The Most Trusted Source of Cyber Security Training, Certification and Research in the World

SANS EMEA

TRAINING CATALOGUE 2016

www.sans.org
@SANSEMEA

See Inside for:

- SANS Training Events Across Europe and Middle East
- SANS Training Curriculum

Security, Digital Forensics & Incident Response, Pen Testing, IT Audit, Secure Software Development, Management, ICS, Defence

Q2 Edition

ABOUT SANS

WWW.SANS.ORG

Contact SANS
Email: emea@sans.org
Tel: +44 20 3384 3470
Address: SANS EMEA,
PO Box 124, Swansea,
SA3 9BB, UK

Allianz für Cyber-Sicherheit Partner

HM Government

SANS is a Cyber Security Supplier to HM Government

HSD The Hague Security Delta

SANS IS THE WORLD'S LARGEST AND MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING. FOUNDED IN 1989, SANS NOW OPERATES ACROSS 30 COUNTRIES AND HAS OVER 125,000 ALUMNI.

For over twenty-five years, we have worked with many of the world's more prominent companies, military organisations, and governments.

Technology may have changed in that time, but our core mission has remained constant: to protect people and assets through sharing cutting-edge cyber security knowledge and skills.

STRENGTH FROM PEOPLE

SANS Instructors are, first and foremost, industry professionals with a wealth of real-world experience – experience that they bring into the classroom.

Across our roster of Instructors are many active security practitioners who work for high profile organisations. The list includes red team leaders, information warfare officers, technical directors, CISOs, and research fellows.

Along with respected technical credentials, SANS Instructors are also expert teachers. Their passion for their subject shines through, making the SANS classroom efficient and effective.

CUTTING EDGE TRAINING

Cybercrime evolves constantly. SANS prepares students to meet today's dominant threats and tomorrow's challenges.

We do this through constantly updating and rewriting our courses and support material. This process is steered by an expert panel that draws on the global community's consensus regarding best practice.

FOCUSSED TRAINING

SANS training is job and skill-specific. We offer more than 60 courses, designed to align with dominant security team roles, duties and disciplines.

The SANS Curriculum spans Digital Forensics, Audit, Management, Pen Testing, ICS, Secure Software Development and more (see pages 16-21). Each curriculum offers a progression of courses that can take practitioners from a subject's foundations right up to top-flight specialisms.

Our training is designed to be practical. Students are immersed in hands-on lab exercises built to let them rehearse, hone and perfect what they've learned.

THE SANS PROMISE

At the heart of everything we do is the SANS Promise: Students will be able to deploy the new skills they've learned immediately.

THE GLOBAL COMMUNITY

SANS Institute is a prominent member of the global cyber security community. We operate the Internet Storm Centre – the internet's early warning system.

SANS also develops, maintains and publishes a large collection of research papers about many aspects of information security. These papers are made available for free.

THE GIAC ADVANTAGE

GIAC validates the skills of information security professionals, proving that those certified have the skills and technical knowledge necessary to work in key areas of cyber security.

GIAC Certifications are respected globally because they measure specific skill and knowledge areas. GIAC offers the only cyber security certifications that cover advanced technical subject areas.

There are over 20 specialised GIAC certifications. Several GIAC certifications are accepted under the ANSI/ISO/IEC 17024 Personnel Certification programme.

Many SANS Training Courses align with GIAC Certifications. As such, SANS Training is an ideal preparation for a GIAC Certification attempt.

WHY SANS IS THE BEST TRAINING AND EDUCATIONAL INVESTMENT

SANS' immersion training is intensive and hands-on and our courseware is unrivalled in the industry.

SANS Instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and SANS' training content.

SANS training strengthens a student's ability to achieve a GIAC Certification. Both SANS and GIAC place an emphasis on learning practical skills.

HOW TO REGISTER FOR SANS TRAINING

A popular option for taking SANS training is to attend a training event. SANS runs public training events in Europe and the Middle East (and globally), offering students the opportunity to take a SANS course across an intensive 5 or 6 days. SANS training events provide the perfect learning environment and offer the chance to network with other security professionals as well as SANS Instructors and staff.

Students should register online by visiting www.sans.org/emea

SANS training can also be delivered online through our OnDemand product, as a private class within an organisation and through other mediums including classroom training in French and Spanish. See page 6 for details of all our training delivery options or visit www.sans.org/emea.

A NOTE FROM SANS

Since joining SANS last year I have been fortunate to have had many fascinating discussions with cyber security leaders and practitioners from various European nations. A commitment to keeping our organisations and national infrastructure secure has been a constant, as has a belief that we need to continue to work diligently and share knowledge in order to keep up with the ever-changing threat landscape.

SANS understands this - security is a journey and not a destination. That's why we are committed to teaching the skills and techniques that can scale today and into the future.

Having worked in other industry sectors previously, the sense of community in the security sector really stands out. This feeling of a common goal is equally apparent within SANS itself. Our courses, for example, are developed through a consensus process that involves hundreds of administrators, security managers, and information security professionals. At the heart of SANS are the many security practitioners in various organisations, from corporations to universities, all working together to help the community.

I've also been impressed by the vast amount of free resources that SANS provides. These include the Internet Storm Center (the Internet's early warning system), the weekly news digest, NewsBites, the weekly vulnerability digest, @RISK, and more than 1,200 award-winning, original information security research papers contained within the always-growing, SANS Reading Room.

Returning to my discussions with industry leaders, the concern most frequently raised is around 'the skills gap'. Clearly we, as an industry, need to encourage more people to pursue cybersecurity as a career. SANS is working with governments around the world to assist in this area, partnering with Germany's BSI, The Hague Security Delta, and HM Government in the UK. SANS also supports local initiatives like the Belgian and UK Cyber Security Challenge and our Cyber Academy Programmes help identify, train and deploy multiple-GIAC certified professionals in 6-8 weeks.

SANS is also increasing the number of Cyber Security Training Events and Training Courses we hold across the EMEA region. Within this brochure you'll find courses that support beginners or develop advanced and specialist skillsets, all available in a training format that best suits your needs.

If you would like to talk about how SANS can help your organisation, please contact me directly.

Jan Pieter Spaans
MANAGING DIRECTOR, MAINLAND EUROPE
SANS INSTITUTE

SANS EMEA CONTACTS

MIDDLE EAST

NED BALTAGI
Managing Director,
ME & GCC Regions
nbaltagi@sans.org

UK & SCANDINAVIA

STEPHEN M JONES
Managing Director,
UK & Scandinavia
sjones@sans.org

MAINLAND EUROPE

JAN-PIETER SPAANS
Managing Director,
Mainland Europe
jspaans@sans.org

Or contact the EMEA team at emea@sans.org or tel +44 (0) 20 3384 3470

"GIAC is the only certification that proves you have hands-on technical skills."
CHRISTINA FORD, DEPARTMENT OF COMMERCE

How Are You Protecting Your...

- DATA?
- NETWORK?
- SYSTEMS?
- CRITICAL INFRASTRUCTURE?

Risk management is a top priority. The security of assets depends on the skills and knowledge of your security team. Don't take chances with a one-size-fits-all security certification.

GIAC tests and validates the ability of practitioners in information security, forensics, and software security.

GIAC Certification proves that holders possess the cyber security skills necessary to protect critical IT infrastructure. Holders are sought globally by government, military and industry.

GIAC offers over 27 specialised certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

LEARN MORE ABOUT GIAC AND HOW TO GET CERTIFIED AT
WWW.GIAC.ORG

CONTENTS

COURSE DESCRIPTIONS

CYBER DEFENCE COURSES - CORE SECURITY / NETWORK & SECURITY OPERATIONS

PEN TEST COURSES

DIGITAL FORENSICS & INCIDENT RESPONSE COURSES

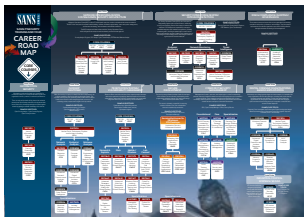
AUDITING COURSES

INDUSTRIAL CONTROL SYSTEMS COURSES

MANAGEMENT COURSES

DEVELOPER COURSES

p14



SANS CAREER ROADMAP

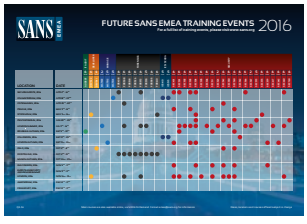
ARE YOU PLANNING YOUR NEXT COURSE OR CAREER MOVE? TURN TO PAGE 14 FOR OUR CAREER ROADMAP AND SEE WHERE SANS TRAINING COULD TAKE YOU.

p16

SANS COURSES

ARE YOU TAKING YOUR FIRST SANS TRAINING COURSE? TURN TO PAGE 16 FOR OUR CURRICULUM GUIDES AND PAGE 22 ONWARDS FOR COURSE DESCRIPTIONS

p60



TRAINING EVENT SCHEDULE AT A GLANCE

SANS PRIVATE TRAINING

Training delivered directly to an organisation's security team in a classroom setting at the employer's premises or training facility. Private training is suitable for organisations that need to train 25 or more staff and/or require an entirely confidential training experience.
Private training allows a SANS Instructor to concentrate on areas directly relevant to that organisation and provides financial advantages across staff travel, subsistence and accommodation.

- **Contact SANS for further information: emea@sans.org**

SECURITY AWARENESS TRAINING

SANS' Securing The Human provides computer-based security awareness training for end users, ICS engineers, developers and the utilities and healthcare industries. Modular videos deliver expert and impactful training to large numbers of employees with measurable results. STH goes beyond compliance and focuses on changing behaviour.

- **www.securingthehuman.org**

SANS MENTOR

Training provided by a top-scoring GIAC student in multi-week classroom settings.

Study at your own pace using SANS courseware and meet weekly in a mentor-led classroom setting.

- **www.sans.org/mentor**

SANS COMMUNITY

1. SANS classroom training in France and Spain. Individual SANS courses taught in French and Spanish by local SANS instructors. SANS course books and materials are in English. 2. Training provided in English by up-and-coming SANS Instructors within their local area. Usually small class sizes and often organised directly by the instructor.

- **See www.sans.org/emea for upcoming Community training opportunities**

SANS SUMMITS

Summits are one or two-day events that take the form of keynote speeches and panel sessions, led by respected thought-leaders and industry practitioners.

A SANS Summit is an invaluable source of targeted learning and typically takes place before or after a SANS Training Event with attendance available at a discounted rate for those attending training.

ESTABLISHED IN 1989, SANS IS THE WORLD'S LARGEST AND MOST TRUSTED SOURCE OF CYBER SECURITY TRAINING

SANS high-standards remain constant across all training delivery options, and all our classes adhere to The SANS Promise - You will learn skills and techniques that can be put to work immediately upon returning to the workplace.

SANS TRAINING FORMATS

SANS TRAINING EVENTS

Instruction in a classroom setting from a qualified SANS Instructor. These are multi-course events located centrally in major cities and hosted at quality hotels or event centres with excellent facilities.

Training Events are a popular method for taking SANS training as they provide an opportunity to learn, network and socialise with peers, colleagues and SANS staff.

Training fees also include break refreshments, lunch and evening functions (where advertised), but not accommodation.

2016 EMEA region Training Events take place across Europe and the Gulf Region.

See the back cover of this brochure or www.sans.org/emea for the latest schedule

BESPOKE TRAINING SOLUTIONS AND CYBER ACADEMY

SANS creates bespoke training programmes that answer specific operational and organisational needs. Training content is drawn from across SANS' Curriculum, and programmes often include assessment phases using SANS CyberTalent.

SANS Cyber Academy identifies candidates with the potential to succeed, then provides intensive training before deploying them as GIAC Certified professionals.

To find out more about SANS partnerships and solutions, turn to page 6 or email emea@sans.org

SANS RESIDENCY

A tailored programme of training for organisations that may require several courses to be run in succession in order to quickly train large existing teams and/or new recruits.

Contact SANS for further information: emea@sans.org

SANS OnDemand

SANS courses available anytime via E-learning. Includes course books, CD/DVDs / Toolkits as applicable and four months of online access to SANS' OnDemand e-learning platform. For students who wish to study on their own at their own pace.

www.sans.org/ondemand

PARTNERSHIPS AND SOLUTIONS

SANS WORKS WITH BUSINESSES AND GOVERNMENTS, CREATING BESPOKE TRAINING AND DEVELOPMENT SOLUTIONS THAT DIRECTLY SUPPORT SPECIFIC OPERATIONAL REQUIREMENTS.

SANS frequently works with organisations to create bespoke, skills development solutions. We consult, advise and then build tailored packages for corporate and government partners looking to enhance their cyber security capability. We also provide tools and solutions that allow organisations to measure and model the effectiveness of these unique solutions.

SANS has the experience and knowledge to deliver solutions across employee assessment, recruitment selection, team development and intense technical training.

"We work with governments and enterprises across different countries, cultures and continents," explains Jan Pieter Spaans, Managing Director Mainland Europe. "Our services include direct solutions, like providing SANS training courses privately."

All of SANS' cyber security training courses can be delivered privately, in an organisation's training facility or HQ. SANS Private Training is delivered by a qualified SANS Instructor with the utmost of discretion. SANS can of course provide security cleared Instructors as required.

