Deutsche Ausgabe

SANS EMEA

www.sans.org
@SANSEMEA

IT SECURITY TRAININGS 2017

Cyber Defence, Digitale Forensik, Incident Handling, Penetrationstests, Ethical Hacking, Sicherheit für Industrielle Kontrollsysteme, Management & Auditing

GIAC

Contact SANS EMEA

Middle East
Ned Baltagi
Managing Director, ME & GCC regions
nbaltagi@sans.org

UK & Nordics
Stephen M Jones
Managing Director, UK & Nordics
sjones@sans.org

Mainland Europe
Jan-Pieter Spaans
Managing Director, Mainland Europe
jspaans@sans.org

Ein paar Worte zu SANS,

Auch in diesem Jahr sehen wir eine Zunahme an Trainingsveranstaltungen in Europa und dem Mittleren Osten, zurückzuführen auf die wachsende Nachfrage nach SANS Trainings. Über das Jahr 2017 werden wir daher in Deutschland, Frankreich und Spanien mehr Trainings ausliefern als je zuvor. Neben unserer bisherigen Präsenz in Europa freuen wir uns, jetzt auch unser komplettes Portfolio zusätzlich an den Standorten Zürich, Paris und Madrid anzubieten.

Bezogen auf unsere mehrsprachigen Trainingsangebote haben wir unser SANS Security Awareness Programm „Securing The Human" komplett überarbeitet und bieten nun ein neues Learning Management System an, das ein modulares online video training in 19 verschiedenen Sprachen beinhaltet. Das speziell auf das SANS Security Awareness Programm ausgerichtete Team ist in der Lage, neben kostenfreien Demos auch eine Beratung anzubieten, falls es in diesem Bereich ein besonderes Interesse gibt.

Die Regierungen Frankreichs und Großbritanniens haben beschlossen, dem Bereich Cyber Security eine besondere Priorität zu geben und ihre Budgets entsprechend erhöht, um die notwendigen Schritte zur Bekämpfung von Cyber Crime einzuleiten. SANS unterstützt diese großangelegten Initiativen und hat bereits begonnen, Großbritannien bei der Implementierung ihrer neuen Strategie zu begleiten. Es wurde eine Cyber Retraining Academy in Partnerschaft mit der Regierung (HM Government) erfolgreich gestartet. Unsere bisherigen Cyber Academy Initiativen haben gezeigt, dass wir mit Hilfe von intensivem Training in Topqualität auch Menschen mit wenig oder keinem Cyber Security KnowHow zu zertifizierten Experten ausbilden können, die sofort in der Praxis eingesetzt werden können. Ich erwarte, dass wir dieses Programm zur Bekämpfung des Mangels an Security-Experten auch in anderen Bereichen und Ländern adaptieren und ich bin hier bereits in Diskussion mit anderen Regierungen und großen Unternehmen.

Es ist immer ein Vergnügen, die vielen Teilnehmer bei unseren Veranstaltungen zu treffen, die leidenschaftlich Ihrem Beruf nachgehen und Ihre Tätigkeit lieben. Ich hoffe, auch Sie bald bei einem unserer Veranstaltungen zu treffen.

Jan-Pieter Spaans
MANAGING DIRECTOR, MAINLAND EUROPE, SANS INSTITUTE

SANS EMEA

Das GIAC-Zertifikat - größtmögliche Klarheit beim Sicherheits-Know-how.

Die „Global Information Assurance Certification (GIAC)“ ist der führende Anbieter und Entwickler von Cyber-SicherheitsZertifizierungen. Schließlich ist ein funktionales und robustes Risiko-Management essentiell für die Sicherheit Ihres Unternehmens. Und das ist vor allem von einem abhängig: Den Kenntnissen und Fähigkeiten Ihres Sicherheits-Teams. Damit Ihr Unternehmen dabei buchstäblich auf der sicheren Seite ist, testet und belegt GIAC die Fähigkeit von Fachleuten in den verschiedenen Disziplinen der Informationssicherheit.

“GIAC IS THE ONLY CERTIFICATION THAT PROVES YOU HAVE HANDS-ON TECHNICAL SKILLS.”

Christina Ford
DEPARTMENT OF COMMERCE

“GIAC ENSURES YOU HAVE THE NECESSARY TECHNICAL SKILLS, WHICH IS HIGHLY VALUED IN ANY INDUSTRY.”

Troy Takaki
NETWORK SECURITY MANAGER, HAWAIIAN AIRLINES

Der Unterschied zu vielen Einheits-Sicherheits Zertifizierungen:

Die GIAC-Zertifizierung bestätigt dem Kurs-Absolventen exakt das Wissen über alle notwendigen Cyber-Sicherheits-Kenntnisse, um die kritische IT-Infrastruktur des Unternehmens zu schützen

Beste Perspektiven mit GIAC.

Die Absolventen und Träger des GIAC-Zertifikates sind weltweit gefragte Fachleute bei Regierungsorganisationen, Militär und in der Industrie. GIAC bietet über 30 spezialisierte Zertifizierungen in digitaler Forensik, Incident Handling, Penetration-Testing, ICS, Management & Auditing.

„SANS-Trainings sind die beste Methode, um sich auf GIAC Prüfungen vorzubereiten. Bei uns lernen die Studenten die praktischen technischen Fähigkeiten, die von GIAC bewertet werden.“

Stephen Sims, Senior SANS Instructor und Kurs-Autor

Mehr zu GIAC und Wege zur Zertifizierung auf www.giac.org

SANS-IT Security:
Global agierend -- weltweit führend.

Die Sicherheit der Informations-Technologie ist eine ständig wachsende Herausforderung für jedes Unternehmen. Seit 1989 meistert SANS diese Herausforderung. Als der global größte und damit führende Anbieter für Cyber-Sicherheit stellen wir uns täglich unserer Kernmission: dem Schutz von IT-Systemen und damit den Organisationen, die diese einsetzen!

Hierfür vermitteln wir top-aktuelles Wissen. Und zwar nicht theoretisch, sondern fokussiert auf die Praxis. Mittlerweile sind wir in über 30 Ländern aktiv und zählen 140.000 erfolg reiche Absolventen. Zu unseren Partnern zählen über 500 weltweit führende Unternehmen, Organisationen und Regierungen

SANS EMEA

Gegründet 1989 als Forschungsund Weiterbildungseinrichtung

Profi tieren Sie vom Wissen der kompetentesten Dozenten.

Unsere Dozenten kommen alle samt aus der Praxis. So können sie als echte Insider reale Erfahrungen in ihren Kursen vermitteln. Zu unserem Team zählen viele aktive Sicherheits-Experten, die für hochkarätige Organisationen tätig sind. Alle Dozenten verfügen über anerkannte technische Zertifi kate und vermitteln ihre Fachthemen mit Leidenschaft. So sind die Kurse besonders lebensnah und damit effektiv.

Bleiben Sie up to date mit top-aktuellen Trainings.

Die Bedrohung durch die Cyber-Kriminalität wächst täglich. Deshalb aktualisieren wir unsere Kurse und Lehrmaterial ständig unter der Leitung eines ExpertenGremiums. So können wir die Studenten jeder zeit für die Bedrohungen von Heute schulen und sie gleichzeitig auf kommende Gefahren vorbereiten.

Belegen Sie Kurse, die auf Ihre Bedürfnisse ausgerichtet sind.

Unsere individuellen Kurse sind ganz auf Ihre berufliche Position und Erfahrung abgestimmt. In über 60 Trainings widmen wir uns den wichtigsten Positionen in heutigen Security-Teams und damit den dortigen Aufgaben und Disziplinen.

Der SANS-Lehrplan umfasst digitale Forensik, Incident Handling, Penetrationstests, Ethical Hacking, sichere Software-Entwicklung, Sicherheit für Industrielle Kontrollsysteme, Management & Auditing und vieles mehr. Jeder Kurs bildet einen Fachmann innerhalb eines Themas von den Grundlagen direkt zum Spezialisten aus. Praktische Fallübungen vertiefen das Wissen und trainieren es zur sofortigen Umsetzung im Unternehmen.

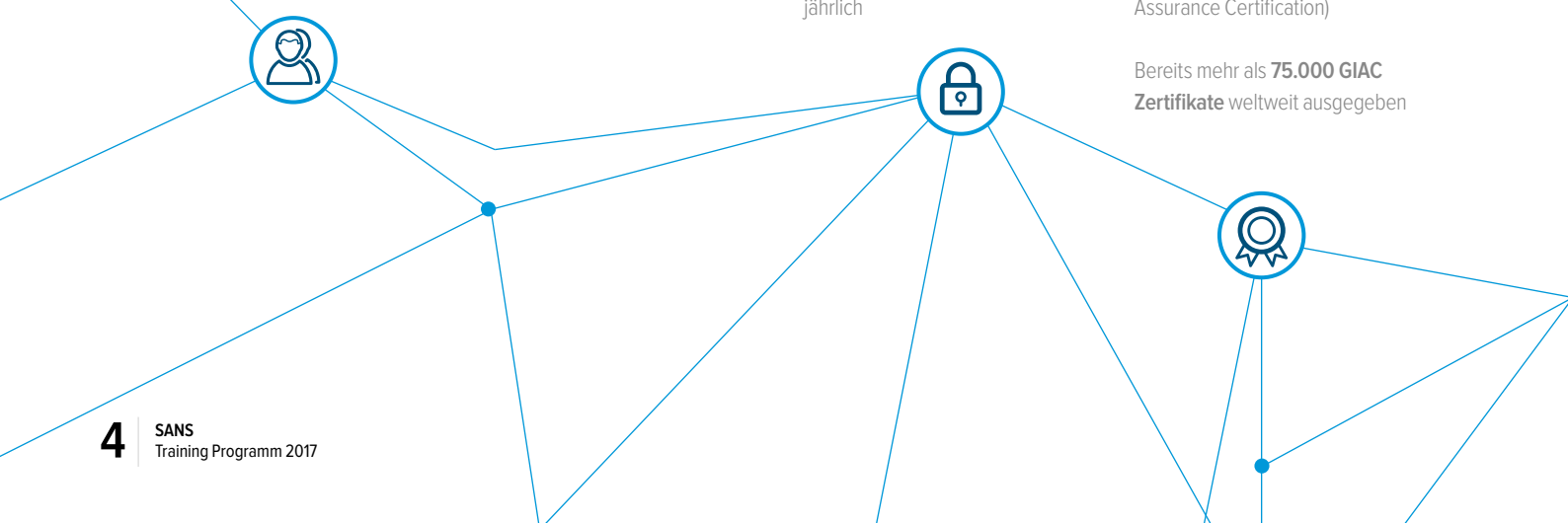
Ganz nach unserem Versprechen: Die Studenten können ihr neues Know-how sofort anwenden.

