CST ACADEMY

CYBER SECURITY TRANSFORMATION

AUS- UND WEITERBILDUNG

UNSER ANGEBOT FÜR IHR UNTERNEHMEN

Erwiesenermaßen trägt der Aufbau von Wissen und Kompetenz zum Thema Informationssicherheit erheblich zum Schutz Ihres Unternehmens vor Angriffen bei. Das Training Ihrer Mitarbeiter*innen ist dabei ein entscheidender Baustein. Wir haben aus diesem Grund unser Know How aus langjähriger Erfahrung in der Analyse und Beratung von IT-Security-Themen in unsere Seminare, Trainings und Workshops einfließen lassen. So ist es uns möglich, ein breites Angebot an individuellen Schulungsformaten für ganz unterschiedliche Zielgruppen anzubieten.

Die Mission der CST Academy ist es, Expertenwissen dahin zu vermitteln, wo es gebraucht wird, und Kompetenz aufzubauen um gemeinsam stärker gegen potentielle Angreifer zu sein. Vom Studierenden bis zum Topmanager. Diese Übersicht an Aus- und Weiterbildungsmaßnahmen vereint und reflektiert genau dies, und darauf bin ich stolz.

Verschaffen Sie sich einen Überblick und suchen Sie sich das geeignete Format für Sie und Ihre Mitarbeiter*innen aus. Sollte noch nicht das genau passende dabei sein, sprechen Sie uns einfach an.

In unserem **Eventkalender** finden Sie aktuelle Termine zu vielen Seminaren, Webinaren und Workshops. Abonnenten unserer **CST Academy News** haben zudem den Vorteil, regelmäßig persönliche Einladungen zu bevorstehenden oder neuen Veranstaltungen zu erhalten.

Mareike Gass
CST Academy
Telefon: +49 6102 8631–550
Mail: academy@usd.de

Unsere Empfehlungen

Organisational Security Professional

- Modul 1
- Modul 5
- Modul 6
- Modul 7
- Modul 8
- Modul 10
- Modul 12
- Modul 20

Technical Security Professional

- Modul 5
- Modul 13
- Modul 14
- Modul 15
- Modul 16
- Modul 17
- Modul 18
- Modul 20

Alle Module können Sie in Reihenfolge und Anzahl individuell buchen. Wir haben für Sie Kombinationsmöglichkeiten für eine Spezialisierung zusammengestellt. Gerne stehen wir Ihnen darüberhinaus bei der Auswahl passender Module zur Seite, um ein auf Ihr Unternehmen zugeschnittenes Aus- und Weiterbildungsprogramm zu definieren.

Fachseminare, Workshops, Vorträge und Trainings

Modul 1: usd Basic Seminar: Einführung eines ISMS nach ISO 27001

Standards wie ISO 27001 geben Anhaltspunkte für die Implementierung eines strukturierten Informationssicherheitsmanagementsystems. Aber wie geht man vor? Wie kann man die Thematik im eigenen Unternehmen etablieren? Unser Seminar vermittelt das notwendige Basiswissen, erstes Handwerkszeug für die Einführung und Best Practices für die Weiterentwicklung.

6 - 8 Stunden

für Berufseinsteiger geeignet

Einzelplatz / Individuelles Gruppen-Seminar vor Ort / Individuelles Online-Gruppen-Seminar

keine Einschränkungen / max. 12 Personen

Modul 2: usd Basic Seminar: Grundlagen des PCI DSS

Mit dem Payment Card Industry Data Security Standard (PCI DSS) hat die Kreditkartenindustrie einen international gültigen Sicherheitsstandard herausgegeben. Die darin enthaltenen Sicherheitsanforderungen folgen Best Practice Ansätze und dienen dem Schutz von Kreditkartendaten. Seit 2004 ist PCI DSS verbindlich für alle Unternehmen, die Kreditkartendaten speichern, verarbeiten oder weiterleiten. Das Seminar vermittelt Ihnen das nötige Hintergrund- und Basiswissen zum Standard und unterstützt Sie so bei der erfolgreichen Planung und Durchführung Ihres PCI DSS Projektes.