"Our services go beyond training though. We also assist security managers in ensuring their team's skills are kept up to date," says Jan Pieter Spaans. "We can build and deploy programmes that increase staff retention through skills development or assess an organisation's needs and then deliver bespoke solutions that deliver across recruitment, on boarding and training."

For an initial discussion with a SANS Institute Director, contact SANS via emea@sans.org or +44 203 384 3470

BESPOKE TRAINING SOLUTIONS

Private training is ideal for organisations that need an entire team to take a particular SANS course. However, often an organisation needs to implement a bespoke training programme that incorporates several SANS training courses.

SANS works closely with organisations, taking time to understand their specific training needs. After a consultation process, a unique training and development solution is created that meets these needs – based on courses from across the SANS Cyber Security Training Curriculum (see pages 16 - 21) and additional SANS products.

Uniquely we are able to provide training recommendations and then deliver that programme ourselves.

BEGIN A DISCUSSION WITH SANS

FOR AN INITIAL DISCUSSION WITH A SANS INSTITUTE DIRECTOR, CONTACT SANS VIA EMEA@SANS.ORG OR +44 203 384 3470. ALTERNATIVELY CONTACT:

STEPHEN M JONES
Managing Director
UK And Scandinavia
sjones@sans.org

NED BALTAGI
Managing Director
ME & GCC Regions
nbaltagi@sans.org

"UNIQUELY WE ARE ABLE TO PROVIDE TRAINING RECOMMENDATIONS AND THEN DELIVER THAT PROGRAMME OURSELVES."

ASSESSMENT AND CANDIDATE SELECTION

SANS works regularly with organisations, helping them to streamline their recruitment processes and procedures.

"The traditional mode of candidate selection generally relies on sifting CVs," explains Ned Baltagi, Director, SANS ME & GCC Regions. "Organisations tell us regularly that this is time consuming and doesn't provide the reliable - and predictable - results they need when selecting front line cyber security staff."

SANS CyberTalent is one such selection product. It is a suite of assessment tools that improve the effectiveness of a cyber security recruitment and selection process.

SANS CyberTalent products use psychometric and skills testing to assess candidates' aptitude and suitability for particular roles. The online assessments leverage SANS' experience in the field of cyber security training and GIAC certification to gauge technical skills and knowledge.

CyberTalent provides managers and HR teams with a deeper understanding of candidates' technical and conceptual makeup.

JAN-PIETER SPAANS
Managing Director, Mainland Europe
jspaans@sans.org

ASSESSING TEAM STRENGTHS AND WEAKNESSES

SANS CyberTalent and other bespoke solutions extend beyond candidate selection. SANS works closely with many organisations, helping them to ensure their security team keeps developing and evolving.

"Security teams must change and adapt – new attack vectors emerge, technologies evolve and businesses themselves change," states Jan Pieter Spaans. "Training is an integral part of this development process... but training needs vary across a team. Training just isn't a one size-fits-all business."

To support managers in developing and improving their team, SANS provides assessment products such as SANS NetWars, SANS CyberCity and SANS CyberTalent. These allow Security and HR managers to achieve a clear understanding of their team's strengths, weaknesses and training needs.

SANS then builds a unique training programme that focusses on addressing a team or individual's specific requirements.

Career development also aids staff retention and ensures a security team remains effective. SANS helps employers create bespoke training programmes using the extensive SANS training curriculum.

Following a consultation process, SANS delivers programmes that meet business needs and also offer security professionals a career roadmap.

www.sans.org/emea

RESIDENTIAL PROGRAMMES

SANS is experienced in building residential training programmes for many different types of organisation – governments, enterprises and military bodies, spanning different geographic regions and business cultures.

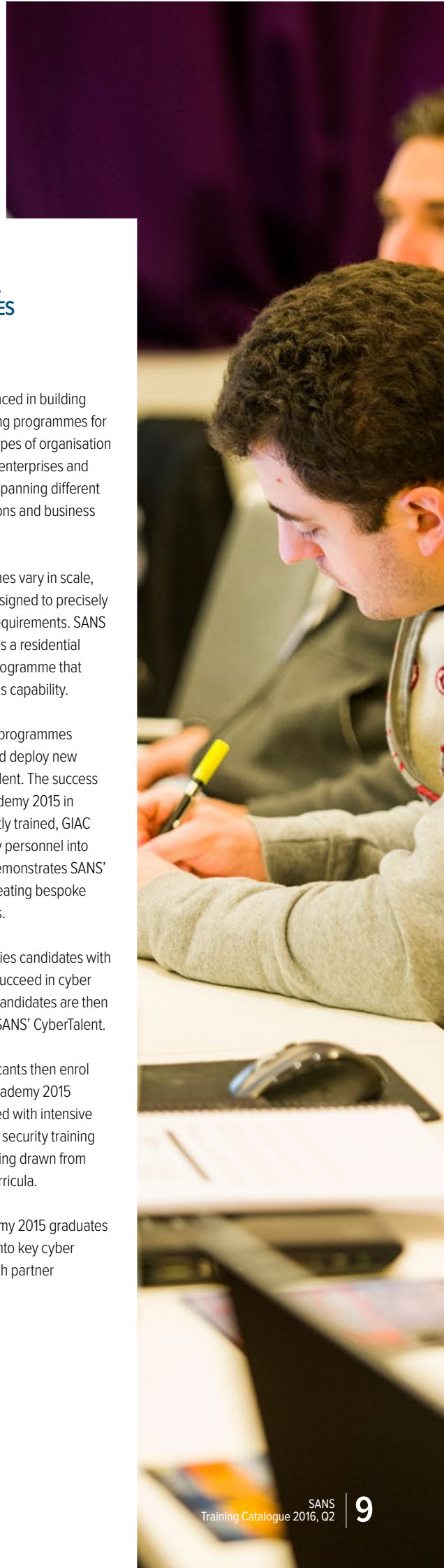
These programmes vary in scale, focus and are designed to precisely meet a client's requirements. SANS Cyber Academy is a residential cyber security programme that demonstrates this capability.

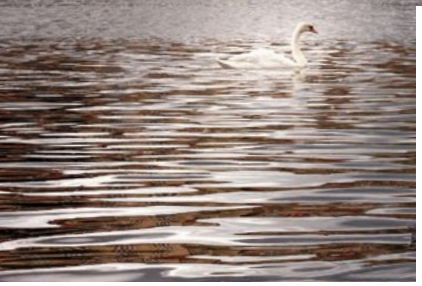
Cyber Academy programmes identify, train, and deploy new cyber security talent. The success of UK Cyber Academy 2015 in delivering expertly trained, GIAC qualified security personnel into the workforce demonstrates SANS' capabilities in creating bespoke training solutions.

SANS first identifies candidates with the potential to succeed in cyber security. Those candidates are then assessed using SANS' CyberTalent.

Successful applicants then enrol into UK Cyber Academy 2015 and were invested with intensive residential cyber security training – the content being drawn from across SANS' Curricula.

UK Cyber Academy 2015 graduates were deployed into key cyber security roles with partner organisations. ●





DFIR PRAGUE 2016

3–15 OCTOBER 2016

#DFIRPRAGUE

DFIR PRAGUE IS AN ANNUAL FIXTURE ON THE SANS EMEA TRAINING CALENDAR. THE UPCOMING TRAINING EVENT HOSTS EIGHT HANDS-ON COURSES FROM SANS' DIGITAL FORENSICS AND INCIDENT RESPONSE CURRICULUM.

DFIR Prague 2016 takes place on 3-15 October, 2016. The training event is focussed on digital forensics and incident response, with SANS hosting all of the DFIR courses available in the EMEA region.

The event also features a dedicated DFIR Summit and a DFIR NetWars Tournament. During Prague 2016 we host SANS@Night evening presentations too.

SANS DFIR Prague happens annually. Classes are led by SANS Instructors and the Prague events themselves are a focal point for the global DFIR community. Students travel from around the world to learn, network and share skills. DFIR Prague 2016 runs for 13 full days. This means students can, schedule allowing, take two SANS DFIR training courses back-to-back. Four courses align with GIAC Certification, meaning the event is ideal for professionals looking to achieve GCFE, GCFA, GNFA or GREM Certification.

The following courses take place:

FOR578: CYBER THREAT INTELLIGENCE

Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defence mechanisms. FOR578 (page 49) teaches defenders to detect, scope, and select resilient courses of action in response to intrusions and data breaches.

FOR408: WINDOWS FORENSIC ANALYSIS

FOR408 focusses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. During FOR408 (page 44) students learn to recover, analyse, and authenticate forensic data on Windows systems. Units focus on understanding how to track detailed user activity on a network, and how to organise findings for use in incident response, internal investigations, and civil/criminal litigation.

FOR508: ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

Incident response tactics and procedures have evolved rapidly over the past few years. This in-depth incident response course provides responders with the advanced skills needed to hunt down, counter, and recover from a wide range of threats within enterprise networks. FOR508 (page 45) is hands on and presents students with practical lab exercises.

FOR518: MAC FORENSIC ANALYSIS

FOR518 (page 46) provides the tools and techniques necessary to take on any Mac case. The intense hands-on forensic analysis skills taught in the course enable investigators to broaden their analytical capabilities. Students gain the confidence and knowledge to comfortably analyse any Mac or iOS system.

FOR526: MEMORY FORENSICS IN-DEPTH

FOR526: Memory Forensics In-Depth (page 47) provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and to analyse captured memory images. The course uses today's most effective freeware and open-source tools and provides an in-depth understanding of how these tools work.

FOR572: ADVANCED NETWORK FORENSICS AND ANALYSIS

FOR572 (page 48) is built, from the ground up, to cover the most critical skills needed to mount efficient and effective post-incident response investigations. Classes focus on the knowledge necessary to expand the forensic skill-set. Students move from exploring residual data on the storage media (system or device), to transient communications that occurred in the past, or that continue to occur.

FOR585: ADVANCED SMARTPHONE FORENSICS

FOR585 concentrates on smartphones as sources of evidence, providing students with the skills needed to handle mobile devices in a forensically sound manner. Students learn how to: manipulate locked devices, understand different technologies, and to discover malware. By diving deeper into the file systems of each smartphone, FOR585 (page 50) also explores how to analyse the results for use in digital investigations.

FOR610: REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

During FOR610, students learn how to set up an inexpensive and flexible malware laboratory. FOR610 (page 51) then teaches how to examine malicious software's inner workings, and how to use the lab to dissect real-world malware samples. Students examine malicious code, its key components and its execution flow.

NETWARS: DFIR TOURNAMENT

During DFIR Prague, SANS is hosting two DFIR NetWars Tournaments. A DFIR NetWars Tournament enables players to learn and sharpen new skills prior to being involved in a real incident. DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges. It is developed by incident responders and forensic analysts who use these skills daily to stop data breaches and to solve complex crimes.

DIGITAL FORENSICS INCIDENT RESPONSE SUMMIT

The DFIR Summit features talks from leading speakers and presentations from an expert panel. The summit is a forum to learn new skills and to hear advice from practitioners on DFIR's front line. The event is chaired by Jess Garcia, a SANS Instructor.

For more information about DFIR Prague 2016 and to register, please visit: www.sans.org/prague-2016

SANS SUMMIT SERIES 2016

LEARN, GAIN TECHNICAL INSIGHT, SHARE OPINIONS AND NETWORK WITH FELLOW PROFESSIONALS AT A SANS SUMMIT

A SANS Summit is a one day event that offers presentations, panel sessions, demonstrations and discussions – all led by thought-leading cyber security practitioners. Summits focus on a particular security discipline.

All this means a SANS Summit offers cyber security professionals an opportunity to learn in a very focussed and effective way. Individual presentations from experts usually last for 45 minutes to an hour. This ensures a wide spectrum of technologies, insights and experiences are explored.

SANS Summits are also designed to be interactive. Attendees are encouraged to ask questions during panel sessions and the events offer many opportunities for professionals to network, and to expand personal networks.

Summits generally run for one day and coincide with a SANS Training Event, allowing students to maximise the learning and networking opportunity.

The registration fee for a SANS Summit is significantly reduced for those taking a training course at the same event.

THE FOLLOWING EUROPEAN SUMMITS ARE TAKING PLACE:

Visit the SANS webpage for an agenda and also information about the associated SANS Training Event. For information about SANS ICS Curriculum, see page 19; for DFIR courses, see page 17; and for more information about SANS' Security Awareness products, see page 31.

SANS INSTRUCTORS

SANS Instructors are considered the best in the world.

SANS cyber security training has achieved its reputation for excellence in part because SANS Instructors are the best in their respective fields.

Whatever their professional sphere - be it defence, management, DFIR, ICS, audit, pen testing or software development - we believe SANS Instructors are second to none.

Our Instructors are real-world expert practitioners who hold influential security roles in prominent organisations across the globe.

SANS Instructors are active practitioners, involved daily in the technical cut-and- thrust of cyber security. They know about the latest threats because it's their job, more often than not, to face them down.

Along with their technical and professional credentials, SANS Instructors are skilled teachers. They understand how to bring their subjects to life and, above all, they are great communicators.