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

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

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

Bereits mehr als **75.000 GIAC Zertifikate** weltweit ausgegeben



Nutzen Sie die globale Gemeinschaft.

SANS engagiert sich in der globalen Cyber-Sicherheits Gemeinschaft. Hier betreiben wir das Internet Storm Center – das Internet Frühwarnsystem. Zudem entwickeln, führen und veröfentlichen wir zahlreiche Forschungsarbeiten zur Informationssicherheit. Diese Publikationen können Sie kostenfrei nutzen.

Lassen Sie Ihr Wissen zertifizieren – mit GIAC.

Die weltweit anerkannten GIAC-Zertifikate bestätigen ofziell das notwendige technische Wissen für die Schlüsselbereiche der Cyber-Sicherheit. GIAC (Global Information Assurance Certification) bietet die einzigen Cyber-Sicherheits-Zertifikate, die fortgeschrittene technische Themenbereiche abdecken. Es gibt über 30 verschiedene GIAC Zertifikate – z. B. unter dem ANSI/ISO/IEC 17024 Personal Zertifizierungs-Programm. Damit Sie sich auf ein GIAC-Zertifikat bestens vorbereiten können, sind viele unserer Kurse speziell auf GIAC ausgerichtet.

Registrieren Sie sich für die SANS-Schulungen.

Unsere Trainings-Events bieten den Studenten die Möglichkeit, verschiedene SANS IntensivKurse live zu besuchen. Dabei erleben Sie nicht nur ein perfektes Lernumfeld, sondern trefen auch andere Sicherheitsfachleute und etablierte SANS-Dozenten zum fachlichen Austausch.

Anmeldungen erfolgen direkt unter www.sans.org/emea

SANS-Kurse können auch online als OnDemand-Version, als Privat-Trainings innerhalb eines Unternehmens und in vielen weiteren Formaten belegt werden.

SANS IT Security – ganz sicher auch für Deutschland.

Bei der IT-Sicherheit ist es in den Unternehmen keine Frage mehr, ob man sie benötigt. Die Frage ist auch in Deutschland nur noch: Wie kann man hier das höchste Level erreichen? Die weltweit führenden SANS Cyber-Sicherheits-Trainings sind unsere Antwort darauf. In München, Berlin, Frankfurt, Hamburg oder anderen Städten Europas bringen wir Sie auf den aktuellsten Stand und zeigen Ihnen, wie Sie erlerntes Knowhow sofort in der Praxis einsetzen können.

Wir bitten um Verständnis, dass die meisten Trainings durch ihre internationale Prägung auf Englisch stattfinden. Allerdings bestätigt die Ausnahme die Regel – einige Trainings können Sie auch auf Deutsch belegen. Zu den Teilnehmern der SANS-Trainings zählen die Mitarbeiter vieler führender deutscher Unternehmen und Organisationen sowie von Regierungs-Behörden oder dem Militär.

Diese Broschüre gibt Ihnen einen ersten Überblick über unsere Kurse. Auf den letzten Seiten finden Sie eine Roadmap für Ihre Karriere in der IT-Security sowie die wichtigsten SANS-Kurse auf einen Blick.

Für weitere Informationen und Anfragen senden Sie einfach eine E-Mail an: germany@sans.org

@SANSEMEA

Mehr unter
sans.org

CURRICULUM **PEN TEST**

Die SANS-Kurse zum Penetration-Testing -

damit Sie auf alles vorbereitet sind.

SANS Penetration-Testing-Kurse zielen darauf ab, Fachleuten hochwertige Pen-Tests zu ermöglichen. Je nach Qualifikation sind sie ausgerichtet auf Anfänger, Fortgeschrittene und Experten.

DIE SANS PEN-TEST EVENTS
jedes Jahr in Berlin
mehr als 5 Kurse

Variabel wie die Gefahren selbst – das SANSPenetration-Testing:

- **Unterschiedliche Ebenen** – Wählen Sie ein Netzwerk-, Web-App-, Mobileoder Wireless-Pen-Test-Kurs.
- **Top-aktuell** – SANS aktualisiert und überarbeitet regelmäßig die Inhalte der Pen-Test-Kurse.
- **Von Experten lernen** – der gesamte Trainingsinhalt ist von einem Pen-Experten-Gremium erstellt.
- **Hochkarätige Dozenten** – SANS Pen-Test-Dozenten sind weltweit anerkannte, praxiserfahrene Experten.
- **Umfangreiches Kursmaterial** – die Studenten erhalten vielfältige Unterlagen, Bücher und Materialien.
- **Flexibler Zugang** – SANS bietet verschiedenste Wege am Training teilzunehmen.

Alle Infos und Termine auf
www.sans.org/de

CURRICULUM **FORENSIK**

Die SANS-Kurse zur digitalen Forensik und zum Incident Response -

keine Chance für Angriffe aus dem Dark-Net.

Unsere Forensik-Kurse helfen Ihnen Sicherheitslücken rechtzeitig zu erkennen. So können Sie Ihre Kunden, Mitarbeiter, Produkte und Erträge schützen, bevor etwas passieren kann. Viele der auf diese Weise bei uns ausgebildeten ForensikSpezialisten sind heute für einige der weltgrößten Unternehmen sowie für Ministerien oder Militäreinrichtungen tätig.

DIE SANS FORENSIK EVENTS
jedes Jahr in Prag
mehr als 9 Kurse

Immer auf dem neuesten Stand – die SANSForensik-Kurse:

- **Fokussiert auf Schutz** – wir vermitteln alle Fähigkeiten, um aktuellste Bedrohungen zu entdecken und wirksam darauf zu reagieren.
- **Individuelle Kursinhalte** – je nach Kenntnisstand sind die Kurse maßgeschneidert für Anfänger, Fortgeschrittene und Spezialisten.
- **Hochkarätige Dozenten aus der Praxis** – unsere Dozenten sind Forensik-Experten allererster Qualität und beruflich in diesem Fachgebiet tätig.
- **Aktuelle Inhalte** – unser Trainingsmaterial ist immer auf dem neuesten Stand der gefährlichsten digitalen Bedrohungen.
- **Praxisorientierte Kursunterlagen** – die Teilnehmer erhalten entsprechende Fachliteratur und – je nach Kurs – Software und Hardware-Material, um ihre neuen Kenntnisse sofort zu nutzen.
- **Teilnahme nach Wahl** – Studenten können ihre Trainings in einem Schulungsraum, online oder privat absolvieren.

Alle Infos und Termine auf
www.sans.org/de

CURRICULUM **ICS**

Die SANS-Kurse zu Industrie-Kontroll-Systemen ICS -

Risiken erkennen und ausschalten.

Der wirksame Schutz einer ICS-Infrastruktur birgt eine Reihe von individuellen Herausforderungen. Oft liegen die Gefahren in einer veralteten Hardware oder in personellen Strukturen, die wirksame Sicherheitsregelungen erschweren. Unsere ICS-Kurse ofenbaren Ihnen die Risiken und zeigen die Lösungen für die Praxis.

DIE SANS ICS-SECURITY EVENTS
Nehmen Sie ICS410
in München

Komplexe Zusammenhänge verstehen – das SANS ICS-Training:

- **Praxisorientiertes Training** – die Kursinhalte werden von führenden Experten auf dem Gebiet der CyberSecurity und der SCADA-Systeme zusammengestellt.
- **Training für Ingenieure** – eines der Trainings zielt speziell darauf ab, Ingenieuren ein Informations Sicherheitsverständnis zu vermitteln.
- **Training für Sicherheits-Experten** – eines der Trainings hilft speziell Sicherheitsfachleuten, die SCADASicherheit und die damit verbundenen Systeme, ihre Funktionen und Grenzen zu verstehen.
- **Umfangreiches Kursmaterial** – ICS Security-Studenten erhalten umfassende Fachliteratur und speziell dafür aufereitetes Material.

Alle Infos und Termine auf
www.sans.org/de

CURRICULUM **CYBER DEFENCE**

Die SANS-Kurse zur Cyber Defence -

wirksamer Schutz beweist sich in der Praxis.

Unsere Cyber Defence-Trainings vermitteln das spezielle Know-how, um aktuellste Bedrohungen aufzudecken und adäquat zu bekämpfen. Dabei legen wir besonderen Wert darauf, konsequent praxisorientiert und ganz nach dem individuellen Kenntnisstand der Teilnehmer zu schulen. So zeigen wir nicht nur die Theorie, sondern vor allem das Wissen für den Einsatz im täglichen Umfeld.

DIE SANS CYBER DEFENCE TRAININGS
das ganze Jahr über in größeren Städten Europas
im Rahmen der SANS Training-Events

Bedrohungen erkennen und ausschalten – mit den SANS-Cyber Defence Kursen:

- **Von Experten geleitet** – die SANSDozenten sind führende Köpfe im Bereich der Cyber Defence und stehen selbst täglich an der vordersten Position der digitalen Verteidigungslinien.
- **Teilnahme nach Wahl** – Studenten können verschiedene Trainingsarten wählen. Z. B. Einheiten im Schulungsraum vor Ort oder alternativ via Online-Zugang.
- **Auf dem neuesten Stand** – unser gesamtes Trainingsmaterial wird regelmäßig aktualisiert und um die neuesten Bedrohungs-Szenarien und Angrifs-Taktiken ergänzt.

Alle Infos und Termine auf
www.sans.org/de

Unsere einzigartigen SANS-Dozenten - weltweit führende Köpfe für Ihren Wissens-Vorsprung.