6 - 8 Stunden

für Berufseinsteiger geeignet

Einzelplatz / Individuelles Gruppen-Seminar vor Ort / Individuelles Online-Gruppen-Seminar

keine Einschränkungen / max. 12 Personen

Modul 3: PCI Best Practice Workshop Online

Inzwischen eine feste Tradition: Mindestens zweimal jährlich informieren wir in unserer Rolle als akkreditierter PCI Assessor über Neuigkeiten rundum die PCI Standards und vermitteln praxisnahes Wissen für die Umsetzung im Unternehmen. Dieser interaktive Workshop bietet Ihnen die Möglichkeit, Fragen an unsere erfahrenen QSA zu stellen und Erfahrungen mit PCI-Verantwortlichen aus anderen Unternehmen auszutauschen.

2 - 3 Stunden

Einzelplatz

PCI-Compliance-Verantwortliche im Unternehmen

Modul 4: usd Basic Seminar: Sichere Entwicklung von Webanwendungen

Die Sicherheit auf Applikationsebene gewinnt zunehmend an Bedeutung. Heute geraten Webapplikationen immer häufiger in den Fokus von Hackern und Kriminellen und stellen die Ursache zahlreicher, aktueller Sicherheitsvorfälle dar. Unsere Sicherheitsexperten haben daher dieses Seminar als Einstieg in das Thema entwickelt: Von der sicheren Softwareentwicklung über die Identifikation von Schwachstellen bis hin zum Erlernen geeigneter Gegenmaßnahmen. In diesem Seminar lernen Sie die Grundlagen kennen.

- 6 - 8 Stunden
- Einzelplatz / Individuelles Gruppen-Seminar vor Ort / Individuelles Online-Gruppen-Seminar
- Softwareentwickler, Qualitätsmanager und IT-Sicherheitsexperten (grobe Grundkenntnisse in der Entwicklung von Webanwendungen erforderlich) / max. 12 Personen

Modul 5: usd Advanced Seminar: Sichere Entwicklung von Webanwendungen

Dieses Seminar gibt einen tiefergehenden Einblick in das Thema Secure Coding. Denn heute geraten Webapplikationen immer häufiger in den Fokus von Hackern und Kriminellen und stellen die Ursache zahlreicher, aktueller Sicherheitsvorfälle dar. Innerhalb von 2 Tagen kombinieren unsere Sicherheitsexperten die theoretischen Inhalte des gleichnamigen usd Basic Seminars mit praktischen Übungen für die Teilnehmer.

- 2 Tage
- Individuelles Gruppen-Seminar vor Ort
- Softwareentwickler, Qualitätsmanager und IT-Sicherheitsexperten (grobe Grundkenntnisse in der Entwicklung von Webanwendungen erforderlich) / max. 12 Personen

Modul 6: Incident Response Tabletop

Datendiebstähle und Hacker-Angriffe auf Unternehmen geschehen fast täglich. Dass Ihre Mitarbeiter in einem solchen Fall zügig und eingespielt reagieren, ist zum Schutz Ihres Unternehmens entscheidend. Wie gut das funktioniert, ist ein Maß für die Qualität Ihres Incident-Response-Plans. Wie verhalten sich Ihre Mitarbeiter im Notfall? Wo liegen notwendige Dokumente? Wer hat welche Aufgabe?

Im Incident Response Tabletop spielen Ihre Mitarbeiter gemeinsam mit einem unserer Experten festgelegte Notfallprozesse durch und gewinnen somit an Sicherheit für den Ernstfall. Ein weiterer Vorteil: Dieser Workshop erfüllt Compliance-Anforderungen gängiger IT-Security-Standards: IT-Grundschutz des BSI, PCI DSS, ISO/IEC 27001:2013 und weitere. Die Basis für den Incident Response Tabletop bildet ein auf Ihr Unternehmen ganz individuell zugeschnittener Incident. Gemeinsam mit Ihnen erarbeiten wir im Vorfeld ein passendes Szenario, das Ihre Richtlinien und Prozesse miteinbezieht.

Hier finden Sie **mehr Informationen** zur Vorgehensweise.

