



CSET Cyber Security Essentials for Technologists

Der Workshop führt die Teilnehmer in das Thema IT-Security anhand einer Übersicht aktueller Gefährdungen und Entwicklungen, sowie des SANS / CIS Critical Security Controls Standards ein. Details bzgl. aktueller War-Stories, Security Operations Central Essentials sowie das Thema Ransomware-safe Backup Management runden das Thema ab.

Listenpreis

2.890,00 € exkl. MwSt
3.439,10 € inkl. MwSt

Dauer

3 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
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.

Lernen Sie in diesem Kompakt-Seminar die wichtigsten Sicherheitsmechanismen und Tools kennen und wie Sie Ihr Unternehmen effizient schützen können.

- **Einführung in aktuelle Gefährdungen und Entwicklungen**
 - Internet / Deep Web / Dark Web
 - Threat Actors / Nation-State Threats & TTPs
 - Important Developments
- **SANS / CIS Critical Security Controls**
 - Inventory of Authorized and Unauthorized Devices
 - Inventory of Authorized and Unauthorized Software
 - Continuous Vulnerability Assessment and Remediation
 - Controlled Use of Administrative Privileges
 - Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
 - Maintenance, Monitoring, and Analysis of Audit Logs
 - Email and Web Browser Protection
 - Malware Defenses
 - Limitation and Control of Network Ports, Protocols, and Services



- Data Recovery Capability
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Boundary Defense
- Data Protection
- Controlled Access Based on Need to Know
- Wireless Device Control
- Account Monitoring and Control
- Security Skills Assessment and Appropriate Training to Fill the Gaps
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises
- **War-Stories**
- **Ransomware-safe Backup Management**
- **Security Operation Center Essentials**

Ziele

Der Workshop führt die Teilnehmer in das Thema IT-Security anhand einer Übersicht aktueller Gefährdungen und Entwicklungen, sowie des SANS / CIS Critical Security Controls Standards ein.

Details bzgl. aktueller War-Stories, Security Operations Central Essentials sowie das Thema Ransomware-safe Backup Management runden das Thema ab.

Die Teilnehmer lernen die Sicht eines Angreifers, dessen Methoden und Vorgehensweisen sowie ein breites Tool-Arsenal kennen, welches Sie in weiterer Folge zur Überprüfung der Sicherheit und zum Schutz Ihres Unternehmens selbstständig anwenden können.

Zielgruppe

- IT-(Sicherheits-)Verantwortliche
- Informationssicherheitsbeauftragte
- IT-Kräfte, Interessierte

Voraussetzungen

- **Grundlagen in**
 - Betriebssysteme (Windows/Unix)
 - Netzwerkgrundlagen (TCP/IP)
- **oder Seminar ADS & RSBM**