SANS-Dozenten sind Technik-Experten auf höchstem internationalen Niveau und zudem begeisternde Lehrer. Sie alle sind Spezialisten Ihres Fachgebietes und verfügen über ein charismatisches Auftreten für besonders lebendige und erfolgreiche Trainings. Darüber hinaus sind sie aktive Sicherheits-Fachleute aus der Praxis. So bringen sie reale und aktuelle Szenarios in ihre Schulungen ein.

Hier sehen Sie eine Auswahl unserer SANS-Dozenten, die für Sie aktiv sind.

Trefen Sie Experten aus Spitzen-Postionen.

Ganz gleich welches Spezialgebiet – sei es Cyber Defence, Management, DFIR, ICS, Audit, Pen-Testing, oder Software Entwicklung – SANS-Dozenten sind praxiserfahrene Cyber-SicherheitsExperten in einflussreichen Positionen prominenter Organisationen weltweit.

Erleben Sie Fachkompetenz zu jeder Zeit.

Zusammen besitzen die SANS Dozenten über 45 Sicherheits Patente und haben vielzählige hochbeachtete Bücher zur Cyber-Sicherheit verfasst. Neben ihrer beruflichen Tätigkeit sind sie u. a. stark engagiert im Bloggen oder Schreiben, um ihr FachKnow-how zu verbreiten.

James Lyne
Certified Instructor
@jameslyne

James ursprünglicher Hintergrund ist die Kryptographie, aber während der letzten Jahre war er in den unterschiedlichsten Sicherheits-Feldern tätig – einschliesslich Anti-Malware, Forensik, Incident Response und Hacking. James ist teil von Industrie-Gremien, Policy-Gruppen und ist ein weltweit vielgefragter Berater-Experte

Rob Lee
Fellow
@RobTLee

Rob hat über 15 Jahre Erfahrung in Computer Forensik, Aufdecken von Sicherheitslücken und Exploits, Ermittlung und Prävention von Systemeinbrüchen und Incident Response. In diesen Bereichen war er für die US-Luftwafe, für einige Regierungs-Agenturen und im Geheimdienst-Umfeld tätig.

Robert M. lee
Certified Instructor
@RobertMLee

Robs Leidenschaft gilt der Control System Trafc Analyse, dem Incident Response und Threat Intelligence Research. Er ist der Autor des Kurses SANS ICS515 – Active Defense and Incident Response und der Co-Autor von SANS FOR578.

Stephen Sims
Senior Instructor
@Steph3nSims

Stephen Sims ist ein Industrie Experte mit über 15 Jahren Erfahrung in Informations technologie und Sicherheit. Momentan arbeitet Stephen als Berater für Reverse-Engineering, ExploitAufdeckung, Bedrohungsmodelle und Penetrationstests.

Die SANS-Trainings-Formate - so flexibel und individuell wie Ihre Ansprüche.

Das SANS-Training ist bekannt als das umfangreichste Cyber-Sicherheits-Programm, das weltweit angeboten wird. Wir schulen die DAX 30-Firmen, Regierungs- und Verteidigungs-Organisationen sowie internationale Industriekonzerne.

Bei SANS können Sie Trainings in folgenden Formaten belegen:

- **Training-Events** – Einheiten in Schulungsraum-Umgebung, geleitet von einem SANS-Dozenten.
- **Private Trainings** – SANS-Trainings vertraulich und exklusiv in einer unserer Zentralen oder in Ihrem eigenen Schulungsraum.
- **OnDemand** – SANS-Training Online mit maximaler Flexibilität.

SANS OnDemand

Jederzeit verfügbar sind die SANS Kurse über E-Learning. Dieses Angebot beinhaltet Kursbücher oder CD/DVDs/ Toolkits und einen viermonatigen Online-Zugang zum SANS-OnDemandE-Learning-Portal.

Mehr Info unter
www.sans.org/ondemand

SANS-Privat-Training:

Dieses Training ist ideal, wenn 25 oder mehr Mitarbeiter streng vertraulich geschult werden sollen. Es findet idealerweise in den Schulungsoder Veranstaltungs-Räumen Ihres Unternehmens statt.

SANS-Training-Events:

Diese Multi-Kurs-Events finden in hochwertigen Hotels oder VeranstaltungsZentren statt. Die Training-Events verbinden „live vor Ort" Lernen und Netzwerken mit Kollegen und den SANS-Teams. Die Teilnahmegebühren beinhalten z. B. auch Pausen-Erfrischungen, Mittagessen und Abendveranstaltungen.

Auch 2016 können Sie unsere TrainingEvents in ganz Europa buchen. Aktuelle Termine und Informationen auf
www.sans.org/emea

SANS-Community in zwei Varianten

1. SANS-Schulungsraum-Unterricht mit lokalen SANS-Dozenten in deutscher Sprache, wobei die SANS-Kursunterlagen in Englisch gehalten sind.
2. Training auf Englisch innerhalb ihres lokalen Gebietes. Die Unterrichtsgruppen werden hierbei für gewöhnlich direkt durch SANS organisiert.

Mehr zu anstehenden Communities auf
www.sans.org/emea

Security-Awareness-Training:

„SANS Securing The Human" bietet Computerbasiertes Security-Awareness-Training für End-Nutzer, Ingenieure oder Entwickler an. Darüber hinaus für die Energieversorgungsund Gesundheitsindustrie. Modulare Videos vermitteln dabei einer großen Zahl an Mitarbeitern ein wirkungsstarkes Training.

www.securingthehuman.org

Das bringt Ihnen SEC401:

1. Entwicklung von VLANs, NAC und 802.1x-basierte NetzwerkArchitekturen.
2. Windows Befehle zur Analyse von Hoch-Risiko-Potenzialen im System.
3. Linux Befehle (ps, ls, netstat etc.) und basic scripting, um Programme zu automatisieren ein permanentes Monitoring durchzuführen.
4. Die Installation von VMWare und die Entwicklung von virtuellen Maschinen um ein virtuelles Lab zu schaffen, das die Sicherheit des Systems testet und evaluiert.
5. Die Entwicklung einer effektiven Strategie, die im Unternehmen eingesetzt werden kann, um eine Checkliste für valide Sicherheit zu schaffen.
6. Die Kenntnisse über variable Tools wie dumpsec und OpenVAS, um das System für eine höhere Sicherheit zu konfigurieren.
7. Die Definition von umfassend gültigen CIS Scoring Tools, um eine System-Grundlage für die gesamte Organisation zu schaffen.

Die Teilnehmer von SEC401:

- Sicherheits-Profis, die Wissenslücken schließen möchten
- Manager, die Informations Sicherheit unter einfachen Terminologien verstehen wollen
- Betriebspersonal, das nicht ständig mit IT-Security-Themen zu tun hat.
- IT-Ingenieure und Supervisoren, die lernen möchten, wie ein
- Verteidigungs-Netzwerk geschaffen wird
- Administratoren, die verantwortlich sind ein Sicherheits-System zu schaffen, welches das Ziel von Angreifern sein kann
- Forensik-Spezialisten, Penetration-Tester, um ein solides SicherheitsFundament zu erhalten, das sie so effzient wie möglich in ihrem Job macht
- Jeder, der fundierte Kenntnisse über eine funktionale Netzwerk- und System-Sicherheit erlernen möchte

WWW.SANS.ORG/SEC401
Dauer: 6 Tage / Laptop benötigt
46 CPE/CMU Credits / GIAC Zertifikat: GSEC

SEC 401

Security Essentials Bootcamp Style-

die Grundlagen zur Abwehr möglicher Angriffe.

SEC401 fokussiert sich darauf, alle nötigen Schritte zu vermitteln, um Attacken vorzubeugen und Gegner zu entdecken. Hier lernen die Teilnehmer das Wissen von Experten aus erster Hand, um für den Kampf gegen die Bedrohungen der Cyber-Welt gerüstet zu sein. Hierbei unterliegt der Kurs der Maxime: „Vorbeugung ist ideal, aber Schutz ist ein unerlässliches Muss."

Die Zielsetzung von SEC401:

Bevor ein Unternehmen in die IT-Sicherheit investiert, müssen drei Fragen beantwortet werden:

1. Was ist das Risiko?
2. Hat das Risiko eine hohe Priorität?
3. Was ist der kosteneffzienteste Weg, um das Risiko zu minimieren?

SEC401 schult die Teilnehmer darin, die Sprache und die zugrundeliegenden Theorien der Computer- und IT-Security zu verstehen. Der Kurs lehrt essentielles und efektives Sicherheits-Know-How. Dazu vermittelt er die notwendigen Skills, um ein System kompetent zu verteidigen und zu wissen, was dazu benötigt wird.

Der Kurs vereint zwei SANS-Kernversprechen:

- Die Vermittlung von Wissen, das bei der Rückkehr ins Unternehmen sofort angewendet werden kann.
- Ein Unterricht von Dozenten, die zu den besten Spezialisten der Industrie zählen.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos auf:
www.sans.org/SEC401

"IT IS MAKING ME QUESTION MY OWN BELIEFS. I WILL BE CHALLENGING COLLEAGUES AND STRATEGIES WHEN I RETURN TO WORK. THE COURSE IS FULL OF LOGICAL, WORKABLE SOLUTIONS."

Anthony Usher
HMRC

WWW.SANS.ORG/SEC503
Praxisorientiert | 6 Tage | Laptop erforderlich
36 CPE/CMU Credits | GIAC-Zertifizierung: GCIA

SEC 503

Intrusion Detection In-Depth

Informationen zum kurs

SEC503: Intrusion Detection In-Depth bietet die technischen Kenntnisse, Informationen und praktischen Übungen, die nötig sind, um Netzwerke zuverlässig verteidigen zu können. Die Teilnehmer werden mit dem theoretischen Fundament von TCP/IP und den gängigsten Anwendungsprotokollen wie HTTP vertraut gemacht. So können sie den Netzwerkverkehr sachgerecht auf Anzeichen eines Einbruchs untersuchen. Sie erlernen den Umgang mit einem breiten Spektrum von Open-Source-Tools wie tcpdump, Wireshark, Snort, Bro und vielen weiteren. Tägliche praktische Übungen für Teilnehmer auf allen Erfahrungsstufen vertiefen den Lehrstoff und geben Gelegenheit, das Gelernte in die Praxis umzusetzen.

