Deutsche Ausgabe

SANS EMEA

SANS ICS-SECURITY TRAININGS.

Vertrauen Sie bei Ihrer Informationssicherheit dem weltweit führenden Anbieter zur Weiterbildung und Zertifizierung.

sans.org

SANS ICS-Security –
wir sichern Sicherheit. Für heute & morgen.

Keine Frage: Die Herausforderungen an eine sichere ICS-Infrastruktur werden täglich anspruchsvoller und stets kritischer. Hier permanent auf dem neuesten Stand des Machbaren zu sein und mit den Angreifern Schritt zu halten, ist nicht nur schwieriger denn je, es ist auch so wichtig wie nie zuvor.

Damit Sie jederzeit auf der sicheren Seite sind, führt das SANS Institut speziell entwickelte Intensiv-Trainings durch. In Kursen, die sich weltweit in über 25 Jahren bewährt haben, behandeln unsere zertifizierten Dozenten Sicherheitsgrundlagen und die entscheidenden Techniken für Ihre ICS-Sicherheit.

Michael Assante

ist bei SANS der führende Kopf für ICS und Mitbegründer der NexDefense, eines ICS Sicherheits-Unternehmens. Darüber hinaus ist er tätig als Vice President und Chief Security Officer der North American Electric Reliability Corporation (NERC).

Praxisorientierte Trainings-Inhalte für den unternehmerischen Vorsprung.

Ob IT-Profi oder Ingenieur – jeder Kurs vermittelt ein praxisorientiertes Know-how, das am Arbeitsplatz sofort umgesetzt werden kann. Unsere Kursteilnehmer werden zu Cyber-Spezialisten, die jederzeit in der Lage sind, Ihre Systeme und Netzwerke effektiv zu schützen. Vor aktuellen und zukünftigen Bedrohungen.

Exklusive Fortbildung durch weltweit anerkannte Lehrkräfte.

Unsere international anerkannten SANS Trainer garantieren, dass Fachwissen auf neuestem Stand greifbar vermittelt wird. Darüber hinaus sind die Kurse so ausgerichtet, dass auch der Spaß an der Sache nicht zu kurz kommt. So veranstalten wir z. B. virtuelle Hacker-Wettbewerbe oder themenspezifische Abendvorträge, die die vermittelten Techniken direkt erlebbar machen.

Das SANS Institut
auf einen Blick:

Gegründet 1989 als Forschungs- und Weiterbildungseinrichtung

Über **25.000 IT-Sicherheitsfachkräfte** werden pro Jahr weltweit mit den Schulungen erreicht

50 verschiedene Kurse in mehr als 200 Live- und Onlineveranstaltungen jährlich

Rund **27 Berufszertifizierungen** über das angeschlossene GIAC Institut (Global Information Assurance Certification)

Bereits **mehr als 70.000 GIAC-Zertifikate** weltweit ausgegeben

Mehr unter **sans.org**

ICS 410

Dauer 5 Tage | Laptop benötigt | 30 CPE Credits | GIAC Zertifikat: GICSP

Industrieanlagen effizient schützen:
Der Grundlagenkurs „ICS410: ICS/SCADA Sicherheitsgrundlagen"

Der Kurs richtet sich an Personen, die in Umfeldern industrieller Steuersysteme tätig sind, mit solchen interagieren oder darauf Einfluss nehmen. Dazu zählen unter anderem IT-Sicherheitsfachkräfte, Betriebsverantwortliche, Ingenieure, Hersteller, Berater oder Integratoren.

Justin Searle

ist Managing Partner der UtiliSec, SANS-zertifizierter Trainer und Co-Autor des Kurses ICS410. Er ist spezialisiert in Smart Grid Sicherheits-Architektur und Penetrationstests. Er ist führend bei der Entwicklung des NIST Interagency Report 7628 und spielt eine Schlüsselrolle beim Advanced Security Acceleration Project für Smart Grid (ASAP-SG). Justin Searle hat einen MBA in International Technology und besitzt neben dem CISSP auch mehrere GIAC-Zertifizierungen.

Die Zielsetzung von Kurs ICS410:

Der Kurs ICS/SCADA Sicherheitsgrundlagen schult industrielle Fachkräfte für Cyber-Sicherheit. Sie erhalten eine Vielzahl standardisierter Kompetenzen und umfassendes Wissen für den Support und die Verteidigung von industriellen Automatisierungssystemen. So können Sie Ihr Betriebsumfeld sicher und widerstandsfähig gegenüber aktuellen und aufkommenden Cyber-Bedrohungen schützen.