Individueller Workshop vor Ort / Individueller Online-Workshop

Chief Information Security Officer, IT-Security Manager, BCM-Verantwortliche Mitarbeiter, CERT-Mitarbeiter, Applikationsverantwortliche, IT-Infrastruktur Mitarbeiter / max. 12 Personen

Modul 7: Live Hacking Demonstration

Wie kaum eine andere Methode demonstriert das Live Hacking eindrücklich und zugleich unterhaltsam, wie einfach es ist, sich Zugang zu Daten Dritter zu verschaffen oder andere auszuspionieren. Ob einzeln oder in eine bestehende Veranstaltung integriert, Live Hacking ist der ideale Weg, Mitarbeiter in Ihrem Unternehmen zu sensibilisieren. Wir bieten ein großes Portfolio an Live-Hacking-Themen, die einzeln oder kombiniert ideal auf die Zielgruppe und deren Bedürfnisse zugeschnitten werden.

Hier finden Sie unseren **Themenkatalog**.

2 Stunden

für Berufseinsteiger geeignet

Individuelle Veranstaltung vor Ort / Individuelle Online-Veranstaltung

keine Einschränkungen / max. 25 Personen

Modul 8: Ausflug ins Darknet

Was ist das Darknet? Wie funktioniert es? Wird es nur für illegale Zwecke genutzt? Zwei Sicherheitsexperten vermitteln, was das sogenannte Dark net ist, wie der Zugriff darauf funktioniert und wie es von Kriminellen genutzt wird. Während eines Live-Zugriffs über den TOR-Browser wird außerdem gezeigt, welche „Produkte" über das Darknet angeboten werden und welche Assets in diesem Zusammenhang besonders schützenswert sind.

2 Stunden
für Berufseinsteiger geeignet
Individuelle Veranstaltung vor Ort / Individuelle Online-Veranstaltung
keine Einschränkungen / max. 25 Personen

Modul 9: (Web-Based-Training) Phishing für Banken

Dieses Training, abrufbar auf unserer Security-Awareness-Plattform, ist speziell auf die Bedürfnisse von Bankmitarbeitern zugeschnitten. Praktische Beispiele aus der Branche helfen den Mitarbeiterinnen und Mitarbeitern, Phishing-Angriffe in ihrem Alltag zu erkennen und abzuwehren.

individuelle Bearbeitung
für Berufseinsteiger geeignet
Einzelbearbeitung auf der Security-Awareness-Plattform
keine Einschränkungen

Modul 10: (Web-Based-Training) Informationssicherheit für Data Owner

Regulatorische Anforderungen nehmen vermehrt Data Owner in die Pflicht, wenn es um den Schutz unternehmerischer Assets geht. Mit diesem Training, abrufbar auf unserer Security-Awareness-Plattform, bereiten wir Data Owner auf ihre neue Rolle vor und erklären, welche Aufgaben auf sie zukommen.

individuelle Bearbeitung
für Berufseinsteiger geeignet
Einzelbearbeitung auf der Security-Awareness-Plattform
Data Owner / Applikationsverantwortliche, BISOs, CBISOs

Modul 11: (Web-Based-Training) Datenschutz

Was muss ich beim Umgang mit personenbezogenen Daten beachten? Was bedeuten Aufbewahrungsfristen, Meldepflichten und TOMs? In unserem Training auf der Security-Awareness-Plattform oder als Präsenzseminar beantworten wir diese und weitere Fragen, damit Ihre Mitarbeiter die gesetzlichen Anforderungen erfüllen können.

 individuelle Bearbeitung  für Berufseinsteiger geeignet

 Einzelbearbeitung auf der Security-Awareness-Plattform

 keine Einschränkungen

Modul 12: Training: Schutzbedarfsfeststellung in der Rolle des BISO

Regulatorische Anforderungen nehmen vermehrt Data Owner in die Pflicht, wenn es um den Schutz unternehmerischer Assets geht. Mit diesem Training wird individuell auf die Rollen und Pflichten der Applikationsverantwortlichen eingegangen und der Informationssicherheits-Compliance-Evaluierung-Prozess (ISCE) ganzheitlich vermittelt.

 4 Stunden  für Berufseinsteiger geeignet

 Individueller Workshop vor Ort / Individueller Online-Workshop

 Data Owner / Applikationsverantwortliche, BISOs, CBISOs / max. 12 Personen

Modul 13: Training: Security Champions

Bei der Einführung von DevSecOps-Methodiken ist einer der Erfolgsfaktoren, die Akzeptanz der Sicherheitsorganisation im Unternehmen zu fördern. Wir empfehlen daher die Schulung und Etablierung von qualifizierten Ansprechpartnern für Sicherheitsfragen (sogenannte „Security Champions“) direkt in der IT- und Projektorganisation. Security Champions reduzieren die Hemmschwelle vor dem Kontakt mit der Sicherheitsorganisation und kennen die Pain-Points der jeweiligen IT- und Projektorganisation verwenden.