Zu den Grundübungen erhalten die Teilnehmer unterstützende Hinweise; die schwierigeren Aufgaben sind auf diejenigen zugeschnitten, die den Stoff bereits kennen oder neuen Stoff schnell erlernt haben. Zudem gibt es zu den meisten Übungen eine „Bonusfrage“, die selbst den fortgeschrittensten Teilnehmer vor Herausforderungen stellen soll.

Der Branchenexperte Mike Poor hat eigens für diesen Kurs eine VMware-Distribution namens Packetrix programmiert. Wie der Name bereits andeutet, zeigt Packetrix zahlreiche Kunstgriffe zur Durchführung von Paket- und Traffic-Analysen auf. Packetrix wird durch Demonstrations-„pcaps“ ergänzt, d.h. Dateien, die Netzwerk-Traffic enthalten.

Die Teilnehmer können den Lehrstoff und die Demonstrationen auf ihren Laptops verfolgen. Mit den pcaps steht ihnen bei der Wiederholung des Lernstoffs und insbesondere bei der Vorbereitung auf die Zertifizierung eine hilfreiche Library des Netzwerkverkehrs zur Verfügung.

SEC503: Intrusion Detection In-Depth soll den Teilnehmern die wichtigsten Kenntnisse, Werkzeuge und Techniken vermitteln, die sie zur Verteidigung von Netzwerken brauchen. Dabei konzentriert sich der Kurs auf neue Fähigkeiten und Kenntnisse, die sofort umgesetzt werden können.

“UM EIN NETZWERK VERTEIDIGEN ZU KÖNNEN, MUSS MAN WISSEN, WIE ES FUNKTIONIERT. DIESER KURS IST EBENSO INTERESSANT WIE ANSPRUCHSVOLL.”
Holly C
MOD UK

NACH DEM KURS KÖNNEN SIE

1. Das Open-Source-Tool Snort konfigurieren und anwenden und Signaturen für Snort schreiben
2. Das Open-Source-Tool Bro konfigurieren und anwenden, um Analysen für hybriden Traffic durchzuführen
3. Die Komponenten der TCP/IP-Schichten verstehen, um normalen und abnormalen Traffic zu identifizieren
4. Open-Source-Tools für Traffic-Analysen anwenden, um Anzeichen für ein Eindringen zu ermitteln
5. Verstehen, warum Netzwerkforensik nötig ist, um Traffic zu überprüfen und einen möglichen Einbruch zu erkennen und zu untersuchen
6. Mit Wireshark verdächtige Dateianhänge analysieren
7. tcpdump-Filter schreiben, um ein bestimmtes Traffic-Merkmal separat zu betrachten
8. Unterschiedliche Logdateien zusammenführen, um Analysen zu erweitern und zu vertiefen
9. Mit dem Open-Source Netzwerkfluss-Tool SiLK Verhaltensanomalien aufdecken
10. Kenntnisse zu Netzwerkarchitekturen und Hardware nutzen, um IDS-Sensoren maßgerecht zu platzieren
11. Netzwerkverkehr mitschneiden

Die Teilnehmer von SEC504:

- Intrusion-Detection-Analytiker
- Netzwerktechniker
- System-, Sicherheits- und Netzwerkadministratoren
- Praktisch tätige Sicherheitsmanager

SECURITY-AWARENESS-TRAINING

Menschliches Verhalten ändern • Risiken beherrschen Compliance wahren • Reputation schützen

SANS Securing The Human ist ein webbasiertes Security-Awareness-Training, das Mitarbeiter zur ersten Verteidigungslinie des Unternehmens macht.

Securing The Human befähigt die Mitarbeiter, die wichtigsten Sicherheitsbedrohungen zu erkennen und richtig auf sie zu reagieren. Die Produktlinie bietet Schulungspakete, die spezifisch auf Endnutzer, Entwickler, ICS-Anwender, Mitarbeiter von Versorgungsbetrieben und Beschäftigte im Gesundheitswesen zugeschnitten sind.

Die Schulungen sind videogestützt und interaktiv. Quizfragen stellen sicher, dass die Mitarbeiter das Gelernte behalten. Securing The Human ist in mehr als 25 verschiedenen Sprachen verfügbar.

Die wichtigsten Vorteile von *Securing The Human:*

- **Rollenbasiertes Training** – Es können Schulungsprogramme mit Inhalten zusammengestellt werden, die genau auf bestimmte Mitarbeitergruppen zugeschnitten sind
- **Zuverlässig und sicher** – Die SANS-Infrastruktur gewährleistet, dass die Schulungen stets verfügbar sind und auf sichere Weise bereitgestellt werden
- **Praktisch** – Die prägnanten, modular aufgebauten Videoschulungen geben den Mitarbeitern die Möglichkeit, das Training in mehreren kurzen Sitzungen zu absolvieren
- **Komplettes Security-Awareness-Training** – Eine sofort einsetzbare, gehostete Lösung für Unternehmen, die ein vordefiniertes Programm suchen
- **Firmenbranding** – Die Trainingsprogramme können personalisiert werden
- **Klares, informatives Backend** – Mittels Dashboards und Berichtssystemen kann der Leiter die Effektivität eines Awareness-Programms überwachen und bewerten
- **Automatisierte Berichte und Erinnerungen** – Die Leiter können dafür sorgen, dass alle Mitarbeiter aufgefordert werden, die erforderlichen Schulungen zu absolvieren

SANS bietet stets den passenden Servicelevel – gleich, ob eine mittelständische Firma Compliance gewährleisten will oder ein Großunternehmen das Sicherheitsbewusstsein erhöhen möchte.

Die SANS Programm-Manager geben gerne Hilfestellung für Unternehmen, die ein Awareness-Programm aufbauen und umsetzen und seine Wirkung messen möchten.

Wie können wir Ihnen helfen?

Um Unternehmen bei der Entwicklung wirkungsvoller Aufklärungsprogramme zu helfen, führt SANS Schulungsveranstaltungen zur Cybersicherheit durch und bietet fachkundig zusammengestellte Ressourcen und Schulungsmaterialien sowie Zugang zu einer globalen Awareness Community. Besuchen Sie bitte www.securingthehuman.org/resources/getting-support

"SANS SECURING THE HUMAN IST EINE UNSCHÄTZBARE HILFE. WIR SIND DANKBAR, DASS DAS SYSTEM SO LEICHT NUTZBAR UND SO GUT ZUGÄNGLICH IST. DASS DIE MITARBEITER DIE SCHULUNGEN 24/7 ABSOLVIEREN KÖNNEN, IST EIN PLUS."

Nic Lee
NORTHROP GRUMMAN IS

Um weitere Informationen zu Securing The Human oder eine Demo anzufordern und professionelle Unterstützung bei der Planung eines Aufklärungsprogramms zu erhalten, wenden Sie sich bitte an unser Expertenteam.
Tel.: +44 203 3384 3470, E-Mail: awarenesstraining@sans.org

www.securingthehuman.org

WWW.SANS.ORG/SEC504
Dauer: 6 Tage / Laptop benötigt
37 CPE/CMU Credits / GIAC Zertifikat: GCIH

SEC 504

Hacker Tools, Techniques, Exploits and Incident Handling-

entdecken Sie die geheimen Tricks der „Gegenseite".

Die Wahrscheinlichkeit, dass ein Unternehmen von Hackern angegriffen wird, ist heute so groß wie nie. Das einzig dafür Nötige ist eine Internet-Verbindung. Von den fünf, zehn oder mehr als hundert täglichen Sondierungen, denen ein System von außen ausgesetzt ist, bis zu wirklich bösartigen Bedrohungen ist die Bandbreite der Risiken immens. Angreifer werden dabei immer unsichtbarer. So schleichen sie sich langsam ein, um größtmöglichen Schaden anzurichten.

Die Zielsetzung von SEC504:

Wer Angreifer entdecken und abwehren will, der muss wissen, wie die andere Seite denkt und handelt. SEC504 schult die Teilnehmer darin, die Taktiken und Strategien der Angreifer zu verstehen. Dazu erhalten die Studenten eine detaillierte Beschreibung, wie Angreifer IT-Systeme unterminieren. Sie lernen die allerneuesten Angriffsvektoren kennen und die „Oldie but Goodie"-Attacken, die immer noch verbreitet sind. Dazu vermittelt SEC504 auch das nötige Wissen, um Fragestellungen zur Legalität zu beantworten, die mit der Abwehr von Angrifen einhergehen.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos finden Sie auf:
www.sans.org/SEC504

"VERY STRUCTURED AND WELL PREPARED COURSE. INTERESTING AND ENGAGING FOR PEOPLE NEW TO THE FIELD AS WELL AS EXPERIENCED PROFESSIONALS"
Ewe Konkolska
PRUDENTIAL

Das bringt Ihnen SEC504:

1. Analyse der Strukturen von Angriffs-Techniken, um die Ausbreitung des Angreifers zu erkennen und zu erwartende Angrife zu durchkreuzen.
2. Nützliche Tools, um anhand bestimmter Anzeichen Schadprogramme zu erkennen. Inklusive „rootkits", „backdoors" und „Trojanischen Pferden". Dazu die wirkungsvollen Taktiken zur Reaktion darauf.
3. Den Gebrauch von „built-in-command-line-tools" wie Windows tasklist, wmic, reg, Linux netstat, ps und lsof, um Angreifer aufzuspüren.
4. Wissen über Analyse Router und System ARP tables die auf CAM tables umgeschaltet werden, um die Aktivität des Angreifers zu verfolgen.
5. Die Anwendung von Memory Dumps und des Volatility Tools, um festzustellen wo sich Angreifer festgesetzt haben und welche Pivot Points im Netzwerk ausgenutzt werden.
6. Den Zugang zu einem Angriffsziel über Metasploit und damit die Entdeckung von Auswirkungen via File-, Log- und Memory-Analysen.
7. Das Wissen, wie der Nmap Port Scanner und Nessus Vulnerability Scanner eingesetzt werden, um offene Löcher im angegriffenen System zu finden.