In part this is down to the rigorous selection and training process SANS Instructors must follow before they are accredited and cleared to run classes – this process can span several years.

Here we profile some of the SANS Instructors that are teaching in the EMEA region in the coming months.

www.sans.org/emea

Steve Armstrong
CERTIFIED INSTRUCTOR
@Nebulator

Steve began working in cyber security while serving in the RAF. Before retiring from active duty, he led the RAF's penetration and TEMPEST testing teams. Today, Steve provides penetration testing and incident response services.

Dr Eric Cole
FELLOW
@drericcole

Dr. Cole is an industry-recognised security expert with over 20 years of hands-on experience. With a master's degree in computer science from NYIT and a doctorate from Pace University, he served as CTO of McAfee and Chief Scientist for Lockheed Martin. He was inducted into the InforSec European Hall of Fame in 2014.

Robert M. Lee
CERTIFIED INSTRUCTOR
@robertmlee

Rob has a passion for control system traffic analysis, incident response, and threat intelligence research. He is the course author of SANS ICS515 - Active Defence and Incident Response and the co-author of SANS FOR578 – Cyber Threat Intelligence.

James Lyne
CERTIFIED INSTRUCTOR
@jameslyne

James comes from a background in cryptography but, over the years, has worked in a wide variety of security domains including anti-malware, forensics, incident response and hacking. James participates in industry panels, policy groups, and is a frequently called upon expert advisor all over the world. He's a director at SANS EMEA and Global Head of Research with Sophos.

Ted Demopoulos

CERTIFIED INSTRUCTOR

@teddemop

Ted Demopoulos' first significant exposure to computers was in 1977 when he had unlimited access to his high school's PDP-11 and hacked at it incessantly. His background includes over 25 years of experience in information security and business, including more than 20 years work as an independent consultant.

Bryce Galbraith

PRINCIPAL INSTRUCTOR

@brycegalbraith

As a contributing author of the internationally bestselling book Hacking Exposed: Network Security Secrets & Solutions, Bryce helps bring the secret world of hacking into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies and was a member of Foundstone's renowned penetration testing team.

Jess Garcia

PRINCIPAL INSTRUCTOR

@j3ssgarcia

Jess is an active researcher in the fields of DFIR and malware analysis. He is an internationally recognised cyber security expert, and has led the response and forensic investigation of some of the world's biggest incidents in recent times.

Paul A. Henry

SENIOR INSTRUCTOR

@phenrycissp

Paul A. Henry is one of the world's foremost information security and computer forensic experts, with over 30 years of experience. Throughout his career, Paul has played a key strategic role in launching new network security initiatives. technologies.

Dave Shackleford

SENIOR INSTRUCTOR

@daveshackleford

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organisations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert.

Stephen Sims

SENIOR INSTRUCTOR

@steph3nsims

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modelling, and penetration testing.

Lance Spitzner

CERTIFIED INSTRUCTOR

@lspitzner

Lance is an internationally recognised leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organisations as small as 50 employees and as large as 100,000.

Erik Van Buggenhout

@erikvabu

Next to his teaching activities for SANS, Erik is the head of technical security services at nViso. At nViso, Erik focuses mainly on security assessments (both on a network and application level). Next to security assessments, he also advises clients on how they can improve their IT security posture.

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION: INFORMATION SECURITY

Information security professionals are responsible for research and analysis of security threats that may effect an organisation's assets, products, or technical specifications.

These security professionals will dig deeper into technical protocols and specifications related to security threats than most of their peers, identifying strategies to defend against attacks by gaining an intimate knowledge of the threats.

SAMPLE JOB TITLES:
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

FUNCTION: NETWORK OPERATIONS CENTRE, SYSTEM ADMIN, SECURITY ARCHITECTURE

A Network Operations Centre (NOC) is where IT professionals supervise, monitor, and maintain the enterprise network. The NOC is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks.

The NOC analysts work hand-in-hand with the Security Operations Centre, which safeguards the enterprise and continuously monitors threats against it.

SAMPLE JOB TITLES:
Security Analyst / Engineer, SOC Analyst, Cyber Threat Analyst, CERT Member, Malware Analyst

CORE COURSES
SEC301 GISF › SEC401 GSEC › SEC501 GCED

SEC505
Securing Windows with PowerShell and the Critical Security Controls
GCWN

SEC506
Securing Linux/Unix
GCUX

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

SEC579
Virtualisation and Private Cloud Security

FUNCTION: INCIDENT RESPONSE

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responder not only has to be technically astute, he/she must be able to handle stress under fire while navigating people, processes, and technology to help respond and mitigate a security incident.

SAMPLE JOB TITLES:
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

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

Endpoint Analysis

FOR408
Windows Forensic Analysis
GCFE

FOR508
Advanced Digital Forensics and Incident Response
GCFA

Malware Analysis

FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

FOR578
Cyber Threat Intelligence

Specialisations

FOR526
Windows Memory Forensics In-Depth

MGT535
Incident Response Team Management

FUNCTION: PENETRATION TESTING/ VULNERABILITY ASSESSMENT

Because offense must inform defense, these experts provide enormous value to an organisation by applying attack techniques to find security vulnerabilities, analyse their business risk implications, and recommend mitigations before they are exploited by real-world attackers.

SAMPLE JOB TITLES:
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

Network & Exploits

SEC560
Network Penetration Testing and Ethical Hacking
GPEN

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GXPN

SEC760
Advanced Exploit Development for Penetration Testers

Web

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

Mobile / Wireless

SEC575
Mobile Device Security and Ethical Hacking
GMOB

SEC617
Wireless Ethical Hacking, Penetration Testing, and Defenses
GAWN

Lab Centred

SEC561
Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

SEC562
CyberCity Hands-on Kinetic Cyber Range Exercise

Specialisations

SEC580
Metasploit Kung Fu for Enterprise Pen Testing

SEC573
Python for Penetration Testers

FUNCTION:

SECURITY OPERATIONS CENTRE/ INTRUSION DETECTION

The Security Operations Centre (SOC) is the focal point for safeguarding against cyber-related incidents, monitoring security, and protecting assets of the enterprise network and endpoints. SOC Analysts are responsible for enterprise situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.

CORE COURSES
SEC301 ▸ SEC401

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

SAMPLE JOB TITLES:
Intrusion Detection Analyst, Security Operations Centre 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

SEC502
Perimeter Detection In-Depth
GPPA

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GCIA

SEC511
Continuous Monitoring and Security Operations
GMON

SEC550
Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence

FOR578
Cyber Threat Intelligence

FUNCTION:

RISK & COMPLIANCE/AUDITING/ GOVERNANCE

These experts assess and report risks to the organisation by measuring compliance with policies, procedures, and standards. They recommend improvements to make the organisation more efficient and profitable through continuous monitoring of risk management.

SAMPLE JOB TITLES:
Auditor, Compliance Officer

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

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

FUNCTION:

SECURE DEVELOPMENT

The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws.

This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

SAMPLE JOB TITLES:
Developer, Software Architect, QA Tester, Development Manager

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

DEV522
Defending Web Applications Security Essentials
GWEB

DEV541
Secure Coding in Java/JEE: Developing Defensible Applications
GSSP-JAVA

DEV544
Secure Coding in .NET: Developing Defensible Applications
GSSP-.NET

Specialisations

SEC542
Web App Penetration Testing & Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing & Ethical Hacking

FUNCTION:

CYBER OR IT SECURITY MANAGEMENT

Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

SAMPLE JOB TITLES:
CISO, Cyber Security Manager / Officer, Security Director

Foundational	Core	Specialisation
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 Communication, 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	

FUNCTION:

DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

With today's ever-changing technologies and environments, it is inevitable that every organisation will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. To help solve these challenges, organisations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

SAMPLE JOB TITLES:
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

FOR518
MAC Forensic Analysis

FOR526
Memory Forensics In-Depth

FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

FUNCTION:

INDUSTRIAL CONTROL SYSTEMS / SCADA

ICS-focused courses are designed to equip both security professionals and control system engineers with the knowledge & skills they need to safeguard critical infrastructure.

ICS410
ICS/SCADA Security Essentials
GICSP

ICS515
ICS Active Response and Defense & Response

SAMPLE JOB TITLES:
IT & OT Support, IT & OT Cyber Security, ICS Engineer

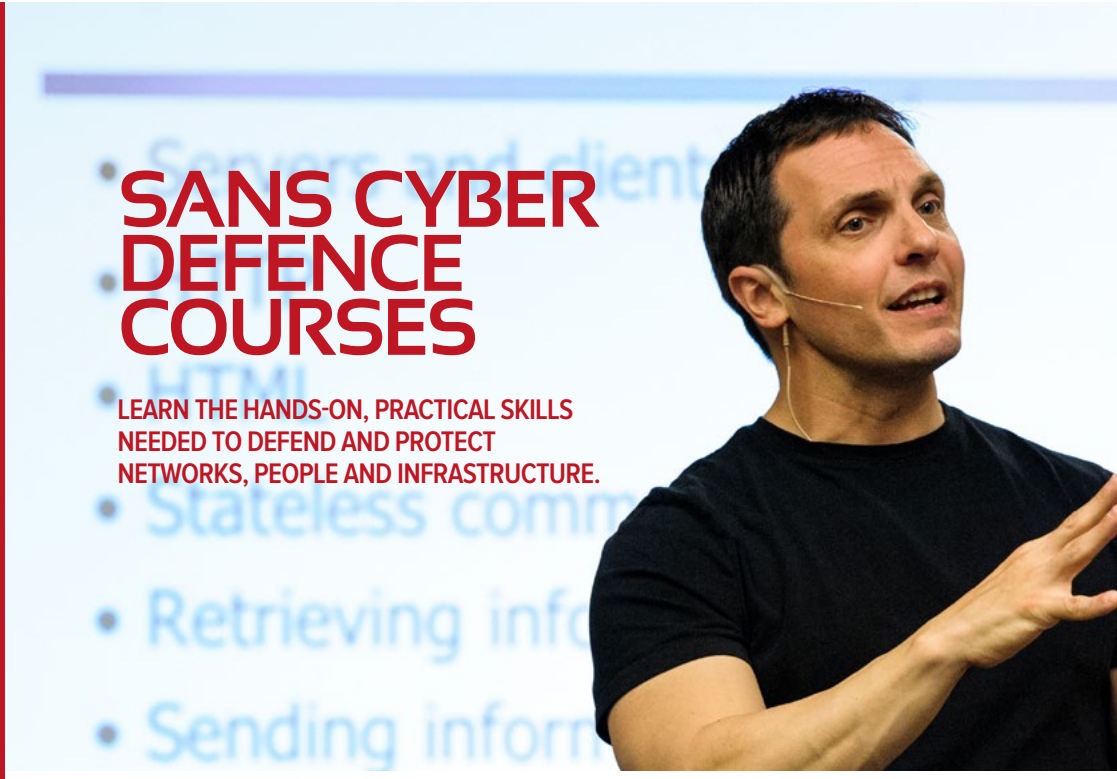
INDEX

COURSES FROM SANS CYBER DEFENCE CURRICULUM

CORE SECURITY

NETWORK & SECURITY OPERATIONS

SANS CYBER DEFENCE COURSES



LEARN THE HANDS-ON, PRACTICAL SKILLS NEEDED TO DEFEND AND PROTECT NETWORKS, PEOPLE AND INFRASTRUCTURE.

SANS Cyber Defence curriculum teaches the cyber security skills necessary to prevent, detect and respond to digital threats. Two sub curricula comprise the full Cyber Defence Curriculum: Core Security and Network and Security Operations.

SANS Cyber Defence Curriculum explores how to perform the following core cyber defence duties:

- Detect, prevent and respond to attacks
- Design and build secure business procedures
- Identify, assess and remediate exposures in existing networks
- Model a threat and plan a defence
- Communicate a cyber attack - and its ramifications - to managers
- Build security solutions that are scalable
- Secure and protect an organisation's intellectual property

SANS Cyber Defence Curriculum teaches all of these skills, and more.

EQUIPPED TO DEFEND

SANS training is hands-on. Rather than just sharing well-known theories, SANS courses place an emphasis on opening a command line prompt and working through an attack or defence situation.

SANS' success is rooted in the quality of its people, specifically our Instructors' experience.

SANS Instructors are experts in their respective fields. They are security practitioners who work on the frontline. They're acquainted with the dominant threats organisations face, and understand the prevailing defences.

SANS also equips students with a wealth of supplementary learning resources. Students are, for example, provided with a library of textbooks. The books are created by the same experts who created the course they support. We also provide students with posters, cheat sheets and software tool kits. All of our training content is updated regularly. ●

"I GOT A REAL INSIGHT INTO THE MIND OF THE ADVERSARY."
London
SEC401

"THIS WAS THE BEST AND MOST WELL-PRESENTED COURSE I EVER ATTENDED."
London
SEC401

SANS FORENSICS AND INCIDENT RESPONSE COURSES

HANDS ON AND INTENSIVE DIGITAL FORENSICS AND INCIDENT RESPONSE TRAINING DELIVERED BY ACKNOWLEDGED SECURITY AND FORENSICS EXPERTS.