Das bringt Ihnen der Kurs ICS410:

- Ein Verständnis der Komponenten, Anwendungsbereiche, Bereitstellungsformen, bedeutenden Einflussfaktoren und technischen Grenzen von industriellen Automatisierungssystemen.
- Gezielte Vermittlung von Lernerfolgen in Praxisübungen zur Kontrolle von Angriffsflächen in Systemen, sowie dafür geeignete Methoden und Tools.
- Beherrschen von systemischen Ansätzen für Architekturen und Techniken zur System- und Netzwerkverteidigung.
- Kompetenzen für die Behandlung von Security Incidents im industriellen Umfeld.
- Governancemodelle und Ressourcen für Fachkräfte in der industriellen Cybersicherheit.

Die Trainings-Inhalte von Kurs ICS410:

- Ausführen sog. Command Line Tools von Windows zum Analysieren des Systems und Durchsuchen desselben in Bezug auf hochriskante Elemente.
- Ausführen sog. Command Line Tools von Linux (Ps, Ls, Netstat usw.) und grundlegendes Scripting zum Automatisieren der Programmausführung zur fortwährenden Überwachung verschiedener Tools.
- Installieren von VMWare und Anlegen virtueller Geräte zur Erstellung eines virtuellen Labors, um die Tools / Sicherheit von Systemen zu testen und zu bewerten.
- Besseres Verstehen verschiedener industrieller Automatisierungssysteme sowie ihres Zwecks, ihrer Anwendung und Funktion, ihrer Abhängigkeiten von IP-Netzwerken und anderer industrieller Kommunikationsprotokolle.
- Arbeiten mit Betriebssystemen (Konzepte der Systemadministration für Unix-/Linux- und/oder Windows-Betriebssysteme).
- Arbeiten mit Netzwerk-Infrastrukturplanung (Konzepte für Netzwerkarchitekturen, darunter Topologie, Protokolle und Komponenten).
- Besseres Verständnis des Sicherheitslebenszyklus von Systemen.

Der GIAC Global Industrial Cyber Security Professional (GICSP) verbindet die Bereiche IT, Engineering und Cyber Security, um durchgängige Sicherheitsmaßnahmen für industrielle Automatisierungssysteme über den gesamten Systemlebenszyklus zu erreichen. Diese einzigartige, herstellerunabhängige und praxisnahe ICS-Zertifizierung ist ein Gemeinschaftsprojekt von GIAC und Vertretern eines globalen Industriekonsortiums.

Melden Sie sich an zum Live-Training ICS410:

SANS Dubai ..... 9.-14. Jan.
SANS ICS Amsterdam .... 18.-23. Apr.
SANS ICS London ..... 18.-24. Sep.
SANS Frankfurt..... 12.-17. Dez.

Weitere Live-Termine für 2016 in Vorbereitung.

ICS410 ist auch verfügbar als:

PrivateTraining* OnDemand

Die aktuellen Termine finden Sie unter **www.sans.org/find-training**

Trainings werden, sofern nicht anders gekennzeichnet, **in Englisch gehalten.**
*Es gilt eine Mindestteilnehmerzahl.
Mehr unter: www.sans.org/emea

ICS 515

Dauer 5 Tage | Laptop benötigt | 30 CPE Credits

Integration von Netz-Sicherheit in der Industrie: Der Praxiskurs „ICS515: Active Defence and Incident Response“

Der Kurs ICS515 schult in praxisorientierten Schritten das Verständnis für die aktiven Verteidigungs-Mechanismen im Zusammenspiel mit industriellen Automatisierungssystemen. Darüber hinaus vermittelt er das Wissen, wie das Erlernte im Unternehmens-Alltag genutzt werden kann, um die Bedrohungen der Cyber-Welt auszuschalten.

Robert M. Lee

ist Mitbegründer der Firma Dragos Security LLC, die sich auf Cyber Security für kritische Infrastrukturen spezialisiert hat. Er ist ein SANS-zertifizierter Trainer und der Entwickler des SANS ICS515 Kurses. Er startete in die Welt der Cyber Security in seiner Rolle als Cyber Warfare Operations Officer bei der U.S. Air Force. Robert M. Lee ist ein bekannter Verfasser von Artikeln in Fachzeitschriften wie Control Engineering oder Wired.