Die Teilnehmer von SEC504:

- Incident-Handler, Penetration-Tester, Ethical Hacker, Incident-Handling-Teamleiter
- System-Administratoren, die in der ersten Linie der System-Verteidigung stehen
- Weiteres Sicherheits-Personal, das dafür verantwortlich ist, als erstes auf Angriffe zu reagieren

Das bringt Ihnen SEC511:

1. Analyse-Fähigkeiten, um Defizite in der Sicherheits-Architektur zu entdecken.
2. Die sofortige Praxis-Anwendung der erlernten Kurs-Inhalte, um eine verteidigungsbereite Sicherheits-Architektur zu erstellen.
3. Die wichtige Bedeutung einer konsequent aufdeckenden SicherheitsArchitektur und eines Security-Operations-Centers (SOC).
4. Das Wissen zur Identifikation von Schlüssel-Komponenten bei der Netzwerk-Sicherheit und beim Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM).
5. Das Erkennen und Festlegen individueller Anforderungen des Sicherheits-Monitorings für Unternehmen und Organisationen jeglicher Größe.
6. Die Fähigkeit zur Implementierung eines robusten „Network Security Monitorings/Continuous Security Monitorings“ (NSM/CSM).
7. Das Wissen zur Definition notwendiger Monitoring Maßnahmen für die eigene SOC-Umgebung.
8. Die Kenntnis, die erforderlichen Ressourcen zu bestimmen, um ein kontinuierliches Monitoring für Schlüssel-Sicherheits-Kontrollen zu unterstützen.
9. Die Verwendung geeigneter Tools zur Unterstützung der Implementierung des „Continuous Monitoring (CM)“ nach den NIST Guidelines SP 800-137

Die Teilnehmer von SEC511:

- Sicherheits-Architekten
- Senior Sicherheits-Ingenieure
- Technische Sicherheits-Manager
- SOC Analysten
- SOC Ingenieure
- SOC Manager
- CND Analysten
- Weitere Mitarbeiter, die in den Bereichen „Continuous Diagnostics and Mitigation“ (CDM), „Continuous Security Monitoring“ (CSM), oder „Network Security Monitoring“ (NSM) arbeiten

WWW.SANS.ORG/SEC511
Dauer: 6 Tage / Laptop benötigt
36 CPE/CMU Credits / GIAC Zertifikat: GMON

SEC 511

Continuous Monitoring and Security -Operations -

automatisch immer in Alarmbereitschaft.

Unternehmen und Organisationen investieren eine Menge Zeit und Ressourcen bei den Versuchen, die Cyber-Angriffe zu bekämpfen. Ungeachtet dieses immensen Aufwandes sind sie immer noch gefährdet. Denn kein Netzwerk ist wirklich undurchdringlich – eine Tatsache, der sich Führungskräfte und Security-Profis stellen müssen. Deshalb wird die Prävention immer ausschlaggebender.

Die Zielsetzung von SEC511:

Die Herausforderung besteht darin, einen Angriffrechtzeitig zu entdecken. Und dazu gehört die ständige Unterhaltung eines funktionierenden Frühwarnsystems, das keine zeitlichen Lücken aufweist. Deshalb trainiert der Kurs SEC511 die Fähigkeit, eine permanente verteidigungsbereite Sicherheitsarchitektur, das „Network Security Monitoring“ sowie eine kontinuierliche Sicherheitsdiagnose, -vorbeugung und -überwachung zu betreiben. Die Teilnehmer dieses Kurses sind bestens dafür gerüstet, Bedrohungen und Anomalien, die auf CyberKriminalität hinweisen, rechtzeitig zu entdecken.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos auf:
www.sans.org/SEC511

“THE INSTRUCTOR’S EXPERIENCE AND EXPERTISE IN THE SUBJECT DOMAIN ARE ESPECIALLY USEFUL FOR ME, HELPING ME TO UNDERSTAND THE CUSTOMER’S REQUIREMENTS AND, THEREAFTER, DEPLOY AN APPROPRIATE MONITORING ENVIRONMENT TO ADDRESS THE NEEDS OF SECURITY OPERATIONS.”
Ryan Wong
ACCEL

WWW.SANS.ORG/SEC542
Dauer: 6 Tage / Laptop benötigt
36 CPE/CMU Credits / GIAC Zertifikat: GWAPT

SEC 542

Web App, Penetration-Testing and Ethical Hacking -

alle Fehler frühzeitig finden und eliminieren.

Web-Applikationen müssen eine hervorragende Funktionalität und einen reibungslosen Datenzugrif garantieren. Das verlangt jedoch die Entwicklung von Applikationen, die perfekt konzipiert und umgesetzt werden. Sollten sich trotzdem Fehler eingeschlichen haben, müssen diese so schnell wie möglich identifiziert werden. Dabei geht es nicht nur um die Funktionalität, sondern auch um die Sicherheit. So beweisen Studien aus der Großindustrie, dass Design-Fehler in Web-Applikationen zu gefährlichen Sicherheits-Lücken führen können.

Die Zielsetzung von SEC542:

SEC542 bildet die Studenten für ein professionelles und hochklassiges Penetration-Testing von Web-Applikationen aus. Die Studenten erlernen einen Praxis-getesteten und wiederholbaren Prozess, um Design-Fehler zu finden und konsequent aufzuzeigen. Nicht theoretisch, sondern zum sofortigen Einsatz in der Praxis

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos finden Sie auf:
www.sans.org/SEC542

"CTF IS A GREAT WAY TO PRACTICE THE COURSE CONTENT, REALLY ENJOYED IT."
Chris Campbell
RBS

Das bringt Ihnen SEC542:

1. Eine detaillierte vierstufige Methodik, um Penetration-Tests erfolgreich durchzuführen – inklusive Recon, Mapping, Discovery und Exploitation.
2. Die Analyse der Ergebnisse von automatisierten Web-Testing-Tools, um Falschmeldungen zu identifizieren.
3. Den Gebrauch von Python, um Test- und Exploitation-Skripts während eines Penetration-Tests zu entwickeln.
4. Die Entwicklung von Konfigurationen und Test-Payloads mit Burp Intruder, um SQL injection, XSS und andere Test-Angriffe durchzuführen.
5. Den Gebrauch von Use FuzzDB, um Angriffs-Traffic zu generieren, der Design-Fehler wie „Command Injection" und „File Include" abfragt.
6. Die Fähigkeit zur richtigen Beurteilung eines Logik- und TransaktionMangels innerhalb einer Ziel-Applikation, um Logik- und BusinessSchwachstellen zu identifizieren.
7. Anwendung von Durzosploit, um XSS Payloads zu verschleiern, die WAFs und Applikationsfilter umgehen.
8. Die Kenntnis, um den Traffic zwischen dem Client und der ServerApplikation zu analysieren. Dazu werden Tools wie Ratproxy und Zed Attack Proxy genutzt, um offene Punkte bei der Sicherheit des Client-seitigen Applikations-Codes zu finden.
9. Die Durchführung kompletter Web-Penetration-Tests während der „Capture the Flag-exercise", um alle Techniken und Tools ausführlich zu testen

Die Teilnehmer von SEC542:

- Praktiker aus der General-Security
- Penetration-Tester
- Ethical Hacker
- Entwickler von Web-Applikationen
- Designer und Architekten von Webseiten

Das bringt Ihnen SEC560:

1. Die Kenntnis, um Scoping-Studien und Handlungsanweisungen für hochwirksame Penetration-Tests zu entwickeln.
2. Das Durchführen von detaillierten Aufklärungs-Missionen mit der Nutzung von Dokument-Metadaten, Suchmaschinen und anderen öfentlich zugänglichen Informations-Quellen. So wird ein genaues Verständnis der technischen und organisatorischen Voraussetzungen der Ziel Umgebung entwickelt.
3. Die Nutzung des Nmap Scanning Tools, um das Verhalten umfassender Network Sweeps oder „Port Scans“ zu erkennen.
4. Die Fähigkeit, den Nessus Vulnerabilityscanner zu konfigurieren und einzusetzen. Dank dessen werden Verwundbarkeiten des Systems durchgehend dokumentiert und Business-Risiken aufgezeigt.
5. Das Wissen, um den Output der Scanning-Tools manuell auf ihre Exaktheit zu prüfen. Dabei werden vor allem die Netcat und Scapy Paketerstellungstools eingesetzt.
6. Die Anwendung der Windows- und Linux-Command Lines, um umfassende Penetration-Tests zu ermöglichen.

Die Teilnehmer von SEC560:

- Sicherheits-Mitarbeiter, deren Schwerpunkt die Auffndung von
- System-Schwächen ist
- Penetration-Tester
- Ethical Hacker
- Auditoren, die ein tieferes Wissen um technische Voraussetzungen benötigen
- Red Team Members
- Blue Team Members

WWW.SANS.ORG/SEC560
Dauer 6 Tage / Laptop benötigt
37 CPE/CMU Credits / GIAC Zertifikat: GPEN

SEC 560

Network Penetration-Testing and Ethical Hacking -

Schwachstellen schließen und Kriminelle aussperren.

Zu den wichtigsten Aufgaben von Sicherheits-Profis zählt die Entdeckung und das Verstehen von Schwachstellen in den Unternehmens-Netzwerken. Dabei erkannte Risiken müssen sorgfältig und gewissenhaft ausgemerzt werden. Und zwar bevor Cyber-Kriminelle sie ausnutzen können.

Die Zielsetzung von SEC560:

SEC560 trainiert die Studenten darin, zielgerichtete Aufklärungs-Missionen durchzuführen, um mögliche Risiken bereits vorab zu identifizieren. Das betrifft zum einen die Untersuchung eines möglichen Angriffs-Ziels. Zum anderen gehört dazu auch der Blick auf genutzte Mini-Blogs, Suchmaschinen, Social-Networks oder andere Internet-Infrastrukturen. Um hier auf der sicheren Seite zu sein, offeriert der SEC560 eine ganze Bandbreite von Praxis-Maßnahmen aus der „real world“ – fundiert vermittelt durch das erprobte Fachwissen der weltweit führenden Pen-Tester.