SANS Digital Forensic and Incident Response curriculum (DFIR) helps organisations investigate and respond effectively to IT security breaches.

SANS DFIR Curriculum offers a great deal of scope for specialisation. SANS offers courses that hone in on Windows, smartphone, Apple operating systems, network and memory forensics, and more.

SANS DFIR Curriculum helps organisations deploy the correct responses. Responses designed to minimise financial and reputation loss, and to help businesses recover strongly from an attack.

RESORUCES

SANS DFIR Instructors are industry practitioners who spend the majority of their professional lives working on security's front line. They bring this real-world experience into the classroom.

Many SANS Instructors are prominent members of the DFIR community. They write, blog, speak, and contribute to the global consensus.

Along with their technical credentials, our DFIR Instructors are skilled teachers. They understand how to get the best from their students.

SANS supplies students with courseware and supplementary resources. We provide every student with a library of textbooks that related directly to the course – books that are written by the course's author.

SANS also supplies students with licences for software tools explored in class. This means students can deploy the skills they've learned as soon as they get back to their desk. ●

INDEX

COURSES FROM SANS DIGITAL FORENSICS AND INCIDENT RESPONSE CURRICULUM:

"INTENSE, NOTHING CAN PREPARE YOU FOR LEARNING FROM A TRUE MASTER OF THEIR ART."

London

FOR508

"MOST INTERESTING COURSE EVER. THIS COURSE BRINGS YOU THE NEXT LEVEL OF FORENSICS. THERE'S A LOT TO LEARN."

Brussels

FOR508

"EXCELLENT. THE BREADTH OF THIS COURSE IS AWE INSPIRING."

London

FOR508

INDEX

COURSES FROM SANS PENETRATION TESTING CURRICULUM:

SANS PENETRATION TESTING COURSES

HANDS-ON PENETRATION TESTING SECURITY TRAINING THAT TEACHES HOW TO THINK, WORK AND ATTACK LIKE A HACKER.

SANS Pen Test courses focus on one objective: equipping students with the technical skills, knowledge and tools they need to make a difference, as soon as they get back to the office.

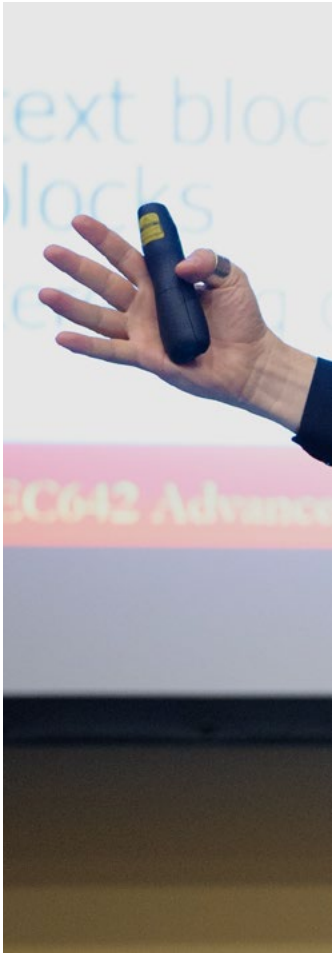
SANS Pen Test training is hands on. Students can expect in-depth lab exercises, simulations, cryptographic challenges and war games.

At the heart of our penetration test training curriculum is a belief in high-value testing. This encompasses:

- Modelling the activities of real-world attackers.
- Finding vulnerabilities in target systems.
- Exploiting them under controlled circumstances.
- Determining and documenting business risk.
- Applying technical excellence.
- Working in a professional, safe fashion according to a carefully designed scope and rules of engagement.
- Helping an organisation prioritise its resources to improve the security stance.

REAL WORLD EXPERIENCE

SANS Penetration Testing Instructors bring expert technical and industrial experience into the classroom. Many Instructors hold prominent positions in high-profile, global organisations. Others run pen test consultancies and work with prominent businesses. SANS Instructors bring this experience into the classroom.



"BEST COURSE I HAVE EVER BEEN ON. WORTH EVERYTHING REGARDLESS OF COST."

London

SEC575

"OVERALL A WELL PRESENTED AND COMPREHENSIVE COURSE THAT I WOULD RECOMMEND TO ANY INFORMATION SECURITY PROFESSIONAL."

London

SEC560

SANS INDUSTRIAL CONTROL SYSTEMS COURSES

LEARN THE SKILLS AND KNOWLEDGE NEEDED TO DEFEND INDUSTRIAL CONTROL SYSTEMS FROM CYBER ATTACK.

SANS ICS Curriculum has been created to assist two groups of professionals: Control system engineers who need to learn more about security best practice and securing their infrastructure, and IT security practitioners who need a clearer understanding of ICS' key technologies.

SANS ICS training curriculum is hands-on. Courses feature many live lab based exercises and simulations. Students can, for example, gain experience of network capture forensics, spoofing Modbus-TCP control signals, and finding passwords in EEPROM dumps.

SANS ICS training provides:

- Real world training – A panel of experts with an intimate understanding of ICS cyber security and SCADA principles create course content.
- Training for engineers – Specialised training is designed to help engineers understand security.
- Training for security professionals –Training helps security staff understand SCADA security and embedded systems, their functions and their limitations.
- Courses led by experts – Training classes are taught by respected experts in the ICS field.
- Extensive courseware –ICS students are equipped with a library of textbooks and extra material.

"VALUABLE COURSE FOR ENGINEERS, IT AND PHYSICAL SECURITY CONSULTANTS FOR INDUSTRIAL CONTROL SYSTEMS."

London
ICS410

INDEX

COURSES FROM SANS ICS CURRICULUM

"I THINK IT SECURITY PERSONNEL AND ENGINEERS FROM ANY COMPANY USING ICS SHOULD ATTEND THIS COURSE."

London
ICS410

INDEX

COURSES FROM SANS MANAGEMENT AND AUDIT CURRICULUM

"THE COURSE HELPED ME TO SHARPEN UP MY AWARENESS PROGRAMME PLANNING FOR NEXT YEAR."

London

MGT433

SANS MANAGEMENT AND AUDIT COURSES

HANDS-ON TRAINING DESIGNED TO EQUIP ADVANCING MANAGERS AND AUDITORS WITH THE SKILLS NEEDED TO BUILD THE RIGHT POLICIES AND PROCESSES, AND TO MAKE THE BEST IT SECURITY DECISIONS.

SANS Management Curriculum teaches students how to manage security. Courses are ideal for newly appointed information security officers, skilled administrators who are stepping up to a management role, and seasoned managers who find themselves managing technical people.

TRAINING FOR IT SECURITY AUDITORS

SANS Audit training equips students to audit many business critical technologies such as applications, databases, networks and perimeter defences. Our curriculum teaches risk-based methodologies that yield far better enterprise security.

SANS Audit training also teaches the practical skills and techniques needed to perform a comprehensive IT audit. With a hands-on approach to training, SANS exposes students to the best tools – and best practices – needed to add business value through their audits.

Our courses develop and expand students' knowledge of audit's Critical Security Controls.

TRAINING FOR SECURITY MANAGERS

Two SANS Management Courses that run at Training Events in the EMEA region are - MGT433: Securing The Human: Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program, and MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™.

MGT512 is a hands-on course designed to impart the skills and knowledge necessary to lead a project or product's security components.

The course empowers managers and auditors to speak the same language as technical staff including system, security and network administrators.

MGT433 focusses on helping managers to create, deploy, and access the efficacy of a high-impact security awareness campaign.

All SANS Management Courses are taught by SANS Instructors. Our Management Instructors are, primarily, practicing cyber security management professionals. They bring this real-world experience into the classroom.

Students are equipped with a wealth of courseware and resources to supplement their learning. We supply, for example, a library of expertly written textbooks. ●

"THIS COURSE IS EXCELLENT AS IT COVERS MOST OF THE TECHNICAL AUDITING TECHNIQUES AND TOOLS USED FOR THE AUDITING."

Dubai UAE

AUD507

"EXCELLENT FOUNDATION FOR NEW SECURITY MANAGERS"

London

MGT512

SANS SECURE SOFTWARE DEVELOPMENT COURSES

PLACING SECURE SOFTWARE DEVELOPMENT PRACTICE AND PRINCIPLES AT ITS HEART, SANS TEACHES HOW TO ARCHITECT DEFENSIBLE APPLICATIONS.

SANS Secure Software Development courses are built with two outcomes in mind. Firstly to equip programmers with the skills and knowledge to write secure code. Secondly, alumni are able to recognise the security shortcomings in existing code.

The SANS Secure Software Development Curriculum covers secure coding across C and C#, .NET, Java/JEE and web applications. We also offer deep dive courses that focus on developing and architecting defensible applications.

Organisations looking to further enhance their software and product security can also access SANS' penetration testing curriculum. Specifically, SANS offers a course designed to teach web application pen testing.

At the heart of SANS Secure Software Development curriculum is a promise. As soon as students return to their team from their training they'll be able to deploy what they've learned.

ARCHITECT SECURELY

SANS Secure Software Development is designed to foster safety by design. Our developer security training courses teach students to:

- Build securely – Our courses teach development's defining security principles.
- Hunt for flaws – Learn to find security issues in existing code.
- Secure across different languages – Courses address .NET, C & C++, JAVA/JEE.
- Stay current - SANS Software Security Curriculum exemplifies our drive to stay one step ahead of criminals.
- Engineer with security in mind – SANS Instructors are real-word practitioners who specialise in architecting defensible applications.
- Be prepared – Students receive a wide selection of textbooks, tools, and learning resources. All of which they can keep and refer back too.

Outside of the classroom our Secure Software Development Instructors are respected practitioners and proponents in the field of defensive programming.

SANS training is designed to be hands on. Expect a long list of live, code based lab exercises.

"DEV522 REALLY COVERS THE SECURITY ASPECTS EVERY WEB DEVELOPER MUST KNOW."
London
DEV522

"THE BEST COURSE TO TAKE YOU FROM ZERO TO HERO IN WEB PENETRATION IN SIX DAYS."
London
SEC542

INDEX

COURSES FROM SANS SECURE SOFTWARE DEVELOPMENT CURRICULUM:

"A VERY KNOWLEDGEABLE INSTRUCTOR WHO DEMONSTRATES VERY WELL THE ISSUES AND SOLUTIONS IN MODERN WEB APPS SECURITY."
London
DEV522

YOU WILL BE ABLE TO...

- Design and build a network architecture using VLAN's, NAC and 802.1x based on an APT indicator of compromise
- Run Windows command line tools to analyse the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat,etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organisation and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilising various tools to include dumpsec and OpenVAS, and once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Determine overall scores for systems utilising CIS Scoring Tools and create a system baseline across the organisation

WHO SHOULD ATTEND?

- Security Professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations Personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT Engineers and Supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

WWW.SANS.ORG/SEC401
Hands On | Six Days | Laptop Required
46 CPE/CMU Credits | GIAC Cert: GSEC

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

SEC401 TRAINING EVENT DATES

SANS PRAGUE
May 9 – 14
SANS LONDON SUMMER
Jul 9 – 18
SANS LONDON AUTUMN
Sep 19 – 24
SANS GULF REGION
Nov 5 – 17
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

SEC401 focusses on teaching the steps necessary to prevent attacks and to detect adversaries. It imparts actionable techniques that students can apply directly when they get back to work. Students who attend learn tips and tricks from the experts, equipping them with the skills needed to win the battle against a wide range of cyber adversaries. The course is built around the maxim: "Prevention is ideal but detection is a must."

With advanced persistent threats, it is almost inevitable that organisations will be targeted. Whether the attacker is successful in penetrating an organisation's network depends on the effectiveness of the organisation's defence.

Defending against attacks is an ongoing challenge, with new vectors emerging all of the time, including the next generation of threats. Organisations need to understand what really works in cyber security. What has worked, and will always work, is the idea of taking a risk-based approach to cyber defence.

Before an organisation spends its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. What is the most cost-effective way to reduce the risk?

Security is all about making sure businesses focus on the right areas of defence. In SEC401, students learn the language and underlying theory of computer and information security. The course teaches essential and effective security knowledge. It also equips defenders who have been given responsibility for securing systems with the skills needed to succeed.

This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security Instructors in the industry.

"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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC501
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCED

SEC 501

ADVANCED SECURITY ESSENTIALS ENTERPRISE DEFENDER

SEC501 TRAINING EVENT DATES

SANS BRUSSELS AUTUMN
Sep 5 – 10
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Cyber security continues to be a critical area for organisations and will increase in importance as attacks become stealthier, have a greater financial impact on businesses, and cause reputational damage. SEC501 lays a solid foundation for the security practitioner to engage the battle.

A key theme is 'prevention is ideal, but detection is a must'. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks continue to pose a threat to an organisation as data becomes more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organisation's best efforts to prevent attacks and protect its critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on networks and looking for indications of attack. This includes performing penetration testing and vulnerability analysis against an organisation to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

SEC501 is ideal for new supervisors and managers who aspire to go beyond being the boss. The course helps build leadership skills to enhance the organisation's climate and team-building skills to support the organisation's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

YOU WILL BE ABLE TO...