Die Zielsetzung von Kurs ICS515:

Mit einer strikt praxisnahen Herangehensweise erlangen die Teilnehmer das technische Verständnis, um Konzepte wie die Entwicklung und die Ausnutzung intelligenter Bedrohungen besser verstehen und bekämpfen zu können. Industrielle Fachkräfte erlangen die Fähigkeit, Ihre Netzwerk-Infrastruktur gründlich zu untersuchen und besser zu verstehen. So werden die Teilnehmer dahin gehend geschult, schädliche Akteure oder Bedrohungen des Automatisierungssystem-Netzwerkes zu identifizieren und eine zweckmäßige Verteidigung zu installieren. Das versetzt Sie in die Lage, modernste Gefährdungen zu erkennen und auch während des Betriebs schnell darauf zu reagieren.

Das bringt Ihnen der Kurs ICS515:

- Erfahrungen mit dem CYBATIWorks Praxis-Kit und virtuelle Maschinen mit PeakHMI.
- Kenntnisse mit den Tools Snort und Bro zum Anpassen und Tunen der Intrusion Detection Systemregeln.
- Wireshark und TCPDump für die Erfassung des Netzwerkverkehrs und die Paketanalyse.
- Nutzung von FTK Imager und MD5Deep zur Erhebung und Überprüfung forensischer Daten.
- OpenIOC und YARA, um Ausgleichs-Indikatoren zu entwickeln.
- Xpilco und NetworkMiner für die Analyse von Netflow.

Die Trainings-Inhalte von Kurs ICS515:

- Das Erlangen des Verständnisses, um im Falle einer Cyber-Bedrohung die Verteidigung des Netzwerkes umzusetzen. Dies geschieht anschaulich anhand der „HAVEX“-Fallstudie oder z.B. eines CYBATI Kit Setups.
- Vermittlung einer genauen Kenntnis des Netzwerkes für die wirksame Abwehr von Angriffen und Bedrohungen. Damit verbunden die Implementierung eines leistungsfähigen Monitorings, um alle ungewöhnlichen Vorgänge und Angriffs-Taktiken zu erkennen.
- Anwendung von effektiven Taktiken in der Incident Response, um die Sicherheit und Zuverlässigkeit der Automatisierungssysteme jederzeit zu garantieren. Speziell im Hinblick auf die Sammlung hochqualitativer forensischer Daten, um Entscheidungsträgern verlässliche Handlungsempfehlungen zu geben.
- Erlernen von Fähigkeiten, um eine Bedrohung exakt zu analysieren und zielgerichtete Abwehr-Maßnahmen einzuleiten. Themen dabei sind u.a. Spear-Phishing-E-Mails oder das Erkennen von Schadsoftware mit Hilfe neuer Analyse-Techniken.
- Die erlernten Strategien, Methoden und Fähigkeiten werden im Rahmen eines intensiven Praxistags gefestigt. Dabei werden zwei verschiedene Szenarien durchgespielt, indem die Reaktion auf verschiedene Angriffe der ICS-Infrastruktur getestet und die richtige Handlungsweise trainiert wird.

Melden Sie sich an zum Live-Training ICS515:

SANS Abu Dhabi ..... 5.-10. Mrz.
SANS ICS Amsterdam .... 18.-23. Apr.
SANS ICS London ..... 18.-24. Sep.
SANS München ..... 24.-29. Okt.

Weitere Live-Termine für 2016 in Vorbereitung.

ICS515 ist auch verfügbar als:

PrivateTraining*

Die aktuellen Termine finden Sie unter **www.sans.org/find-training**

Trainings werden, sofern nicht anders gekennzeichnet, **in Englisch gehalten.**
*Es gilt eine Mindestteilnehmerzahl.
Mehr unter: www.sans.org/emea

SEC 562

Dauer 6 Tage | Laptop benötigt | 36 CPE Credits

Cyber-Krieg im Maßstab 1/87:
Praxiskurs „SEC562: CyberCity Hands-On Kinetic Cyber Range Exercise“

CyberCity aus dem NetWars Programm ist unser ambitioniertestes Kurs-Angebot. Es wurde entwickelt, um Sicherheitsverantwortliche und Ihre Vorgesetzten dahin gehend zu schulen, dass virtuelle Aktionen im Cyber-Raum signifikante Auswirkungen auf die reale Welt haben können.

Ed Skoudis

ist der Gründer von „Counter Hack“, einer innovativen Organisation, die realistische Cyber-Simulationen betreibt. Dazu gehören u.a. CyberCity oder NetWars. Als Direktor des CyberCity-Projektes leitet Ed Skoudis verschiedenste Missionen, um eine miniaturisierte Stadt zu verteidigen. Ed Skoudis hat zahllose Security-Bewertungen bei Regierungen oder Unternehmen mit den Schwerpunkten Anti-Virus oder Anti-Spyware durchgeführt. Zudem bloggt er regelmäßig über das Thema Penetrationstests.

