre IT-Fortbildung.

Bei der Durchführung eines Seminars als Einzeltraining verkürzen wir die Seminardauer und intensivieren die Lernphasen im Trainer-Teilnehmer-Dialog. Somit profitieren Sie bei gleichem oder ähnlichem Seminarpreis und kürzerer bzw. angepasster Seminardauer von einem intensiven und individuellem Lernerlebnis. Bitte erfragen Sie diese Garantie für den jeweiligen Kurs.

## Firmenschulungen - individuell angepasst

Bei einer individuellen Firmenschulung werden nur die eigenen Mitarbeiter:innen des eigenen Unternehmens gemeinsam geschult. Die Termine, Zeiten und Inhalte werden individuell definiert und können live online, in Präsenz oder hybrid organisiert werden. Somit können u.a. halbtägige Schulungen für unterschiedliche Gruppen und Themen definiert werden. Unsere Firmenschulungen minimieren Ihre Kosten für Ihre interne Weiterbildung.

### ⇒ Firmenschulung - im Trainingszentrum

Ihre individuelle Firmenschulung in Präsenz wird hierbei in einem unserer bundesweiten 21 Trainingszentren organisiert und durchgeführt. Ihr gewünschtes Catering wird hierbei gemeinsam definiert.

### ⇒ Inhouseschulung – vor Ort beim Kunden

Wir organisieren gemeinsam Ihre individuelle Inhouseschulung vor Ort in Präsenz und stellen Ihnen erfahrene und kompetente Trainer:innen zur Verfügung. Auf Wunsch stellen wir Ihnen gerne vorkonfigurierte PCs bzw. Notebooks, Beamer und mobile Leinwände gegen Aufpreis zur Verfügung.

### ⇒ Firmenschulung - live online

Hierbei findet die Schulung, wie bereits oben beschrieben, im virtuellen Klassenzimmer statt.

### ⇒ Firmenschulung – hybrid

Eine weitere Möglichkeit Mitarbeiter:innen gemeinsam zu schulen besteht darin, in Ihrer Präsenzveranstaltung, weitere Teilnehmer:innen aus anderen Filialen oder dem Homeoffice live online dazuschalten.

### ⇒ Floorwalking

Floorwalking ist eine spezielle Art der Inhouseschulung. Beim Floorwalking von Büro zu Büro, schulen unsere Trainer:innen die einzelnen Anwender:innen direkt am eigenen PC-Arbeitsplatz, um ganz konkret und gezielt, individuelle Lösungen für den täglichen Bedarf zu erarbeiten. Floorwalking eignet sich somit auch im Anschluss einer bereits erfolgten Schulung.

### ⇒ Workshop

Ein konkretes Workshop- oder Coaching-Thema wird mit dem Kunden gemeinsam vor Seminarbeginn genau definiert. Unsere Trainer:innen beschäftigen sich vorab intensiv mit Ihren Workshopthemen, bereiten ein Konzept vor und erstellen bei Bedarf entsprechende Workshop-Unterlagen, Folien und Übungen. Für Rückfragen stehen wir gerne zur Verfügung.

www.kebel.de  
0231.5191986

Alle genannten Marken und Produkte sind Warenzeichen oder eingetragene Markenzeichen der entsprechenden Unternehmen.