- Identify network security threats against infrastructure and build defensible networks that minimise the impact of attacks
- Access tools that can be used to analyse a network to prevent attacks and detect the adversary
- Decode and analyse packets using various tools to identify anomalies and improve network defences
- Understand how the adversary compromises systems and how to respond to attacks
- Perform penetration testing against an organisation to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process
- Use various tools to identify and remediate malware across your organisation
- Create a data classification program and deploy data-loss-prevention solutions at both a host and network level

WHO SHOULD ATTEND?

- Incident response and penetration testers
- Security operations centre engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

"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

"GREAT COURSE CONTENT VERY INTERESTING AND COMPREHENSIVE."
John O'Brien
AIRBUS DEFENCE & SPACE

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Apply perimeter security solutions in order to identify and minimise weaknesses to properly protect your perimeter
- Deploy and utilise multiple firewalls to understand the strengths and weaknesses that each present
- Use built-in tools to audit, protect and identify if systems have been compromised
- Utilise tcpdump to analyse network traffic in detail to understand what packets are communicating and how to identify potential covert channels
- Understand and utilise techniques to compromise and protect against application layer attacks
- Utilise tools to evaluate packets and identify legitimate and illegitimate traffic
- Use tools to evaluate and identify the risks related to Cloud Computing
- Inspect the intricate complexities of IP, including identifying malicious packets
- Evaluate and secure SSL, wireless networks, VPNs, applications and more
- Implement a logging solution that properly identifies risk and is manageable

WHO SHOULD ATTEND?

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network & system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

"JUST OUTSTANDING. THE INSTRUCTOR KNOWS HIS STUFF. BRINGS REAL WORLD EXPERIENCE TO THE DISCUSSIONS."

Stephen Dillon
MITRE

WWW.SANS.ORG/SEC502
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GPPA

SEC 502

PERIMETER PROTECTION IN-DEPTH

SEC502 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

There is no single fix for securing a network. Defending infrastructure requires mastery of multiple security techniques. Defenders cannot focus on a single OS or security appliance.

A proper security posture must consist of multiple layers. SEC502 is developed to provide the knowledge, and experience of the tools, necessary to ensure networks are secure at every layer. The course starts by looking at common problems. It explores questions such as: Why is unexpected traffic passing through a firewall? How did a machine that appears disconnected from the internet become compromised? Is there a better solution than anti-virus for controlling malware?

Cyber security professionals spend a great deal of time learning about the Internet Protocol. As such the majority of practitioners know how to assign an IP address. To secure a network, defenders need more. They need a clear understanding of the protocols.

SEC502 explores how IP works, how to spot abnormal patterns, and how to control them on the wire. From there, students experience a hands-on tour through wire-level assessment of a potential product, as well as what options and features are available.

The course delves into deploying traffic control while avoiding some of the most common mistakes. This isn't possible on the wire. A proper, layered defence needs to include each individual host - not just the hosts exposed to access from the internet. Hosts that have any kind of direct or indirect internet communication capability need to be assessed too.

SEC502 starts with OS lockdown techniques and moves on to third-party tools that permit anything from sandboxing insecure applications to full-blown application policy enforcement.

While technical knowledge is important, what really matters are the skills to properly leverage it. As such, the course focusses on problem solving and root cause analysis. They are vital to effective security architecture. Along with the technical training, students receive risk management capabilities.

"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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC503
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCIA

SEC 503

INTRUSION DETECTION IN-DEPTH

SEC503 TRAINING EVENT DATES

SANS PRAGUE
May 9 – 14
SANS LONDON SUMMER
Jul 9 – 18
SANS LONDON AUTUMN
Sep 19 – 24
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training needed to defend networks with confidence. Students learn about the underlying theory of TCP/IP and the most commonly used application protocols, such as HTTP. This enables students to intelligently examine network traffic for signs of an intrusion. Students master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so students transform knowledge into execution.

Basic exercises include assistive hints. Advanced options provide a more challenging experience for students who may already know the material, or for those who have quickly mastered new material. In addition, most exercises include an "extra credit" question intended to challenge even the most advanced student.

"IN ORDER TO DEFEND A NETWORK YOU NEED TO UNDERSTAND HOW IT WORKS, THIS COURSE IS BOTH ENJOYABLE AND CHALLENGING"
Holly C
MOD UK

Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade needed to perform packet and traffic analysis. It is supplemented with demonstration "pcaps," which are files that contain network traffic.

This allows students to follow along on their laptops with the class material and demonstrations. The pcaps provide a good library of network traffic to use when reviewing the material, especially for certification.

Our goal in SEC503: Intrusion Detection In-Depth is to acquaint students with the core knowledge, tools, and techniques necessary to defend networks. The training focusses on imparting new skills and knowledge that are deployable immediately.

"I LOVED THE COURSE. I HAD BIG EXPECTATIONS, BECAUSE I HAVE ALSO TAKEN THE 401 SECURITY ESSENTIALS COURSE AND IT WAS AMAZING TOO. ALL MY EXPECTATIONS HAVE BEEN COMPLETED. I HAD GREAT CLASSMATES AND WE HAD A LOT OF FUN DURING THE DAY AND THE EVENINGS."
Diana Moldovan
BETFAIR

YOU WILL BE ABLE TO...

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Synthesize disparate log files to widen and augment analysis
- Use the open-source network flow tool SiLK to find network behaviour anomalies
- Use knowledge of network architecture and hardware to customise placement of IDS sensors
- Sniff traffic off the wire

WHO SHOULD ATTEND?

- Intrusion Detection Analysts
- Network Engineers
- System, Security, and Network Administrators
- Hands-on Security Managers

"GOOD INTRODUCTION TO THE FUNDAMENTALS OF HOW PACKETS ARE CONSTRUCTED, HAPPY WITH THE CONTENT AND ORGANISATION."
Colin Sharp
HP

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Use Group Policy to harden Windows and applications, deploy Microsoft EMET, do AppLocker whitelisting, apply security templates, and write your own PowerShell scripts
- Implement Dynamic Access Control (DAC) permissions, file tagging, and auditing for Data Loss Prevention (DLP)
- Use Active Directory permissions and Group Policy to safely delegate administrative authority in a large enterprise to better cope with token abuse, pass-the-hash, service/task account hijacking, and other advanced attacks
- Install and manage a full Windows PKI, including smart cards, certificate auto-enrollment, and detection of spoofed root CAs
- Harden SSL, RDP, DNS, and other dangerous protocols
- Deploy Windows Firewall and IPSec rules through Group Policy and PowerShell
- Learn how to automate security tasks on local and remote systems with the PowerShell scripting language and remoting framework

WHO SHOULD ATTEND?

- Anyone who wants to learn PowerShell
- Windows security engineers and system administrators
- Anyone implementing the Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- Anyone who needs to reduce APT malware infections

"I HAVE BEEN TO OTHER WINDOWS TRAINING, BUT NEVER ONE WITH A FOCUS ON SECURITY. HAS BEEN EYE-OPENING EXPERIENCE. I HOPE TO ATTEND MORE EVENTS LIKE THIS IN THE FUTURE.."

Dewayne Wasson
KELLOGG COMPANY

WWW.SANS.ORG/SEC505
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCWN

SEC 505

SECURING WINDOWS WITH POWERSHELL AND THE CRITICAL SECURITY CONTROLS

SEC505 TRAINING EVENT DATES

SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

What is Windows Hello in Windows 10? How can defenders protect against pass-the-hash attacks, administrator account compromises, and the lateral movement of hackers inside a networks? How should the Critical Security Controls be implemented in a large Windows environment? SEC505 tackles these tough problems, and more.

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defences against them, especially when working in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is very useful, but there is no simple patch against the abuse of these tools.

SEC505's goal is teaching how to defend against both current Windows attack techniques, and also the likely types of attacks we can expect in the future. This requires more than just reactive patch management - we need to proactively design security into systems and networks.

Adversaries want to elevate their privileges to win control of servers and domain controllers. As such, a major theme of this course is controlling administrative powers through Group Policy and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows administrators, especially with the trend toward cloud computing. This course devotes the entire first day to PowerShell, then delivers more PowerShell exercises throughout the rest of the week. Don't worry, prior scripting experience
isn't necessary.

"THE TRAINING COURSE IS VERY PRACTICAL AND INTERESTING. SUPERIOR TO COMPARABLE MICROSOFT COURSE TITLES. VERY REAL WORLD ORIENTATED."

Paul Bendall
FIL

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC506
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCUX

SEC 506

SECURING LINUX / UNIX

SEC506 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

SEC506 provides in-depth coverage of Linux and Unix security issues. The course includes specific configuration guidance, practical advice, real-world examples, tips, and tricks.

The course examines how to mitigate or eliminate general problems that apply to all Unix-like operating systems. The list includes vulnerabilities in the: password authentication system, file system, virtual memory system, and in applications that commonly run on Linux and Unix.

The course teaches the skills and tools needed to handle security issues. The software tools explored are freely available and include: SSH, AIDE, sudo, lsof, and many others.

To ensure students can use the tools and techniques they've learned as soon as they return to work, SANS' classes are very practical. Hands-on exercises happen daily. SEC506 also puts these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

SEC506 TEACHES THE FOLLOWING SKILLS, TOOLS AND TECHNIQUES:

- Memory attacks, buffer overflows
- File system attacks, race conditions
- Trojan horse programs and rootkits
- Monitoring and alerting tools
- Unix logging and kernel-level auditing
- Building a centralised logging infrastructure
- Network security tools
- SSH for secure administration
- Server lockdown for Linux and Unix
- Controlling root access with sudo
- SELinux and chroot() for application security
- DNSSEC deployment and automation
- Mod security and web application firewalls
- Secure configuration of BIND and Apache
- Forensics investigation of Linux systems

GIAC CERTIFIED UNIX SECURITY ADMINISTRATOR
GCUX

"I HAVE BEEN A UNIX SYSTEMS ADMINISTRATOR FOR A COUPLE OF DECADES, BUT IN SEC506 I LEARNED SOMETHING NEW EVERY DAY."
Sheryl Coppenger
NCI INC.

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Analyse a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection dominant security architecture and security operations centres (SOC)
- Identify the key components of Network Security, Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organisations of all sizes
- Implement a robust Network Security Monitoring / Continuous Security Monitoring (NSM/CSM)
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Utilise tools to support implementation of Continuous Monitoring (CM) per NIST guidelines SP 800-137

WHO SHOULD ATTEND?

- Security Architects
- Senior Security Engineers
- Technical Security Managers
- SOC Analysts
- SOC Engineers
- SOC Managers
- CND Analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

WWW.SANS.ORG/SEC511
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GMON

SEC 511

CONTINUOUS MONITORING AND SECURITY OPERATIONS

SEC511 TRAINING EVENT DATES

SANS PRAGUE
May 9 – 14
SANS BRUSSELS AUTUMN
Sep 5 – 10
SANS GULF REGION
Nov 5 – 17
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Organisations invest significant amounts of time and resources trying to combat cyber attacks. Despite this tremendous effort, organisations are still compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture fails to prevent intrusions.

No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organisations to detect threats that will inevitably slip through their defences.

The underlying challenge for organisations is timely incident detection. Industry data suggests that most security breaches typically go undiscovered for an average of seven months. Attackers know that a lack of visibility and internal security controls allow them to methodically carry out their mission and achieve their goals.

"VERY COMPREHENSIVE, HANDS-ON AND CAN BE APPLIED TO WORKING ENVIRONMENT."
Ewa Konkolska
PRUDENTIAL, PGDS

The Defensible Security Architecture, Network Security Monitoring / Continuous Diagnostics and Mitigation / Continuous Security Monitoring, taught in this course will best position an organisation or Security Operations Centre to analyse threats and detect anomalies that could indicate cybercriminal behaviour.

The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology developed guidelines described in NIST SP 800-137 for Continuous Monitoring, and day five greatly increase students' understanding and enhances their skills in implementing Continuous Monitoring systems utilising NIST framework.

"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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC579
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

SEC 579

VIRTUALISATION AND PRIVATE CLOUD SECURITY

SEC579 TRAINING EVENT DATES

SANS LONDON AUTUMN
Sep 19 – 24
SANS GULF REGION
Nov 5 – 17

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Server virtualisation is one of today's most rapidly evolving and widely deployed technologies. Many organisations are already realising the cost savings from implementing virtualised servers. What's more, administrators love virtualised systems' ease of deployment and management.

With these benefits comes a dark side. Virtualisation technology is the focus of many new potential threats and exploits, and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams.

SEC579 starts with two days of architecture and security design for both virtual and private cloud infrastructures. The entire range of components is covered, ranging from hypervisor platforms to virtual networking, storage security, and locking down the individual virtual machine files.

The third and fourth days of SEC579 detail offense and defence - how virtualised environments can be assessed using scanning and penetration testing tools and techniques. The course also asks: how do things change when we move to a cloud model?

Once offense has been covered, SEC579 takes the opposite approach and goes into detail on performing intrusion detection and logging within the virtual environment, as well as covering anti-malware advances and changes within virtual infrastructure.

Day five helps students adapt existing security policies and practices to the new virtualised or cloud-based infrastructure. SEC579 shows how to design a foundational risk assessment program and then build on this with policies, governance, and compliance considerations within an environment.

