



## CSEE Cyber Security Essentials for Executives (SAN/CIS Critical Security Controls Essentials)

Die SANS / CIS Critical Security Controls stellen einen technisch fokussierten Sicherheitsstandard dar, welcher Unternehmen auf aktuelle und zukünftige Cyber- & Ransomware-Risiken vorbereitet.

### Listenpreis

2.850,00 € exkl. MwSt

3.391,50 € inkl. MwSt

### Dauer

2 Tage

### Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

### Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

### Ihre Ansprechpartnerin



**Manuela Krämer**  
Leitung  
Informationssicherheit

### Kontakt/Fragen:

[m.kraemer@cbt-training.de](mailto:m.kraemer@cbt-training.de)

Telefon: +49 (0)89-4576918-12

## Inhalte

Cyber-Angriffe, teils mit nationalen oder internationalen Auswirkungen stehen an der Tagesordnung und die Vernetzung, Digitalisierung und Globalisierung schreitet unaufhaltsam voran. Während die Komplexität der eingesetzten IT weiter steigt, führen die damit entstehenden Exponierungen teils zu katastrophalen Folgen für das Unternehmen, deren Kunden und Dienstleistern.

Die SANS / CIS Critical Security Controls stellen einen technisch fokussierten Sicherheitsstandard dar, welcher Unternehmen auf aktuelle und zukünftige Cyber- & Ransomware-Risiken vorbereitet.

Mit dem Wissen über aktuelle Risiken und Sicherheitskonzepten bewaffnet, können Sie die IT-Sicherheit in Ihrem Unternehmen überprüfen und entscheidend zum Schutz Ihrer System- und Netzwerk-Landschaft beitragen. So können finanzielle Kosten, Reputations- und Opportunitätsverluste sowie Aufwände für die nachträgliche Behandlung von Schwachstellen bzw. erfolgten Cyber-Angriffen minimiert werden.

- **Einführung in aktuelle Gefährdungen und Entwicklungen**
  - Internet / Deep Web / Dark Web
  - Threat Actors / Nation-State Threats & TTPs
  - Important Developments
- **Überblick technischer Maßnahmen und Prozesse anhand der SANS / CIS Critical Security Controls**
  - Autorisierte Geräte /Software
  - Schwachstellenmanagement
  - Schutz administrativer Privilegien
  - Systemhärtung
  - Ereignisüberwachung
  - Email, Web Browser & Malware-Schutz
  - Limitierung der Netzwerkservices
  - Data Recovery
  - Boundary Defense & Data Protection
  - Need to Know / Account Review
  - Wireless Device Control
  - Training & Penetration Tests
  - Application Software Security



- Incident Response and Management
  - War-Stories & Ransomware-safe Backup Management
- 

### Ziele

Das Seminar führt die Teilnehmer in das Thema Informationssicherheit, anhand einer Übersicht der aktuellen Technologien und Cyber-Angriffsvektoren, Sicherheitskonzepte & Best Practices, ein.

Zudem wird Basiswissen im Kontext Angreiferverhalten, Kryptographie, Kommunikationssicherheit, Datenschutz und Incident/DRP/BCM Management sowie allgemeiner Sorgfaltspflichten vermittelt.

Das Seminar liefert viele Beispiele aus dem Kontext Wirtschaftsspionage sowie Strategien, Hinweise und Handlungsalternativen für das Management von Informations- und IT-Sicherheit in der betrieblichen Umgebung.

---

### Zielgruppe

- Geschäftsleitung
  - IT-Verantwortliche
  - Informationssicherheitsbeauftragte
  - Datenschutzbeauftragte und -koordinatoren
  - Manager
- 

### Voraussetzungen

IS Management-Erfahrung

---