Die Zielsetzung von SEC562 CyberCity Hands-On:

Computer-Technologien, Netzwerke oder industrielle Steuersysteme drängen nahezu in jeden Bereich des modernen Lebens. Von Unternehmens-Organisationen über das Militär bis hin zu Regierungen. CyberCity bildet diese Umgebungen im Maßstab 1:87 nach, um die ständig wachsenden Ansprüche an geeignete Sicherheitssysteme zu schulen und entsprechende Kenntnisse zu trainieren. Damit sich Fälle wie der Hacker-Angriff auf ein deutsches Stahlwerk möglichst nicht wiederholen.

Das bringt Ihnen SEC562 CyberCity Hands-On:

CyberCity ist eine echte Stadt – allerdings im gängigen Eisenbahn Maßstab H0. Wie in der Realität verfügt CyberCity über eine SCADA-kontrollierte Stromversorgung, über eine Wasserversorgung, Verkehrssysteme, Krankenhäuser, Banken, Einzelhandel und Wohngebiete. CyberCity trainiert die Teilnehmer anhand der verkleinerten Umgebung, wie Ihre Stadt gegen Angriffe von Cyber-Terroristen bestmöglichst verteidigt werden kann. Darüber hinaus wird lebensnah demonstriert, wie verlorengegangene entscheidende Kontroll-Möglichkeiten zurückgewonnen werden können.

Die Trainings-Inhalte von SEC562 NetWars CyberCity:

- Demonstriert Sicherheitsverantwortlichen und Ihren Vorgesetzten in 15 Missionen die realen Auswirkungen von virtuellen Cyber-Angriffen.
- Entwickelt die Fähigkeiten zur Verteidigung und Rückgewinnung der Kontrolle über entscheidende Infrastrukturen wie Wasserwerke oder das Power Grid.
- Einsatz gängiger Analysetools in einer ICS/SCADA-Umgebung, einschließlich Analyse und Manipulation weit verbreiteter aber meist wenig verstandener Protokolle wie Profinet, DNP3 und Modbus
- Capture-the-Flag Challenge am letzten Kurstag, in der ein Angreifer- und ein Verteidigungsteam in einem fiktiven Cyber-Krieg gegeneinander antreten.

Melden Sie sich an zum Live-Training SEC562:

SANS ICS London ..... 18.-24. Sep.

Weitere Live-Termine für 2016 in Vorbereitung.

SEC562 ist auch verfügbar als:

PrivateTraining*

Die aktuellen Termine finden Sie unter **www.sans.org/find-training**

Trainings werden, sofern nicht anders gekennzeichnet, **in Englisch gehalten.**
*Es gilt eine Mindestteilnehmerzahl.
Mehr unter: www.sans.org/emea

STH

Security Awareness Programm | 5 Themengebiete | modulare Videos | mehrsprachig

Verbessern des menschlichen Sicherheitsbewusstseins: SANS Securing the Human

Das Security Awareness Programm „Securing The Human“ wurde geschaffen, um Nicht-IT-Fachkräften computerbasierte Schulungen zur Entwicklung des Sicherheitsbewusstseins bereitzustellen. Die Produktlinie wurde konzipiert, um Endnutzer, Entwickler, ICS-Ingenieure, Anwender aus dem Versorgungswesen und dem Gesundheitsmarkt gleichermaßen zu schulen.

Lance Spitzner

ist ein international anerkannter Vordenker im Bereich der Forschung von Bedrohungen aus der Cyber-Welt. Lance Spitzner erwarb seinen MBA an der Universität von Illinois/Chicago und hat weltweit zahllose multikulturelle Security-Awareness-Programme entwickelt und eingeführt. Zu den Auftraggebern zählen Unternehmen von 60 bis über 100.000 Mitarbeitern. Er ist Gründer des Honeynet-Projektes, Autor zahlreicher Fachtitel und der Verfasser von mehr als 30 Whitepapern. Sein Wissen vermittel er rund um den Globus bei Veranstaltungen und Seminaren in mehr als 20 Ländern.

Die allgemeine Zielsetzung des STH-Programms:

Virtuelle Bedrohungen sind für Mitarbeiter oft nur schwer zu erkennen. Deshalb schult das STH Security Awareness Programm das menschliche Verhalten und sensibilisiert die Teilnehmer für die Risiken einer Cyber-Attacke. So können sie mögliche Gefährdungen erfolgreich managen und leicht in den Griff bekommen, selbstverständlich unter der Berücksichtigung und Beibehaltung Ihrer internen Unternehmensrichtlinien. Schlussendlich geht es darum, dass Ihre Mitarbeiter ihr Unternehmen und seine Assets jederzeit proaktiv schützen können.