Day six covers the top virtualisation configuration and hardening guides from Defense Information Security Agency (DISA), Center for Internet Security (CIS), Microsoft, and VMware. The course focusses on the most critical lessons and instructions from these guides. Students then perform a scripted, hands-on audit of VMware technology using controls guidance from the VMware hardening guide.

YOU WILL BE ABLE TO...

- Lock down and maintain a secure configuration for all components of a virtualisation environment
- Design a secure virtual network architecture
- Evaluate virtual firewalls, intrusion detection and prevention systems, and other security infrastructure
- Evaluate security for private cloud environments
- Perform vulnerability assessments and pen tests in virtual and private cloud environments, and acquire forensic evidence
- Perform audits and risk assessments within a virtual or private cloud environment

WHO SHOULD ATTEND?

- Security personnel who are tasked with securing virtualisation and private cloud infrastructure
- Network & Systems Administrators who need to understand how to architect, secure, and maintain virtualisation and cloud technologies
- Technical Auditors and Consultants who need to gain a deeper understanding of VMware virtualisation from a security and compliance perspective

"EVERY SINGLE VIRTUALISATION ADMIN (IN OUR ORGANISATION) SHOULD TAKE THIS COURSE. I AM GOING TO PROMOTE THIS COURSE! "
Cory Verboom
DMO

"EXCELLENT COURSE, VERY RELEVANT TO MY OWN DUTIES. SO I WILL BE ABLE TO APPLY SKILLS TO THIS. A LOT OF INFO TO TAKE IN BUT WILL USE THE GOOD BOOKS TO REFRESH!"
Mike Costello
QUALCOMM

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defence
- Obfuscate DNS entries
- Create non-attributable Active Defence Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

WHO SHOULD ATTEND?

- General Security Practitioners
- Penetration Testers
- Ethical Hackers
- Web Application Developers
- Website Designers and Architects

WWW.SANS.ORG/SEC550
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits

SEC 550

ACTIVE DEFENCE, OFFENSIVE COUNTER-MEASURES AND CYBER DECEPTION

SEC550 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

COURSE DETAILS

The current threat landscape is shifting. Traditional defences are failing. Organisations need to develop new strategies to defend themselves. Even more importantly, cyber security professionals need to better understand who is attacking and why.

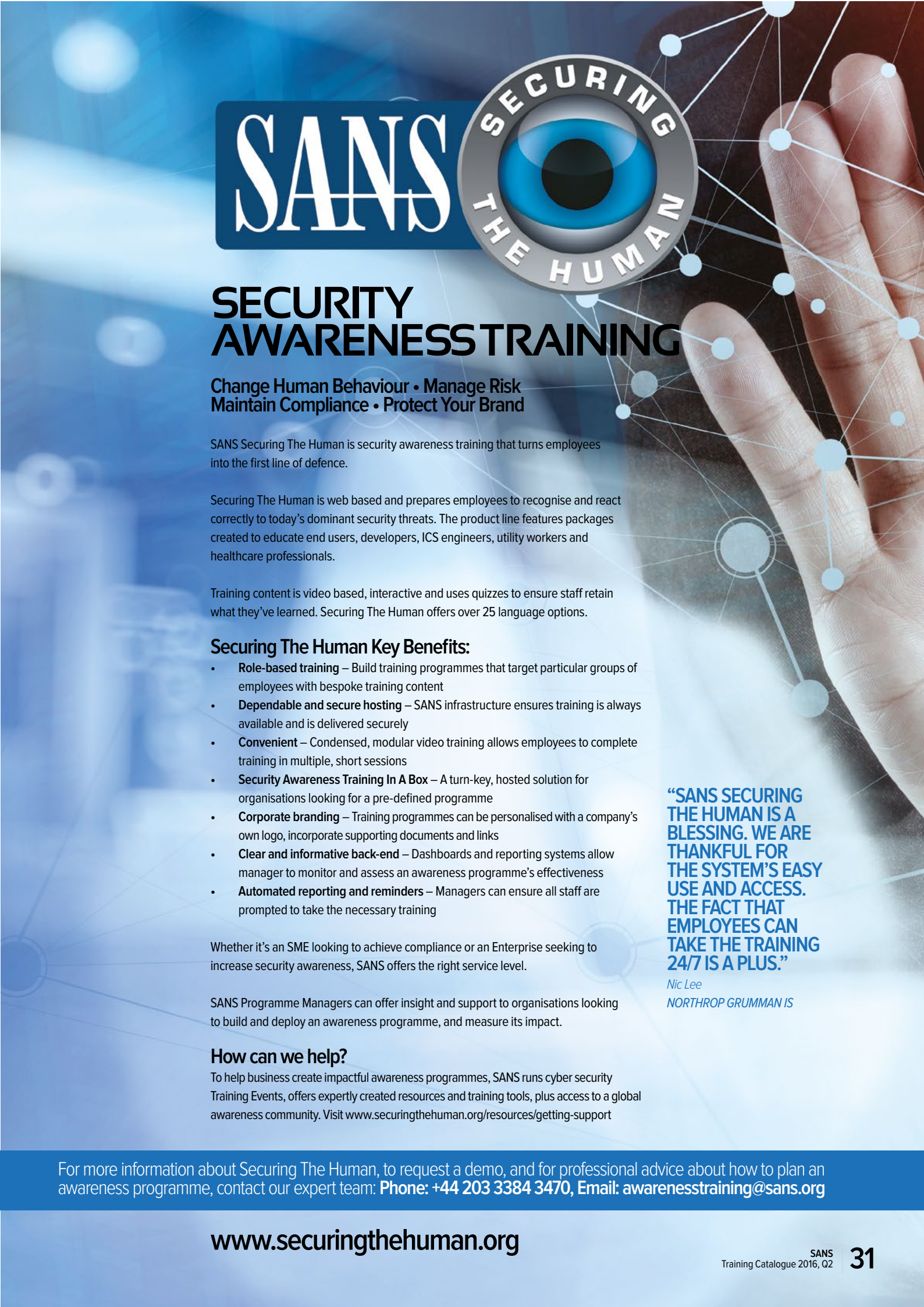
Students may be able to immediately implement some of the measures discussed on this course, while others may take a while. Either way, students should consider what to discuss during SEC550 as a collection of tools. Students can deploy them when they need to annoy attackers, determine who is attacking, and, finally, attack the attackers.

SEC550: Active Defence, Offensive Countermeasures and Cyber Deception are based on the Active Defence Harbinger Distribution live Linux environment. The Linux distro is funded by the Defence Advanced Research Projects Agency (DARPA).

This virtual machine is built from the ground up for defenders to quickly implement Active Defences in their environments. The course emphasises hands-on activities – SEC550 doesn't just talk about Active Defences, it works through labs that enable defenders to quickly and easily implement what's learned in their own working environment.

"REAL WORLD, AND BLUE TEAMS NEED THESE TYPES OF TOOLS AND PROCESSES, NOT ONLY WILL THIS HELP THEM DEFEND BUT GOOD FOR ALERTING-METRICS."
Bryon Mangler
MANDIANT

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)



SECURITY AWARENESS TRAINING

Change Human Behaviour • Manage Risk Maintain Compliance • Protect Your Brand

SANS Securing The Human is security awareness training that turns employees into the first line of defence.

Securing The Human is web based and prepares employees to recognise and react correctly to today's dominant security threats. The product line features packages created to educate end users, developers, ICS engineers, utility workers and healthcare professionals.

Training content is video based, interactive and uses quizzes to ensure staff retain what they've learned. Securing The Human offers over 25 language options.

Securing The Human Key Benefits:

- **Role-based training** – Build training programmes that target particular groups of employees with bespoke training content
- **Dependable and secure hosting** – SANS infrastructure ensures training is always available and is delivered securely
- **Convenient** – Condensed, modular video training allows employees to complete training in multiple, short sessions
- **Security Awareness Training In A Box** – A turn-key, hosted solution for organisations looking for a pre-defined programme
- **Corporate branding** – Training programmes can be personalised with a company's own logo, incorporate supporting documents and links
- **Clear and informative back-end** – Dashboards and reporting systems allow manager to monitor and assess an awareness programme's effectiveness
- **Automated reporting and reminders** – Managers can ensure all staff are prompted to take the necessary training

Whether it's an SME looking to achieve compliance or an Enterprise seeking to increase security awareness, SANS offers the right service level.

SANS Programme Managers can offer insight and support to organisations looking to build and deploy an awareness programme, and measure its impact.

How can we help?

To help business create impactful awareness programmes, SANS runs cyber security Training Events, offers expertly created resources and training tools, plus access to a global awareness community. Visit www.securingthehuman.org/resources/getting-support

"SANS SECURING THE HUMAN IS A BLESSING. WE ARE THANKFUL FOR THE SYSTEM'S EASY USE AND ACCESS. THE FACT THAT EMPLOYEES CAN TAKE THE TRAINING 24/7 IS A PLUS."

Nic Lee

NORTHROP GRUMMAN IS

For more information about Securing The Human, to request a demo, and for professional advice about how to plan an awareness programme, contact our expert team: **Phone: +44 203 3384 3470, Email: awarenesstraining@sans.org**

www.securingthehuman.org

YOU WILL BE ABLE TO...

- Analyse the structure of common attack techniques to be able to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilise tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defences and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyse router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access of a target machine using Metasploit, and then detect the artefacts and impacts of exploitation through process, file, memory, and log analysis
- Analyse a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyse the impacts of the scanning activity

WHO SHOULD ATTEND?

- Incident Handlers, Penetration Testers, Ethical Hackers, Incident Handling Team Leaders.
- System Administrators who are on the front line, defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack.

WWW.SANS.ORG/SEC504
Hands On | Six Days | Laptop Required
37 CPE/CMU Credits | GIAC Cert: GCIH

SEC 504

HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

SEC504 TRAINING EVENT DATES

SANS STOCKHOLM
May 9 - 14
SANS PEN TEST BERLIN
Jun 20 – 25
SANS LONDON SUMMER
Jul 9 – 18
SANS LONDON AUTUMN
Sep 19 – 24
SANS GULF REGION
Nov 5 – 17

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Organisations' systems are likely to get hacked. All that's needed is an internet connection or a disgruntled employee or two. From the five, ten, or even one hundred daily probes against internet infrastructure, to the malicious insider slowly creeping through vital information assets, attackers target systems with increasing viciousness and stealth.

SANS SEC504 helps defenders understand attackers' tactics and strategies in detail. It gives hands-on experience of finding vulnerabilities and discovering intrusions. This course equips students with a comprehensive incident handling plan. The in-depth information in this course helps turn the tables on computer attackers.

This course addresses the latest cutting-edge, insidious attack vectors, the "oldie but-goodie" attacks that are still so prevalent, and criminal methods between these extremes. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents. Students receive a detailed description of how attackers undermine systems. This empowers defenders to prepare for, detect, and respond to attacks. The course features hands-on workshops for discovering holes before the bad guys do.

Additionally, SEC504 discusses the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead, or are a part of, an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

GIAC CERTIFIED INCIDENT HANDLER
GCIH

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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC542
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GWAPT

SEC 542

WEB APP PENETRATION TESTING AND ETHICAL HACKING

SEC542 TRAINING EVENT DATES

SANS PEN TEST BERLIN
Jun 20 – 25
SANS OSLO
Oct 3 – 8
SANS GULF REGION
Nov 5 – 17
SANS LONDON
6 Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organisation. Unfortunately, there is no "patch Tuesday" for custom web applications. As a result, major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications, or by focusing on web apps as targets after an initial break-in.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organisations.

Students come to understand major web application flaws and their exploitation. More importantly, students learn a field-tested and repeatable process to consistently find these flaws and to convey what they have learned to their organisations.

Pen testing is a technical discipline. A high value penetration test doesn't however end with pure security findings. Rather, the best pen testers are able to explain what their discoveries mean to business leaders and budget holders. Organisations need to understand security flaws and they need to take them seriously.

In addition to high-quality course content, SEC542 focusses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn. The course features more than 30 formal hands-on labs, and culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture the Flag event brings students into teams to apply their newly acquired command of web application penetration testing techniques.

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

YOU WILL BE ABLE TO...

- Apply a detailed, four-step methodology to your web application penetration tests, including Recon, Mapping, Discovery, and Exploitation
- Analyse the results from automated web testing tools to remove false positives and validate findings
- Use Python to create testing and exploitation scripts during a penetration test
- Create configurations and test payloads within Burp Intruder to perform SQL injection, XSS, and other web attacks
- Use FuzzDB to generate attack traffic to find flaws such as Command Injection and File Include issues
- Assess the logic and transaction flaw within a target application to find logic flaws and business vulnerabilities
- Use Durzosploit to obfuscate XSS payloads to bypass WAFs and application filtering
- Analyse traffic between the client and the server application using tools such as Ratproxy and Zed Attack Proxy to find security issues within the client-side application code
- Use BeEF to hook victim browsers, attack the client software and network, and evaluate the potential impact XSS flaws have within an application
- Perform a complete web penetration test during the Capture the Flag exercise to pull all of the techniques and tools together into a comprehensive test.

WHO SHOULD ATTEND?