Auf diese Weise schult SEC560 die Teilnehmer konsequent darin, ihre Pflichten im Sicherheits-Bereich perfekt zu erfüllen. SEC560 startet mit sorgfältiger Planung, Scoping und Aufklärung. Anschließend beschäftigt er sich intensiv mit Scanning, Target Exploitation und Passwortattacken sowie Wireless- und Web-App-Themen. Insgesamt bietet SEC560 über 30 detaillierte Anwendungen aus der Praxis.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos auf:
www.sans.org/SEC560

“IT INTRODUCES THE WHOLE PROCESS OF PEN TESTING FROM START OF ENGAGEMENT TO END.”
Barry Tsang
DELOITTE

WWW.SANS.ORG/FOR508
Dauer: 6 Tage / Laptop benötigt
36 CPE/CMU Credits / GIAC Zertifikat: GCFA

FOR 508

Advanced Digital Forensics and Incident Response -

verborgene Bedrohungen aufspüren und entfernen.

Über 80% der Unternehmen, die von Cyber-Attacken betroffen sind, konnten von ihren Sicherheits-Teams nicht vor den Gefährdungen gewarnt werden. Teilweise waren Angreifer sogar monate- oder jahrelang in den Unternehmens-Netzwerken aktiv – ohne jemals entdeckt zu werden. Um die damit verbundenen Stör- und Zwischenfälle zu verhindern, benötigen die Sicherheits-Verantwortlichen ein top-aktuelles und übergreifendes Fachwissen. Denn im schlimmsten Fall betreffen Sicherheitsverletzungen nicht nur ein oder zwei Systeme im Unternehmen – sie könnten Hunderte umfassen.

Die Zielsetzung von FOR508:

Dieser tiefgehende und intensive Kurs schult die Sicherheits-Kräfte im Unternehmen mit den aktuellsten Erkenntnissen aus der Praxis. So werden verdeckte Eindringlinge gejagt, enttarnt und nachhaltig entfernt. Das Ergebnis ist die Wiedergewinnung der Sicherheits-Hoheit und der Schutz der Unternehmens-Netzwerke vor aktuellen und kommenden Bedrohungen.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos finden Sie auf:
www.sans.org/FOR508

"COURSE IS VERY UP TO DATE AND CHALLENGES EXISTING IDEAS TO HELP BECOME A BETTER INVESTIGATOR. COURSE IS WELL PREPARED."
Frank Visser
PWL

Das bringt Ihnen FOR508:

1. System-umfassende Tools wie F-Response oder die SIFT Workstation, um Forensik-Analysen durchzuführen und APT Beach Head und Spear Phishing Angriffs-Mechanismen zu entdecken.
2. Ein Volatility-Toolset mit dem Sie aktive Schad-Software im Systemspeicher erkennen und herausfinden auf welche Weise sie platziert wurde. Zudem die Fähigkeit, bei Störungen korrekte Scoping-Maßnahmen anzuwenden.
3. Die Fähigkeit, modernste Angriffs-Formen und Viren wie z. B. Stuxnet, TDSS, oder APT sowie Command and Control-Software umgehend zu identifizieren. Dazu das Wissen, wie Sie mit dem Redline's Malware Rating Index (MRI) schnell feststellen, wie groß eine Datenschutzverletzung ist.
4. Das Können, um den Weg eines Angreifers quer durch die Systeme exakt zu verfolgen und zu sehen, welche Daten das Ziel eines Angrifs waren. Mit einem log2timeline Toolset werden die Bewegungen des Angreifers im Netzwerk exakt offengelegt.
5. Die Kenntnis zur Wiederherstellung und Sanierung geschädigter Systeme mit den Indicators of Compromise (IOC) sowie von IR/ Forensics Key Scanning-Techniken, um aktive Schad-Software und die von der Datenschutzverletzung betroffenen Netzwerk-Systeme zu erkennen.
6. Eingriffe in das Filesystem über das Sleuth Kit Tool, um das Filesystem zu kontrollieren und gleichzeitig forensische Artefakte wie NTFS $I30 Directory Dateiindizes, Journal Parsing oder Master File Tables aufzudecken.

Die Teilnehmer von FOR508:

- Incident Response Team Leader
- Security Operations Center (SOC) Personal und Information Security Fachleute
- Erfahrene Digital-Forensic-Analysten
- System Administratoren

Das bringt Ihnen FOR572:

1. Das Wissen, wie man Dateien aus Netzwerkpaket-Captures und Proxy Cache Dateien extrahiert, um Schad-Software zu analysieren oder den definitiven Datenverlust festzustellen.
2. Den richtigen Gebrauch von gesammelten NetFlow-Daten, um vergangene Netzwerk-Ereignisse zu analysieren und das exakte Problem einer Störung zu bestimmen.
3. Das Zurücksetzen von Netzwerk-Protokollen, um die Command andControl-Fähigkeiten eines Angreifers zu identifizieren.
4. Die Entschlüsselung von entnommenem SSL-Traffic, um die einzelnen Aktionen eines Angreifers zu dokumentieren und somit zu wissen, welche Daten erbeutet wurden.
5. Die Nutzung der Daten üblicher Netzwerk-Protokolle, um die Genauigkeit von Untersuchungs-Ergebnissen zu steigern.
6. Die Prüfung des Traffics anhand der Netzwerk-Protokolle, um die Muster fremder Aktionen zu erkennen und die Basis für weitere Untersuchungen zu legen.
7. Das Erlernen, auf welche Weise Angreifer Man-in-the-Middle-Tools einsetzen, um in eine anscheinend sichere Kommunikations-Struktur einbrechen zu können.
8. Die Prüfung von geschützten Netzwerk-Protokollen, um zu bestimmen welche Probleme tatsächlich bei den Endgeräten entstanden sind.
9. Die Analyse-Fähigkeiten, um auch den WLAN-Traffic auf die Anzeichen böswilliger Aktivitäten zu untersuchen.

Die Teilnehmer von FOR572:

- Incident Response Team-Mitglieder
- Beamte, Vertreter oder Detektive der Strafverfolgung
- IT-Sicherheits-Manager
- Netzwerk-Verteidiger
- IT-Spezialisten
- Netzwerk-Ingenieure
- Auf IT spezialisierte Juristen und Anwaltsgehilfen

WWW.SANS.ORG/FOR572
Dauer 6 Tage / Laptop benötigt
37 CPE/CMU Credits / GIAC Zertifikat: GNFA

FOR 572

Advanced Network Forensics and Analysis -

mit der richtigen Methodik zur klaren Erkenntnis.

Ob bei einem Einbruch in die Systeme, einem Datendiebstahl oder auch bei Fehlverhalten von Mitarbeitern – das Netzwerk ist oftmals eine einzigartige Quelle für einen Überblick auf die Vorfälle. Seine Beweiskraft sorgt für den erforderlichen und definitiven Beleg, welche kriminellen Vorgänge sich tatsächlich ereignet haben.

Die Zielsetzung von FOR572:

Von Grund auf ist der Kurs FOR572 darauf ausgelegt, alle notwendigen Skills zu vermitteln, um nach einem Vorfall hoch effziente Untersuchungen durchzuführen. Das Training ist fokussiert darauf, vorhandenes forensisches Wissen zu steigern, um eindeutige Ergebnisse zu erzielen.

Ob es darum geht, verbliebene Daten bei den Speichermedien zu entdecken, oder vorübergehende Störungen und Eingriffe der Vergangenheit zu entschlüsseln – FOR572 schult die Teilnehmer auf jeden individuellen Fall.

Der Kurs vermittelt dazu die Tools, die Technik und die notwendigen Prozesse, um im Netzwerk alle Quellen und Beweise für CyberKriminalität zu finden und klar zu belegen. Dazu erhalten die Studenten eine top-ausgerüstete Toolbox und ein praktisches Wissen, das sie vom ersten Tag an in ihrem beruflichen Umfeld einsetzen können.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos auf:
www.sans.org/FOR572

"GREAT INFORMATION. I FOUND THE MALWARE IDENTIFICATION INTERESTING AND I THANK THE INSTRUCTOR FOR OFFERING TO GET ME IN TOUCH WITH SOME PEOPLE WORKING IN THE FIELD OF CYBER-SECURITY RESEARCH."

Habib Gorine
SHEFFIELD UNIVERSITY

WWW.SANS.ORG/FOR610
Dauer 6 Tage / Laptop benötigt
36 CPE/CMU Credits / GIAC Zertifikat: GREM

FOR 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques -

Schad-Software verstehen und bekämpfen.

Das grundlegende Verständnis für das Gefährdungs-Potenzial von moderner Schad-Software ist lebenswichtig für Unternehmen und Organisationen. Nur so lässt sich eine wirkungsvolle und schlagkräftige Verteidigung gegen CyberAngriffe organisieren. Und damit die Fähigkeit, bei Zwischenfällen wirksame Gegenmaßnahmen zu ergreifen.

Die Zielsetzung von FOR610:

Dieser Kurs schafft ein starkes und praxis-orientiertes Wissens Fundament, um Schad-Software mit den neuesten Reverse-Engineering Methoden zu bekämpfen. Er präsentiert eine vielseitige Palette von System- und Netzwerk-Monitoring-Utilities, Disassembler, Debuggern und anderen Tools, mit denen die Details von Schad-Software offengelegt werden.