 4 Termine à 2 Stunden zzgl. Hausaufgaben

 Individueller Workshop vor Ort / Individueller Online-Workshop

 Mitarbeiter in den IT- und Projektorganisationen / max. 12 Personen

Modul 14: Seminar: Grundlagen der IT Security

Die Situation rund um IT-Sicherheit ist kritischer denn je. Angreifer werden immer stärker und entwickeln immer komplexere Angriffsmethoden. Je mehr Kolleginnen und Kollegen sich mit dem Thema IT-Sicherheit beschäftigen und die Grundlagen beherrschen, umso besser sind Sie vorbereitet. Dieses Gruppenseminar mit Theorieinhalten, kritischen Diskussionen und der Betrachtung praxisnaher Fallstudien bildet eine tolle Grundausbildung. Wie erkennt man Bedrohungen? Welche entsprechenden Gegenmaßnahmen kann man auf organisatorischer und technischer Ebene festlegen? Wie könnten Konzepte für ein umfassendes Sicherheitsmanagement aussehen?

6 Termine à 3 Stunden

für Berufseinsteiger geeignet

Individuelles Gruppen-Seminar vor Ort / Individuelles Online-Gruppen-Seminar

keine Einschränkungen / max. 12 Personen

Modul 15: Training: Sicherer Systembetrieb

Dieses Training vermittelt wichtige Security-relevante Inhalte für Administratoren im Systembetrieb. Es werden gängige Fragen und Problemstellungen dieser Zielgruppe betrachtet, sowie das allgemeine Verständnis für System Hardening, Patch- und Change-Management sowie Alerting und Überwachung verbessert.

6 - 8 Stunden

Individueller Workshop vor Ort / Individueller Online-Workshop

IT-Administratoren für Linux und Windows / max. 12 Personen

Modul 15A: Training: PCI DSS – Technical Scoping für Administratoren

Dieses Training vermittelt wichtige PCI DSS- und Security-relevante Inhalte für Administratoren im Systembetrieb. Es werden gängige Fragen und Problemstellungen dieser Zielgruppe betrachtet, mit besonderem Fokus auf Systeme im PCI Scope: Typische Systeme im Scope, Anforderungen an diese Systeme und regelmäßig wiederkehrende Anforderungen.

6 - 8 Stunden

Individueller Workshop vor Ort / Individueller Online-Workshop

IT-Administratoren für Linux und Windows / max. 12 Personen

Modul 16: Betreuung von Pentest-Verantwortlichen im Unternehmen

Wir unterstützen beratend bei der initialen Implementierung eines Prozesses zur Überprüfung von Schwachstellen im Kontext von technischen Sicherheitsanalysen, von der Einweisung bzw. der Einarbeitung der verantwortlichen Mitarbeiter im Kontext eines Pentest-Workflows bis zur Etablierung eines kontinuierlichen Schwachstellenmanagements.

- individuelle Bearbeitung
- Coaching vor Ort / Online-Coaching
- Verantwortliche Mitarbeiter im Kontext eines Pentest-Workflows

Modul 17: Praktikum bei einem usd HeroLab Pentester

Können Unbefugte in Ihre Systeme und Applikationen eindringen? Um dies zu testen, haben Sie die Security Analysten des usd HeroLabs beauftragt. Dieser nutzt zur Informationsbeschaffung professionelle Werkzeuge und versucht gezielt, individuell und erfinderisch, in Ihre Systeme und Applikationen einzudringen. Diese Simulation eines realen Angriffs liefert qualitativ hochwertige Ergebnisse für Sie.
Unser Praktikum bietet Ihnen eine einmalige Chance: Lesen Sie nicht nur abschließend den Pentestbericht, son-dern schauen Sie sich gemeinsam mit dem verantwortlichen Pentester live in Ihrem System oder Ihrer Applikation an, wie er vorgegangen ist und welche Schwachstellen er aufgedeckt hat.