- General Security Practitioners
- Penetration Testers
- Ethical Hackers
- Web Application Developers
- Website Designers and Architects

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines and other publicly available information sources to build a technical and organisational understanding of the target environment
- Utilise the Nmap scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning to develop a map of target environments
- Configure and launch the Nessus vulnerability scanner so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customise the output from such tools to represent the business risk to the organisation
- Analyse the output of scanning tools to manually verify findings and perform false positive reduction using Netcat and the Scapy packet crafting tools
- Utilise the Windows and Linux command lines to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise and help determine business risks
- Configure the Metasploit exploitation tool to scan, exploit and then pivot through a target environment in-depth

WHO SHOULD ATTEND?

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Red team members
- Blue team members

WWW.SANS.ORG/SEC560
Hands On | Six Days | Laptop Required
37 CPE/CMU Credits | GIAC Cert: GPEN

SEC 560

NETWORK PENETRATION TESTING AND ETHICAL HACKING

SEC560 TRAINING EVENT DATES

SANS PRAGUE
May 9 – 14
SANS PEN TEST BERLIN
Jun 20 – 25
SANS BRUSSELS AUTUMN
Sep 5 – 10
SANS OSLO
Oct 3 – 8
SANS GULF REGION
Nov 5 – 17
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Security professionals have critical responsibilities: finding and understanding an organisation's vulnerabilities, and working diligently to mitigate these risks before criminals exploit them. SEC560 prepares practitioners to fulfill these duties, and more.

SEC560 starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps. The course has over 30 detailed hands-on labs.

SEC560 prepares students to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other internet and intranet infrastructure. The course offers many real-world, hands-on tips – all from the world's leading pen testers.

Students learn to scan target networks using best-of-breed tools. In these tools, the course explores run-of-the-mill options and configurations. Lessons and units discuss these tools' more advanced capabilities.

"THANK FOR THE QUALITY (TECHNICAL AND RELATIONSHIP) ... IT WAS GREAT!"
Guillame Durand
NEOLASE

After scanning, students learn dozens of methods for exploiting target systems. SEC650 explores how to gain access and how to measure real business risk. Students learn to examine post-exploitation situations, password attacks, wireless, and web apps. SEC560 moves through the target environment to model real-world attacks too.

After building skills in five days of challenging labs, the course culminates in a full-day, real-world network penetration test scenario. Students conduct an end-to-end penetration test, applying the knowledge, tools and principles from SEC560. Students discover and exploit vulnerabilities in a realistic sample target organisation.

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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC561
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

SEC 561

IMMERSIVE HANDS-ON HACKING TECHNIQUES

PRIVATE TRAINING*

COURSE DETAILS

Top penetration testing professionals have fantastic hands-on skills. They are adept at finding, exploiting and resolving vulnerabilities. To help students achieve these skills quickly, SANS engineered SEC561: Immersive Hands-On Hacking Techniques from the ground up.

The course teaches in-depth security capabilities through 80%+ hands-on exercises. The course maximises the amount of time students spend in hands-on lab exercises. SEC561 is SANS' most hands-on course. With over 30 hours of intense labs, students experience a leap in their technical capabilities. Students leave the classroom equipped with the practical skills needed to handle demanding pen test and vulnerability assessment projects in enterprise environments.

"80% HANDS ON IS INTENSE AND AWESOME. BEST WAY TO BUILD ON PREVIOUS PEN TESTING FOCUSSED SANS COURSES."
Timothy McKenzie
DELL/SECUREWORKS

Throughout the course, an expert SANS Instructor coaches students as they work through solving increasingly demanding real-world information security scenarios. The skills learned are immediately deployable in the workplace.

Topics addressed in the course include:

- Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritise discovered vulnerabilities for effective remediation.
- Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defences against such attacks.
- Analysing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super-powerful Windows Remote Management (WinRM) tools.
- Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorised server access.
- Scouring through web applications and mobile systems to identify and exploit devastating developer flaws.
- Evading anti-virus tools and bypassing Windows User Account Control to understand and defend against these advanced techniques.
- Honing phishing skills to evaluate the effectiveness of employee awareness initiatives.

The course focusses on practical lessons and innovative tips, all with direct hands-on application. SEC561 also put students' new skills to the test in NetWars. NetWars scenarios are brand new and custom-developed.

"THE AMOUNT OF TOOLS AND INFORMATION PROVIDED IS EXTREMELY VALUABLE."
Roger Szulc
MDA

YOU WILL BE ABLE TO...

- Use network scanning and vulnerability assessment tools to effectively map out networks and prioritise discovered vulnerabilities for effective remediation
- Use password analysis tools to identify weak authentication controls leading to unauthorised server access
- Evaluate web applications for common developer flaws leading to significant data loss conditions
- Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- Bypass authentication systems for common web application implementations
- Exploit deficiencies in common cryptographic systems
- Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- Harvest sensitive mobile device data from iOS and Android targets

WHO SHOULD ATTEND?

- Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- Systems & network administrators who want to gain hands-on experience in information security skills to become better administrators
- Incident response analysts who want to better understand system attack and defence techniques
- Forensic analysts who need to improve their analytical skills through experience with real-world attacks
- Penetration testers seeking to gain practical hands on experience for use in their own assessments

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC562
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

SEC 562

CYBERCITY HANDS-ON KINETIC CYBER RANGE EXERCISE

YOU WILL BE ABLE TO...

- Scan for and discover the details associated with computer, network, and ICS assets
- Analyse and manipulate commonly used, very powerful, but often less-well-understood protocols such as Profinet, DNP3, Modbus, and more
- Work as part of a team analysing attacker actions and preventing kinetic impacts against industrial control systems
- Look for vulnerabilities in systems associated with electrical power distribution, water systems, traffic systems, and other infrastructures
- Use a variety of hands-on tools for analysing and interacting with target systems, including Wireshark, tcpdump, Nmap, Metasploit, and more
- Control various Human Machine Interfaces and Operator Interface Terminals widely used by SCADA and other Industrial Control Systems (ICSs)
- Prevent attackers from wreaking havoc by manipulating computers that control physical infrastructures

WHO SHOULD ATTEND?

- Red & Blue team members
- Cyber Warriors
- Incident Handlers
- Penetration Testers
- Ethical hackers
- Other security personnel who are first responders when systems come under attack.

"THIS COURSE IS THE GREATEST. I HAVE BEEN WAITING FOR THIS KIND OF COURSE CTF FOREVER. I LEARNT MANY THINGS FROM THIS COURSE."
Masashi Fujimara
HITACHI LTD

SEC562 TRAINING EVENT DATES

SANS ICS LONDON
Sep 19 – 25

PRIVATE TRAINING*

"BEST CLASS EVER!"
Timothy McKenzie
DELL/SECUREWORKS

COURSE DETAILS

Computers, networks, and programmable logic controllers operate most of our modern world's physical infrastructure. Systems ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation.

Increasingly, security professionals need the skills to assess and defend these important infrastructures. SEC562 is based on the SANS CyberCity kinetic range. Students learn how to analyse and assess the security of control systems and related infrastructures, finding vulnerabilities that could result in significant kinetic impact.

YOU WILL LEARN:

- How to analyse cyber infrastructures that control and impact kinetic infrastructures.
- How to manipulate a variety of key industrial protocols, including Modbus, CIP, DNP3, Profinet, and other SCADA-related protocols.
- How to rapidly prototype computer attack tools against specific vulnerabilities
- How to discover security flaws in a variety of SCADA and Industrial Control Systems (ICSs) and thwart attacks against them.
- How to conduct penetration tests and assessments associated with kinetic infrastructures.

AUTHOR STATEMENT

The world faces a critical shortage of professionals with the skills needed to defend the computer systems and network infrastructures that control our physical world.

SANS built SEC562 to help fill that gap, teaching practitioners how to analyse, control, and defend countless control systems, protocols, and other kinetic infrastructures they will increasingly face in the future.

SEC562 features SANS CyberCity, a cyber range where students can see the impact their hands-on lab work has on a model city, through real-time streaming video to the classroom. For example, when students restore the power grid, they see the lights in the city turn back on (and a newspaper article get published in real-time about the end of the blackout). Nearly every mission in the course provides visual impacts, which inspire and excite students and SANS Instructors alike.
(Ed Skoudis, Josh Wright, and Tim Medin)

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC573
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits | GIAC Cert: GPYC

SEC 573

PYTHON FOR PENETRATION TESTERS

SEC573 TRAINING EVENT DATES

SANS PEN TEST BERLIN
Jun 20 – 25

PRIVATE TRAINING*

COURSE DETAILS

SEC573: Python for Penetration Testers teaches the skills needed to tweak and customise existing tools. The course also explores how to develop original tools from scratch. SEC573 is designed to meet many different levels of skills, and appeals to a wide variety of backgrounds. Whether students have absolutely no coding experience, or are a skilled Python developer looking to apply coding skills to penetration testing, this course has something for everyone.

Practitioners cannot become a world-class tool builder by merely listening to lectures, so this course is chock full of hands-on labs. Every day we teach the skills needed to develop serious Python programs, and show how to apply those skills in penetration testing engagements.

The course begins with an introduction to SANS pyWars: a four-day Capture the Flag competition that runs parallel to the course material. It challenges existing programming skills and helps develop new skills. Experienced programmers quickly progress to more advanced concepts, while novice programmers spend time building a strong foundation.

Students then cover the essential skills required to get the most out of the Python language. The essentials workshop labs teach the concepts and techniques required to develop original tools. The workshop concentrates on essential programming skills and how to apply them in real-world scenarios.

The course also shares shortcuts that make even experienced developers more deadly. Once everyone understands the essentials, we apply those skills by developing tools to help in students' next penetration test.

In class, we develop a port-scanning, anti-virus-evading, client-infecting backdoor for placement on target systems, as well as a SQL injection tool to extract data from websites that are immune to off-the-shelf tools.

Students learn the concepts required to build a multi-threaded password guessing tool and a packet assembling network reconnaissance tool. The course concludes with a capstone one-day Capture the Flag event that complements the pyWars challenge. It tests the ability to apply those new tools and coding skills in a penetration testing challenge.

The ability to read, write, and customise software is what distinguishes the good penetration tester from the great one. The best penetration testers can customise existing open-source tools or develop their own tools. Unfortunately, even though organisations serious about security continually emphasise their need for skilled tool builders, many testers do not have these skills. Developing these skills is not beyond your reach. So when you are ready to fully weaponize your penetration testing skillset and build and use your own tools to automate your penetration testing skills, join SANS for SEC573: Python for Penetration Testers.

"EXCELLENT CLASS FOR BEGINNERS AND ADVANCED ALIKE. IT HAS SOMETHING FOR EVERYONE"
Mike Perez
DISNEY

YOU WILL BE ABLE TO...

- Write a backdoor that uses Exception Handling, Sockets, Process execution, and encryption to provide an initial foothold in a target environment The backdoor will include features such as a port scanner to find an open outbound port, techniques for evading antivirus software and network monitoring, and the ability to embed payload from tools such as Metasploit.
- Write a SQL injection tool that uses standard Python libraries to interact with target websites. You will be able to use different SQL attack techniques for extracting data from a vulnerable target system
- Develop a password-guessing attack tool with features like multi-threading, cookie handlers, support for application proxies such as Burp, and much more
- Write a network reconnaissance tool that uses SCAPY, StringsIO, and PIL to reassemble TCP packet streams, extract data payloads such as images, display images, extract metadata such as GPS coordinates, and link those images with GPS coordinates to Google maps

WHO SHOULD ATTEND?

- Security professionals who want to learn how to develop Python applications.
- Penetration testers who want to move from being a consumer of security tools to being a creator and modifier of security tools.
- Technologists who need custom tools to test their infrastructure and want to create those tools themselves.

"GREAT COMBINATION OF PRACTICE AND THEORY. FUN CHALLENGES."
Marek Kuczynski
SHELL

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Use jailbreak tools for Apple iOS and Android system
- Conduct an analysis of iOS and Android file system data to plunder compromised devices and extract sensitive mobile device use information
- Analyse Apple iOS and Android applications with reverse-engineering tools
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorised access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

WHO SHOULD ATTEND?

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

"I AM LEARNING A LOT REGARDING MOBILE PLATFORMS AND KEY DIFFERENCES BETWEEN ALL OF THEM. I RECOMMEND THIS COURSE FOR ANYONE THAT WANTS TO LEARN ABOUT MOBILE OS."

Hilal Lootah
TRA

WWW.SANS.ORG/SEC575
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GMOB

SEC 575

MOBILE DEVICE SECURITY AND ETHICAL HACKING

SEC575 TRAINING EVENT DATES

SANS STOCKHOLM
May 9 - 14

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

In most organisations mobile devices present the biggest attack surface, yet few professionals have the skills needed to assess them. SEC575 teaches these skills, and more. The course covers Android Marshmallow, iOS 9, Apple Watch and Android Ware.

SEC575 enables students to understand popular mobile operating systems' strengths and weaknesses. With these skills, students can evaluate the security weaknesses of built-in and third party applications.

As the course progresses, students learn to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. SEC575 also explores how to leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels.