FOR610 startet mit den fundamentalen Aspekten der Schad-Software Analyse. Die Teilnehmer lernen genau, wie man das Innenleben der Schad-Software überprüft. Hierzu wird Schad-Software untersucht, die in der realen Welt tatsächlich eingesetzt wurde und wird. So gewinnen die Studenten die Kenntnis darüber, wie sich Muster und Codes zusammen verhalten und wie das essentielle x86 Assembler Sprachkonzept funktioniert.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos finden Sie auf:
www.sans.org/FOR610

"IT REALLY GIVES A NICE REALISTIC GUIDANCE ON HOW TO APPROACH COMPLEX PROBLEMS IN MALWARE ANALYSIS."
Markus Jeckeln
LUFTHANSA

Das bringt Ihnen FOR610:

1. Das genaue Verständnis zur Analyse des Codes und des Verhaltens von Schad-Software.
2. Die Kenntnis, mit Netzwerk- und System-Monitoring-Tools zu überprüfen, wie Schad-Software mit dem File-System interagiert – speziell im Hinblick auf die Registrierung, das Netzwerk und andere Prozesse bei Microsoft Windows.
3. Die Fähigkeit, schadhafte JavaScript, VB Script und ActionScriptKomponenten von Webseiten aufzudecken und zu analysieren.
4. Die Möglichkeit, das Verhalten von Schad-Software innerhalb des Netzwerk-Traffics zu kontrollieren, zu unterbrechen und ein CodePatching durchzuführen,
5. Den Gebrauch von Disassembler und Debuggern, um das Innenleben von schadhaften Windows-Ausführungen zu untersuchen.
6. Das Wissen, wie man eine Vielzahl von Verteidigungs-Mechanismen umgeht, mit der die Schad-Software ausgestattet ist.
7. Die Erkenntnis und das Verständnis für gemeinsame Ebenen und Muster im Code der Schad-Software – z. B. die DLL Injection.
8. Die Beurteilung von Bedrohungen durch schadhafte Dokumente wie PDFs oder Microsoft Ofce-Files.
9. Den Nutzen von Indicators of Compromise (IOCs), um die Auswirkungen von Schäden einzudämmen.

Die Teilnehmer von FOR610:

- Profis mit Verantwortung in den Bereichen des Incident Handlings, der forensischen Untersuchung, der Windows-Security und der System-Administration
- Profis, die mit Zwischenfällen zu tun haben, die durch Schad-Software verursacht werden und deshalb die Schlüssel-Aspekte dieser Software verstehen wollen
- Personen, die mit den Aspekten der Schad-Software experimentiert haben und ihre forensische Erfahrung dahingehend erweitern möchten

Das bringt Ihnen ICS410:

1. Das Erlernen von Windows Commandlinetools, um das System im Hinblick auf hochriskante Punkte zu prüfen.
2. Das Wissen, wie Run Linux Commandlinetools (ps, ls, netstat, ect) und ein Basic Scripting ausgeführt wird, um den Ablauf von Programmen zu automatisieren. Zielsetzung: Ein kontinuierliches Monitoring von verschiedenen Tools.
3. Die Installation von VMWare und die Entwicklung von virtuellen Maschinen, um eine virtuelle Laborumgebung zu erstellen und dort die Sicherheit der Systeme zu testen.
4. Das bessere Verständnis für die verschiedenen industriellen KontrollSysteme, der Applikationen, Funktionen und ihre Abhängigkeiten von der Netzwerk-IP.
5. Das Arbeiten mit Betriebssystemen (Systemadministrationskonzepte für Unix/Linux und/oder Windows Betriebssysteme).
6. Die Konzipierung der Netzwerk-Infrastruktur-Planung (NetzwerkArchitektur-Konzepte inklusive der Topologie, der Protokolle und Komponenten).
7. Ein umfassendes Verstehen der Prinzipien und Grundsätze der Informations-Sicherheit (Diskretion, Integrität, Verfügbarkeit, Authentifizierung, Nichtabstreitbarkeit).
8. Das praktische Anwenden erlernter Skills bei der Verteidigung des Netzwerkes. Z. B. die Entdeckung von Host- und Netzwerk-basierten Einbrüchen mithilfe spezieller Technologien.

Die Teilnehmer von ICS410:

- IT – inklusive des technischen Supports
- IT-Securitybeschäftigte, die Sicherheitsaspekte der ICS/SCADAKomponenten kennenlernen möchten
- OT-Ingenieure, die die Sicherheit auf der Anlagenbetreiberseite sicherstellen müssen

WWW.SANS.ORG/ICS410
Dauer 5 Tage / Laptop benötigt
30 CPE/CMU Credits / GIAC Zertifikat: GICSP

ICS 410

ICS/Scada Security Essentials -

Grundlagen-Wissen für den Schutz der Industrie.

SANS konzentriert sich gemeinsam mit der Industrie darauf, Sicherheits-Profis und Ingenieuren von Kontroll-Systemen mit den innovativsten Cyber-Security-Skills auszustatten. So werden sie in die Lage versetzt, die wichtigen Infrastrukturen gegen jedweden Angriff zu verteidigen.

Die Zielsetzung von ICS410:

ICS410 wurde entwickelt, um die Cyber-Security-Profis so zu schulen, dass sie die den Kontroll-Systemen zugrunde liegenden Design Prinzipien vollauf verstehen. Durch dieses Wissen werden sie in die Lage versetzt, die Sicherheit der Systeme kompetent zu gewährleisten. Deshalb bietet der Kurs eine grundlegende Zusammenstellung standardisierter Skills und essentiellen Know-hows. Die Teilnehmer werden so trainiert, dass sie die Steuerungs-Systeme im betrieblichen Umfeld jederzeit schützen können – gegen aktuelle und kommende Bedrohungen.

Nach Abschluss des Kurses verfügen die Teilnehmer über einen einheitlichen Kenntnisstand, mit dem sie gemeinsam für die Sicherheit von industriellen Steuerungssystemen sorgen können.

Eine Übersicht aller weiterführenden Kurs-Module finden Sie weiter hinten, auf der Ausklapp-Seite.

Alle Termine und mehr Infos auf:
www.sans.org/ICS410

"GREAT INTRODUCTION INTO ICS LANDSCAPE AND ASSOCIATED SECURITY CONCERNS. THE ICS MATERIAL PRESENTED WILL PROVIDE IMMEDIATE VALUE RELATIVE TO HELPING SECURE MY COMPANY."
Mike Poulos
COCA-COLA ENTERPRISE

Teilnehmer-Stimmen:

"IT IS MAKING ME QUESTION MY OWN BELIEFS. I WILL BE CHALLENGING COLLEAGUES AND STRATEGIES WHEN I RETURN TO WORK. THE COURSE IS FULL OF LOGICAL, WORKABLE SOLUTIONS"

Anthony Usher
HMRC
SEC401

"BY FAR THE BEST COURSE I HAVE EVER ATTENDED. EVERY DAY I HAVE LEARNT THINGS THAT CAN BE APPLIED AT WORK."

Stuart Long
BANK OF ENGLAND
SEC501

"GREAT COURSE CONTENT, VERY INTERESTING AND COMPREHENSIVE."

John O'Brien
AIRBUS DEFENCE & SPACE
SEC501

"THIS COURSE, ON THE FIRST DAY, MADE CLEAR SEVERAL TOPICS THAT I HAD QUESTIONS ON FOR YEARS. THE EXPLANATIONS PROVIDED WERE UNLIKE OTHER INFORMATION CONTAINED ON WEBSITES AND IN BOOKS."

M. Cook
ARROWHEAD INTERNATIONAL
SEC502

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

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.

Profi tieren Sie von:

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

@RISK: The Consensus Security Alert
bietet eine wöchentliche Zusammenfas sung von:
- neu entdeckten Angrif svektoren
- 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 CyberSicherheit immer up to date.

Jetzt kostenlos anmelden auf sans.org

SANS EMEA

SANS IT Security Training und Ihre

Karriere-Road-Map

KERN-KURSE

FUNKTION:

NETWORK OPERATIONS CENTER, SYSTEM ADMIN, SECURITY ARCHITECTURE

In einem Network Operations Center (NOC) werden IT Fachleute eingesetzt, um ein Unternehmens-Netzwerk zu überwachen, zu überprüfen und zu erhalten. Das NOC bildet den Schwerpunkt für Fehlerbehandlungen im Netzwerk, Bereitstellung und Aktualisierung von Software, Router und System Management, Leistungsüberwachung und Koordination mit weiteren Netzwerken. Die NOC Analysten arbeiten Hand in Hand mit dem Security Operations Center, das dafür sorgt, ein Unternehmen abzusichern und konstant auf Bedrohungen zu überprüfen

Berufs-bezeichnungen Z.B.:
Security Analyst / Engineer, SOC Analyst, Cyber Threat Analyst, CERT Member, Malware Analyst

CORE COURSES
SEC301 GISF ▸ SEC401 GSEC ▸ SEC501 GCED

- **SEC505** Securing Windows and PowerShell Automation GCWN
- **SEC506** Securing Linux/Unix GCUX
- **SEC566** Implementing and Auditing the Critical Security Controls - In-depth GCCC
- **SEC579** Virtualisation and Private Cloud Security

FUNKTION:

INFORMATION SECURITY

Fachleute für Informations-Sicherheit sind dafür verantwortlich, Sicherheits-Bedrohungen aufzuspüren, die den Anlagen, Produkten oder technischen Spezifikationen eines Unternehmens gefährlich werden können. Sie beschäftigen sich intensiv mit technischen Protokollen und Spezifikationen, die mit den Bedrohungen der Sicherheit verbunden sind. Sie verfügen über genaueste Kenntnisse möglicher Risiken und Bedrohungen und können so Angrifsstrategien entschlüsseln.

Berufs-bezeichnungen Z.B.:
Cyber Security Analyst , Cyber Security Engineer, Cyber Security Architect

- **SEC301** Intro to Information Security GISF
- **SEC401** Security Essentials Bootcamp Style GSEC
- **SEC501** Advanced Security Essentials Enterprise Defender GCED

FUNKTION:

INCIDENT RESPONSE AND THREAT HUNTING

Sobald die Sicherheit eines Systems oder Netzwerks geschädigt wurde, tritt der Incident Responder als Erste-Hilfe Verteidigung in Aktion. Der Responder muss dabei nicht nur technisch versiert sein, er muss zudem in stressigen „unter Beschuss"-Situationen mit kühlem Kopf Personen, Prozesse und die Technologie steuern, um adäquat auf den Sicherheitsvorfall zu reagieren und ihn abzuschwächen.

Berufs-bezeichnungen Z.B.:
Security analyst/engineer, SOC analyst,Cyber threat analyst, CERT member, Malware analyst

CORE COURSES
SEC301 GISF ▸ SEC401 GSEC

- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling GCIH

Network Analysis	Endpoint Analysis	Malware Analysis
SEC503 Intrusion Detection In-Depth GCIA	**FOR408** Windows Forensic Analysis GCFE	**FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques GREM
FOR572 Advanced Network Forensics and Analysis GNFA	**FOR508** Advanced Digital Forensics and Incident Response GCFA	
FOR578 Cyber Threat Intelligence		

Spezialisierungen

- **FOR526** Windows Memory Forensics In-Depth
- **MGT535** Incident Response Team Management

FUNKTION:

PENETRATION TESTING/ VULNERABILITY ASSESSMENT

Da sich die Verteidigung auf den Angrif ausrichtet, sind diese Experten für ein Unternehmen sehr wertvoll. Sie wenden Angrifstechniken an, um Sicherheitslücken aufzuspüren, analysieren die Risiko-Potentiale und empfehlen abwehrende Maßnahmen, bevor die Unternehmen von tatsächlichen Angreifern geschädigt werden.