- individuell und zielgruppenorientiert
- Praktikum vor Ort / (Online-Praktikum auf Anfrage)
- Verantwortliche für die zu untersuchenden Systeme und Anwendungen

Modul 18: usd Advanced Seminar: Understanding A Hacker's Mind

Ein toller Einstieg ins Thema Pentesting. Nur wenn Sie die relevanten Bedrohungen in IT-Systemlandschaften kennen und verstehen, können Sie wirksame Gegenmaßnahmen treffen. In unserem usd Advanced Seminar zeigen wir Ihnen mithilfe von Theorie und viel Praxis, mit welchen Intentionen, Methoden und Tools ein Hacker vorgeht und gehen darauf ein, wie Sie Ihre Systeme bestmöglich schützen können.

- 2 Tage
- für Berufseinsteiger geeignet
- Individuelles Gruppen-Seminar vor Ort
- Systemadministratoren, IT-Betriebsverantwortliche, Information Security Officers (ISOs). Es eignet sich grundsätzlich aber auch für alle anderen IT-Security-Interessierten, die verstehen möchten, wie Angreifer vorgehen und wie man die eigenen IT-Systeme gegen solche Angriffe schützt. Ein Grundverständnis von technischen Aspekten der IT sollte mitgebracht werden, um den Praxisbeispielen folgen zu können / max. 12 Personen

Modul 19: usd PentestLab

Das PentestLab ist das Herzstück unserer Technologie-Umgebung. Mit einer ständig wachsenden Anzahl vorkonfigurierter Serverumgebungen, unterschiedlicher Technologien und Schwachstellen verschiedener Schwierigkeitsgrade, können Pentester ihr methodisches Können, ihre Kreativität und ihr Durchhaltevermögen im „Real life Pentesting“ trainieren. Die Plattform wird von unseren eigenen Pentestern für Aus- und Weiterbildung genutzt und ist zudem die technische Basis die regelmäßig stattfindenden Hackertage an Hochschulen und in der CST Academy.

- individuelle Bearbeitung
- Einzelbearbeitung
- Kenntnisse in Kali Linux und der Arbeit mit virtuellen Maschinen ist erforderlich. Dieses Modul ist eine tolle Ergänzung zu den Modulen 18 und 22.

Modul 20: Theorie-Seminar: Einführung in Pentesting

Während eines Penetrationstest, kurz Pentest, schlüpft der durchführende Analyst in die Rolle eines Angreifers. Bevor er überhaupt einen Angriff starten kann, braucht es eine gründliche Vorbereitung: Der Pentester muss die entsprechenden Kali-Linux Tools beherrschen und genügend Informationen zum Zielsystem und bekannter Schwachstellen gesammelt haben. Unser Theorie-Seminar führt die Teilnehmer durch alle Phasen - von der Methodologie in Kali Linux bis zur Erstellung des finalen Pentestberichts.

- mehrere Wochen
- Individuelles Gruppen-Seminar vor Ort / Individuelles Online-Gruppen-Seminar
- IT-Security-Interessierte, die verstehen möchten, wie Pentester vorgehen. Ein Grundverständnis von technischen Aspekten der IT sollte mitgebracht werden, um den Praxisbeispielen folgen zu können / max. 12 Personen

Modul 21: Praktisches Gruppen-Seminar: Pentesting

Du möchtest nicht nur Zugang zum usd PentestLab erhalten und unsere virtuellen Maschinen übernehmen, son-dern deine Ergebnisse mit anderen diskutieren und mehr über die dort zu finden Schwachstelen lernen? Dann ist dies genau das richtige Praxisseminar für dich! Die Teilnehmer können in der abgesicherten Umgebung des usd PentestLabs Angriffsmethoden und Schutzmaßnahmen für Netzwerke, Systeme und Applikationen ausprobieren. Während festgelegter Module werden Pentest-spezifische Themen, wie beispielsweise eine Auswahl an OWASP Top 10 Web-Schwachstellen, behandelt und Ergebnisse der Praxiseinheiten besprochen.