Das bringt Ihnen das STH-Programm:

- Computerbasierte Schulungen gestatten es Mitarbeitern, Schulungen zu einer ihnen beliebigen Zeit an einem von ihnen gewünschten Ort zu absolvieren.
- Kurze, modular aufgebaute Videos erlauben es Mitarbeitern, Schulungen in mehreren kurzen Sitzungen durchzuführen.
- Eine Auswahl aus zahlreichen Modulen ermöglicht, dass Schulungen maßgeschneidert werden und somit spezifische Zielgruppen wie Ingenieure angesprochen werden können.
- Kurze Quizfragen während der Schulung testen das Verständnis der Lernenden.
- Schulungsabschlüsse können für Compliance-Reportings nachverfolgt werden.
- Optionale Sprachvarianten bieten konsistente Schulungen in Ihrem gesamten Unternehmen – unabhängig vom regionalen Standort.

Die Trainings-Inhalte des STH.Engineer Programms:

- Entwickeln eines prinzipiellen Verständnisses, wie ein Automatisierungssystem unter Cyber-Sicherheits-Gesichtspunkten im Detail verwaltet wird und mit anderen Systemen verflochten ist.
- Aufzeigen eines beispielhaften Überblicks über im „Trend“ liegende ICS-Angriffsvarianten sowie die möglichen Angreifer. Darüber hinaus Veranschaulichung denkbarer Angriffsziele innerhalb des ICS-Systems.
- Arbeiten mit verschiedenen Konzepten im Rahmen der Server- und Netzwerksicherheit. Zielsetzung ist die Schulung der Teilnehmer, um die ICS-Umgebung auf den verschiedenen Serverebenen verteidigen zu können.
- Schulung der Fähigkeiten bei allen Mitarbeitern, die mit der ICS-Umgebung interagieren, um im Falle eines Störfalles die richtigen Informationen weitergeben zu können.
- Veranschaulichung eines fiktiven Angriffs-Szenarios in einem Schritt-für-Schritt-Ablauf. Extrem realistisch aus der umgekehrten Sicht des Cyber-Angreifers dargestellt.
- Trainieren grundsätzlicher Fähigkeiten, um beim ICS-System Tätigkeiten wie z.B. Patching, Backup-Erstellungen, Change-Management, Monitoring oder Logging vornehmen zu können.
- Vermittlung von ICS-fokussierten Sicherheits-Konzepten wie Risiko-Management, Account-Management, Daten-Klassifizierung und der tiefgehenden Netzwerk-Verteidigung.

Erfahren Sie mehr über das Programm STH Securing the Human:

Gerne besprechen wir Ihre individuellen Anforderungen und stellen Ihnen eine kostenlose Demo zur Verfügung.

Sprechen Sie uns einfach an.

Tel: **+49 89 950 85 769**
Email: **germany@sans.org**

Alle Details auch unter:
www.securingthehuman.org

Bei der Sicherheit jederzeit up to date – und das sogar kostenlos!

SANS EMEA

Melden Sie sich für Ihren SANS Portalzugang an.

Mit dem SANS Portalzugang erhalten Sie brandaktuelles Insider-Wissen mit kostenlosen Webcasts, Newslettern und Updates zum Thema Cyber-Security.

Profitieren Sie von:

SANS NewsBites

Ein halbwöchentlicher High-Level Executive Summary der wichtigsten Newsartikel zum Thema Computersicherheit.

@RISK: The Consensus Security Alert

bietet eine wöchentliche Zusammenfassung von:

- Neu entdeckten Angriffsvektoren.
- Verwundbarkeiten durch aktive und neue Exploits.
- Erklärungen zur Funktionsweise aktueller Attacken.

OUCH!

ist der erste monatliche Security Awareness Konsensreport für Endanwender. Er zeigt, worauf man achten muss und wie man Phishing und andere Betrügereien vermeiden kann – einschließlich Viren und anderer Malware. Praxisnah gezeigt am Beispiel jüngster Angriffe.

SANS Webcasts

zur Informationssicherheit sind Live-Broadcasts im Internet, in denen bekannte Sprecher aus der Branche wissenswerte Themen präsentieren. So bleibt Ihr Wissen über die Cyber-Sicherheit immer up to date.

Jetzt kostenlos anmelden auf sans.org

Kontakt:

SANS Institut
Theatinerstr. 11
80333 München

Tel: +49 89 950 85 769
Email: germany@sans.org
Web: www.sans.org