Berufs-bezeichnungen Z.B.:
Penetration tester, Vulnerability assessor, Ethical hacker, Red/Blue team member, Cyberspace engineer

CORE COURSES
SEC301 GISF ▸ SEC401 GSEC

- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling GCIH
- **SEC550** Active Defense, Offensive Countermeas-ures & Cyber Deception

Network & Exploits	Web	Mobile / Wireless	Lab Centerd
SEC560 Network Penetration Testing and Ethical Hacking GPEN	**SEC542** Web App Penetration Testing and Ethical Hacking GWAPT	**SEC575** Mobile Device Security and Ethical Hacking GMOB	**SEC561** Immersive Hands-on Hacking Techniques
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking GXPN	**SEC642** Advanced Web App Penetration Testing and Ethical Hacking	**SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses GAWN	**SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise
SEC760 Advanced Exploit Development for Penetration Testers			

Spezialisierungen

- **SEC567** Social Engineering for Penetration Testers
- **SEC580** Metasploit Kung Fu for Enterprise Pen Testing
- **SEC573** Python for Penetration Testers GPYC

FUNKTION:

SECURITY OPERATIONS CENTER/ INTRUSION DETECTION

Das Security Operations Center (SOC) bildet den Schwerpunkt für Absicherung gegen Cyber-bezogene Störfälle, Sicherheits-Überwachung und den Schutz von Anlagen des Unternehmensnetzwerks sowie -Endpunkte. SOC Analysten tragen die Verantwortung für das Sicherheitsbewusstsein eines Unternehmens sowie seine konstante Überwachung inklusive Überprüfung Traffic, Blockieren von unerwünschtem Trafc in das und aus dem Internet sowie das Aufspüren jeglicher Angrifsformen. Somit bilden Sie die Basis, um das Netzwerk gegen mögliche Eindringliche zu stärken.

CORE COURSES
SEC301 ▸ SEC401

SEC504
Hacker Tools, Techniques, Exploits, & Incident Handling
GCIH

Berufs-bezeichnungen Z.B.:
Intrusion Detection Analyst, Security Operations Center Analyst / Engineer, CERT Member, Cyber Threat Analyst

Endpoint Monitoring

SEC501
Advanced Security Essentials - Enterprise Defender
GCED

FOR508
Advanced Digital Forensics and Incident Response
GCFA

Network Monitoring

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

SEC511
Continuous Monitoring and Security Operations
GMON

SEC550
Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence

FOR578
Cyber Threat Intelligence

FUNKTION:

RISK & COMPLIANCE/AUDITING/ GOVERNANCE

Diese Experten bewerten und berichten den Organisationen über Risiken. Sie messen die Einhaltung von Richtlinien, Prozessen und Standards. Sie empfehlen Optimierungen hinsichtlich Efzienz und Profitabilität, abgeleitet aus Erkenntnissen ihrer konstanten Überprüfung des Risiko Managements.

Berufs-bezeichnungen Z.B.:
Auditor, Compliance Officer

MGT433
Securing The Human: Building and Deploying an Effective Security Awareness Programme

SEC566
Implementing & Auditing the Critical Security Controls - In-Depth
GCCC

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

LEG523
Law of Data Security and Investigations
GLEG

FUNKTION:

SECURE DEVELOPMENT

Der Sicherheits-versierte Software Entwickler leitet alle Entwickler in der Erstellung von sicherer Software durch den Einsatz sicherer Programmier-Techniken frei von logischem Design und technischen Anwendungsfehlern. Dieser Experte ist letztendlich dafür verantwortlich, dass die Kunden-Software keine Sicherheitslücken aufweist, die voneinem Angreifer ausgenutzt werden könnten.

Berufs-bezeichnungen Z.B.:
Developer, Software Architect, QA Tester, Development Manager

Core

Securing the Human for Developers STH. Developer
Application Security Awareness Modules

DEV522
Defending Web Applications Security Essentials
GWEB

DEV531
Defending Mobile Applications Security Essentials

DEV534
Secure DevOps: A Practical Introduction

Secure Coding

DEV541
Secure Coding in Java/JEE
GSSP-JAVA

DEV544
Secure Coding in .NET
GSSP-.NET

DEV543
Secure Coding in C/C++

Spezialisierungen

SEC542
Web App Penetration Testing & Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing & Ethical Hacking

FUNKTION:

CYBER OR IT SECURITY MANAGEMENT

Das Management von Personen, Prozessen und Technologien ist schwierig vereinbar mit einer pro-aktiven Situationsbewusstheit eines Unternehmens und einem stetigen Erfolg einer konstanten Überwachung. Diese Manager müssen Führungsqualitäten, aktuellstes Wissen und Best Practice Beispiele parat haben, um rechtzeitig efektive Entscheidungen zu trefen, die der gesamten Unternehmens Informations-Infrastruktur zugute kommen.

Berufs-bezeichnungen Z.B.:
CISO, Cyber Security Manager / Officer, Security Director

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™
GSLC

MGT514
IT Security Strategic Planning, Policy & Leadership

MGT433
Securing The Human: Building and Deploying an Effective Security Awareness Programme

MGT525
IT Project Management, Effective Communica-tion, and PMP® Exam Prep
GCPM

MGT535
Incident Response Team Management

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

MGT414
SANS Training Programme for CISSP® Certification
GISP

LEG523
Law of Data Security and Investigations
GLEG

SEC566
Implementing and Auditing the Critical Security Controls - In-depth
GCCC

MGT415
A practical Introduction to Cybersecurity Risk Management

FUNKTION:

DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

Angesichts heutiger sich ständig ändernder Technologien und Umgebungen, ist es unvermeidlich, dass jede Organisation mit Cyber-Kriminalität konfrontiert wird – einschliesslich Betrug, Bedrohungen von Innen, Industrie-Spionage und Phishing. Zur Lösung dieser Herausforderungen holen sich Organisationen Hilfe von Digital Forensic Experten und verlassen sich auf Cyber-Kriminalitäts Strafverfolgungs-Agenten, um einen umfassenden Bericht über das aktuelle Geschehen zusammen zu stellen.

Berufs-bezeichnungen Z.B.:
Computer Crime Investigator, Law Enforcement, Digital Investigations Analyst, Media Exploitation Analyst, Information Technology Litigation Support & Consultant, Insider Threat Analyst

FOR408
Windows Forensic Analysis
GCFE

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
GCIH

FOR508
Advanced Digital Forensics and Incident Response
GCFA

FOR585
Advanced Smartphone Forensics
GASF

FOR518
MAC Forensic Analysis

FOR526
Memory Forensics In-Depth

FUNKTION:

INDUSTRIAL CONTROL SYSTEMS

ICS-fokussierte Kurse sind darauf ausgelegt, sowohl Sicherheits-Fachkräfte als auch Control System Ingenieure mit dem Wissen und den Fähigkeiten auszustatten, um kritische Infrastruktur abzusichern.

ICS410
ICS/SCADA Security Essentials
GICSP

ICS515
ICS Active Response and Defense & Response

Berufs-bezeich-nungen Z.B.:
IT & OT Support, IT & OT Cyber Security, ICS Engineer

Auf einen Blick -
unsere wichtigsten Kurse für Sie:

CYBER DEFENCE

SEC301	Intro to Information Security
SEC401	Security Essentials: Bootcamp Style
SEC501	Advanced Security Essentials Enterprise Defender
SEC503	Intrusion Detection In-Depth
SEC505	Securing Windows with PowerShell and the Critical Security Controls
SEC506	Securing Linux/Unix
SEC511	Continuous Monitoring and Security Operations
SEC550	Active Defence, Offensive Countermeasures, and Cyber Deception
SEC579	Virtualisation and Private Cloud Security

PEN TEST COURSES

SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling
SEC542	Web App Penetration Testing and Ethical Hacking
SEC560	Network Penetration Testing and Ethical Hacking
SEC561	Immersive Hands-On Hacking Techniques
SEC562	CyberCity Hands-On Kinetic Cyber Range Exercise
SEC573	Python for Penetration Testers
SEC575	Mobile Device Security and Ethical Hacking
SEC580	Metasploit Kung Fu for Enterprise Pen Testing
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defences
SEC642	Advanced Web App Penetration Testing and Ethical Hacking
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
SEC760	Advanced Exploit Development for Penetration Testers

DIGITAL FORENSICS & INCIDENT RESPONSE COURSES

FOR408	Windows Forensic Analysis
FOR508	Advanced Digital Forensics and Incident Response
FOR518	Mac Forensic Analysis
FOR526	Memory Forensics In-Depth
FOR572	Advanced Network Forensics and Analysis
FOR578	Cyber Threat Intelligence
FOR585	Advanced Smartphone Forensics
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques

MANAGEMENT COURSES

MGT414	SANS Training Program for CISSP® Certification
MGT433	Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Programme
MGT512	SANS Security Leadership Essentials For Managers (with Knowledge Compression ™)
MGT514	IT Security Strategic Planning, Policy and Leadership

AUDITING COURSES

SEC440	Critical Security Controls: Planning Implementing and Auditing
AUD507	Auditing & Monitoring Networks, Perimeters and Systems
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth

INDUSTRIAL CONTROL SYSTEMS COURSES

ICS410	ICS/SCADA Security Essentials
ICS515	ICS Active Defence and Incident Response

DEVELOPER COURSES

DEV522	Defending Web Applications Security Essentials
DEV544	Secure Coding in .NET: Developing Defensible Applications

Kontakt:
germany@sans.org
@SANSEMEA
www.sans.org/de

Alle Angaben ohne Gewähr

SANS EMEA