- mehrere Wochen
- Individuelles Gruppen-Seminar vor Ort
- Kenntnisse in Kali Linux und der Arbeit mit virtuellen Maschinen ist erforderlich / max. 8 Personen

Modul 22: Veranstaltung: Hackertag

Die Teilnehmer erhalten Einblicke in den Berufsalltag eines professionellen usd HeroLab Pentesters. Die Tätigkeit fordert eine Vielzahl an Fähigkeiten. Was gehört alles dazu und wie sieht ein typischer Tag im usd HeroLab aus? Gibt es überhaupt typische Tage? Doch wir reden an dem Tag nicht nur über Hacking, wir machen es auch – gemeinsam mit den Teilnehmern. Egal ob MySQL, PHP, Axis, Tomcat, JBoss, ftp, webdav, oder snmp – eine Vielzahl an Technologien wird gemeinsam und unter Anleitung ausgebildeter Security Analysten auf Schwachstellen untersucht.

1 Tag

für Berufseinsteiger geeignet

Individuelle Veranstaltung vor Ort

Kenntnisse in Kali Linux sind erforderlich / max. 12 Personen

Community-Formate der CST Academy

Im CST Academy Eventkalender veröffentlichen wir unterjährig Formate zu aktuelle Themen und spannenden Fragestellungen für die Community.

usd Webinare

usd Webinare – kompakt, interaktiv, aktuell. Mehrmals im Jahr bieten wir einstündige kostenlose Webinare zu aktuellen oder praxisrelevanten IT-Security-Themen an. Melden Sie sich gerne als Referent*in für eines unserer Webinare und teilen Sie Ihr Expertenwissen mit der CST Academy Community.

1 Stunde für Berufseinsteiger geeignet

Online / Deutsch und Englisch / kostenlos

CST Academy Cyber Security Forum

Wir laden alle ein, sich bei diesem kompakten Abendformat zu wichtigen Entwicklungen in der Welt der Cyber Security auszutauschen und gemeinsame Handlungsfelder zu identifizieren. Unabhängig von Beruf, technischen Vorkenntnissen und Wissensstand. Vom Studierenden zum Topmanager.

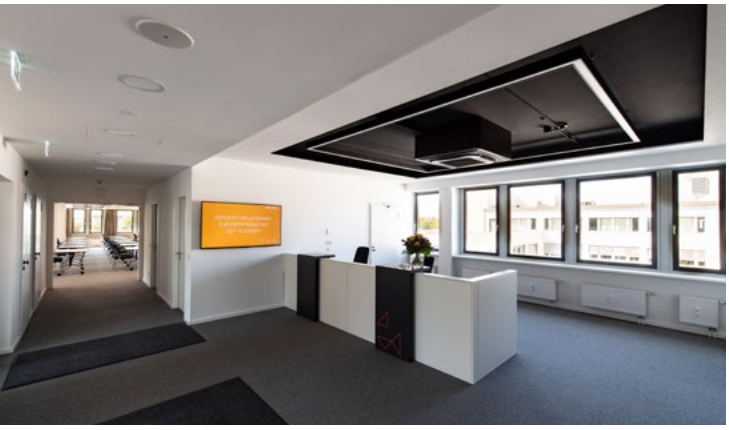
3 Stunde für Berufseinsteiger geeignet

Vor Ort / Deutsch / kostenlos

Melden Sie sich gerne als Speaker für eines unserer Cyber Security Foren und teilen Sie Ihr Expertenwissen mit der CST Academy Community.

Nutzen Sie die hochwertigen Konferenzflächen der CST Academy

Die 550 m² große klimatisierte Konferenzetage mit separatem Eingang wurde im Jahr 2018 kernsaniert und besticht durch modernste Konferenztechnik sowie lichtdurchflutete Räume zur flexiblen Nutzung. Die insgesamt drei Konferenzräume in unterschiedlichen Größen können flexibel bestuhlt werden. Der Aufenthaltsraum mit Teeküche sowie die Dachterrasse laden zum Verweilen ein.



Unsere drei Konferenzräume verfügen jeweils über modernste Konferenztechnik, Bildschirme/Leinwände sowie Beamer und sind flexibel bestuhlbar:

- 1 Plenum für ca. 60 Personen
- 1 Konferenzraum für ca. 12 Personen
- 1 Konferenzraum für ca. 8 Personen

usd AG
Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg

Telefon: +49 6102 8631-550
Mail: academy@usd.de

www.usd.de | usd.de/cst-academy