Malware is addressed too. Students learn to work safely with samples and how to understand data exposure – across Android and iOS operating systems. SEC575 also addresses how to exploit lost or stolen devices, and how to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, students explore how to effectively communicate threats to key stakeholders. This process includes leveraging tools such as Mobile App Report Cards to characterise threats for management and decision makers, while identifying sample code and libraries that developers can use to address risks for in-house applications.

Through the use of their new skills, students learn to apply a mobile device deployment penetration test in a step-by-step fashion. This starts with gaining access to wireless networks to implement man-in-the-middle attacks and finishes with mobile device exploits and data harvesting. Students examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, students return to work prepared to conduct their own test, or better informed on what to look for and how to review an outsourced penetration test.

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC617
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GAWN

SEC 617

WIRELESS ETHICAL HACKING, PENETRATION TESTING, AND DEFENCES

SEC617 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Despite the security concerns many of us share regarding wireless technology, it is here to stay - and it is growing. Witness the deployment and utilisation of wireless LAN technology and Wi-Fi as well as with other applications including cordless telephones, smart homes, embedded devices, and more.

Technologies like ZigBee and Z-Wave offer new methods of connectivity to devices, while other wireless technologies, including Wi-Fi, Bluetooth, Bluetooth Low Energy, and DECT continue their massive growth rate - each introducing their own set of security challenges and attacker opportunities.

To be a wireless security expert, practitioners need a comprehensive understanding of the technologies, threats, exploits, and defensive techniques. Hands-on experience in evaluating and attacking wireless technologies are also essential skills.

Practitioners should also avoid limiting their skill-set to Wi-Fi alone. Standards-based and proprietary wireless technologies must also be evaluated too.

SEC617 takes an in-depth look at the security challenges posed by many different wireless technologies, exposing students to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students navigate the techniques attackers use to exploit Wi-Fi networks.

These include attacks against: WEP, WPA/WPA2, PEAP, TTLS, and other systems, including developing attack techniques leveraging Windows 7 and Mac OS X.

The course also examines commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, students receive the SWAT Toolkit, which is used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

Using assessment and analysis techniques, this course shows how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

YOU WILL BE ABLE TO...

- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, CarWhisperer, and btaptap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- Utilise wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organisation
- Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilise wireless fuzzing tools including Metasploit, file2air, and Scapy to identify new vulnerabilities in wireless devices

WHO SHOULD ATTEND?

- Ethical hackers and Penetration Testers
- Network & System Administrators
- Incident Response Teams
- Technical Auditors
- Wireless System Engineers
- Embedded Wireless System Developers
- Network Security Staff
- Information security policy decision makers
- Information security consultants

"GOOD COURSE. I WOULD RECOMMEND IT INTENSELY IN MY COMPANY. LARRY WAS GREAT."
Yaacon Apelbaum
AGT INT

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Assess and attack complex modern applications.
- Understand the special testing and exploits available against content management systems such as SharePoint and WordPress.
- Use techniques to identify and attack encryption within applications.
- Identify and bypass web application firewalls and application filtering techniques to exploit the system.
- Use exploitation techniques learned in class to perform advanced attacks against web application flaws such as XSS, SQL injection and CSRF.

WHO SHOULD ATTEND?

- Web Penetration Testers
- Security Consultants
- Developers
- QA Testers
- System Administrators
- IT Managers
- System Architects

"HANDS-ON AND TO THE POINT!"
Frans Kollée
MADISON GUIRKHA B.V.

WWW.SANS.ORG/SEC642
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

SEC 642

ADVANCED WEB APP PENETRATION TESTING AND ETHICAL HACKING

SEC642 TRAINING EVENT DATES

SANS COPENHAGEN
Apr 25 – 30
SANS LONDON AUTUMN
Sep 19 – 24

PRIVATE TRAINING*

COURSE DETAILS

SEC642 teaches the advanced skills and techniques required to test web applications. This advanced pen testing course uses a combination of lectures, real-world experiences, and hands-on exercises to impart the techniques used to test the security of enterprise applications. The course culminates in a Capture the Flag event.

The course begins by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced concepts and skills to exploit the system through various controls and protections.

SEC642 explores encryption as it relates to web applications. Students learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, students learn methods for exploiting or subverting this encryption, again through lecture and labs.

As students move through the course they learn to identify web application firewalls, filtering, and other protection techniques. Students explore methods to bypass these controls. To further the evaluation of security within the application, students gain skills in exploiting the control itself.

Following these general exploits, students study techniques that target specific enterprise applications. Participants attack systems such as content management and ticketing systems.

We explore the risks and flaws found within these systems and how to better exploit them. Due to their prevalence within modern organisations, this part of the course includes web services and mobile applications.

SEC642 ends with a day-long Capture the Flag event. This targets an imaginary organisation's web applications, includes both internet and intranet applications and various technologies.

In summary, SEC642 enhances students' exploitation and defence skill sets. It also fulfils a need to teach more advanced techniques, such as those covered in the foundational course, SEC542: Web Application Penetration Testing and Ethical Hacking.

"VERY GOOD TECHNIQUES AND METHODS COVERED WHICH WILL BE USEFUL TO ANY NEW APP TESTER."
Vivek Veerappan
GEMALTO

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC660
Hands On | Six Days | Laptop Required
46 CPE/CMU Credits | GIAC Cert: GXPN

SEC 660

ADVANCED PENETRATION TESTING, EXPLOIT WRITING, AND ETHICAL HACKING

YOU WILL BE ABLE TO...

- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform zero-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse engineer vulnerable code to write custom exploits

WHO SHOULD ATTEND?

- Network and Systems Penetration Testers
- Incident Handlers
- Application Developers
- IDS Engineers

SEC660 TRAINING EVENT DATES

SANS SECURE EUROPE
Apr 4 – 16
SANS LONDON SUMMER
Jul 9 – 18
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

The course presents students with dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment. This approach solidifies advanced concepts and allows for immediate application of techniques in the workplace.

Each classroom day includes a two-hour evening bootcamp, allowing students to further master the techniques discussed.

Course topics include: Weaponising Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, Return Oriented Programming (ROP), Windows exploit-writing, and much more.

SEC660 begins by introducing advanced penetration concepts and, to help prepare students for what lies ahead, provides an initial overview.

The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others.

Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments.

Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques.

Days four and five explore exploiting programs on the Linux and Windows operating systems. The final course day is dedicated to numerous penetration testing challenges, requiring students to solve complex problems and participate in capture the flag exercises.

"FROM HIGH-LEVEL CONCEPTS TO HANDS ON TRAINING THIS COURSE PROVIDES ENOUGH DETAILS AND DEPTH TO ALLOW ME TO SHOW THE SKILLSETS LEARNED IMMEDIATELY AFTER THE LEARNING, ALLOWING MY EMPLOYER TO SEE THEIR RETURN ON INVESTMENT."
Brian Anderson
NORTHROP GRUNMAN CORPORATION

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- Use the advanced features of IDA Pro and write IDC and IDA Python scripts
- Perform remote debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows
- Write Return Oriented Shellcode
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows heap overflows and use-after-free attacks
- Use precision heap sprays to improve exploitability
- Perform Windows Kernel debugging up through Windows 8 64-bit
- Jump into Windows kernel exploitation

WHO SHOULD ATTEND?

- Senior Network & System Penetration Testers
- Secure Application Developers (C & C++)
- Reverse-Engineering professionals
- Senior Incident Handlers
- Senior Threat Analysts
- Vulnerability Researchers
- Security Researchers

"THIS COURSE IS THE CHALLENGE I WAS LOOKING FOR. IT WILL BE OVERWHELMING, BUT WELL WORTH IT."

William Stott
RAYTHEON

WWW.SANS.ORG/SEC760
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

SEC 760

ADVANCED EXPLOIT DEVELOPMENT FOR PENETRATION TESTERS

SEC760 TRAINING EVENT DATES

SANS PEN TEST BERLIN
Jun 20 – 25

PRIVATE TRAINING*

COURSE DETAILS

Vulnerabilities in prominent operating systems are often very complex and subtle. Yet, they could expose organisations to significant attacks, undermining their defences when wielded by very skilled attackers. Few security professionals have the skillset to discover, let alone even understand at a fundamental level, why a vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity.

SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyse patches for one-day exploits, and write complex exploits (such as use-after-free attacks) against modern software and operating systems. Some of the skills you will learn in SEC760 include:

- How to write modern exploits against prominent operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilising a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modelling
- How to effectively utilise various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

"SEC760 IS A KIND OF TRAINING WE COULD NOT GET ANYWHERE ELSE."

Jenny Kitaichit
INTEL

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

CHALLENGE YOURSELF BEFORE THE ENEMY DOES

NETWARS

NetWars is a series of hands-on, in-depth computer and network security challenges designed to test a participants' experience and skills. NetWars Tournaments comes in two forms - Core and DFIR.

Core NetWars Tournament

SANS Core NetWars is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. In SANS' expertly designed courses, attendees consistently rate our hands-on exercises as the most valuable part of the course. With Core NetWars, we have raised the bar, as participants learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day.

Who should attend?

- Security professionals
- System Administrators
- Network Administrators
- Ethical Hackers
- Penetration Testers
- Incident Handlers
- Security Auditors
- Vulnerability Assessment Personnel
- Security Operations Center (SOC) staff members

DFIR NetWars Tournament

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges. DFIR NetWars Tournament is packed with challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

Who should attend?

- Digital Forensic Analysts
- Reverse Engineering & Malware Analysts
- Incident Responders
- Law Enforcement Officers, Agents, or Detectives
- Forensic Examiners Security Operations Center (SOC) analysts
- Cyber Crime Investigators
- Media Exploitation Analysts

sans.org/netwars

Students who register and pay for any long course (5 or 6 days) at a SANS event that includes a NetWars Tournament may participate in the tournament at that event free of charge.

YOU WILL BE ABLE TO...

- Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including: Who placed an artefact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artefact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information that the suspect was interested in finding and accomplish detailed damage assessments
- Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing Windows artifacts such as the Registry and log files

WHO SHOULD ATTEND?

- Information Security Professionals
- Incident Response Team Members
- Law Enforcement Officers, Federal Agents, or Detectives
- Media Exploitation Analysts
- Anyone interested in a deep understanding of Windows forensics

WWW.SANS.ORG/FOR408
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCFE

FOR 408

WINDOWS FORENSIC ANALYSIS

FOR408 TRAINING EVENT DATES

SANS SECURE EUROPE
Apr 4 – 16
SANS DFIR PRAGUE
Oct 3 – 15

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

FOR408: Windows Forensic Analysis focusses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. Defenders can't protect what they don't know about, and understanding forensic capabilities and artefacts is a core component of information security. Students learn to recover, analyse, and authenticate forensic data on Windows systems. Units focus on understanding how to track detailed user activity on a network, and how to organise findings for use in incident response, internal investigations, and civil/criminal litigation. Students also learn new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Windows is silently recording a huge amount of data about its users. FOR408 teaches how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Attendees learn to analyse everything from legacy Windows XP systems to just discovered Windows 10 artefacts.

FOR408 Windows Forensic Analysis teaches to:

1. Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012
2. Identify artefact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geo-location, file download, anti-forensics, and detailed system usage
3. Focus capabilities on analysis instead of how to use a specific tool
4. Extract key answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/FOR508
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCFA

FOR 508

ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

FOR508 TRAINING EVENT DATES

SANS COPENHAGEN
Apr 25 – 30
SANS LONDON SUMMER
Jul 9 – 18
SANS DFIR PRAGUE
Oct 3 – 15
SANS LONDON
Nov 14– 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Over 80% of breach victims learn about a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through a network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past few years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in an enterprise - they compromise hundreds. A team can no longer afford antiquated incident response techniques – techniques that fail to identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks. Situations include APT adversaries, organised crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on response tactics and techniques that elite responders are successfully using in real-world breach cases.

Elsewhere in the course, a hands-on enterprise intrusion lab (developed from a real-world targeted APT attack on an enterprise network and based on how an APT group will target your network) leads students through the challenges and solutions via extensive use of the SANS SIFT Workstation collection of tools.

During the intrusion lab exercises, students identify where the initial targeted attack occurred and lateral movement through multiple compromised systems. Participants extract and create crucial cyber threat intelligence that can help properly scope the compromise and detect future breaches.

"WE'RE SETTING UP A NEW FORENSIC CAPABILITY AND THIS COURSE HAS GIVEN ME EVERYTHING I NEED TO DO JUST THAT."
Simon Fowler
VIRGIN MEDIA

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Discover every system comprised in an enterprise utilising incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head and spear phishing at- tack mechanisms, lateral movement, and data exfiltration techniques.
- Use system memory and the volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response.
- Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI) to quickly ascertain the threat to an organisation and aid in scoping the true extent of the data breach
- Track the exact footprints of an attacker crossing multiple systems and observe data they have collected. Track an adversary's movements in a network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuth kit tool to discover how filesystems work and uncover powerful forensic artefacts such as NTFS $I30 directory file indexes, journal parsing, and detailed Master File Table analysis

WHO SHOULD ATTEND?

- Incident Response Team Leaders
- Security Operations Center (SOC) personnel and Information Security Practitioners
- Experienced Digital Forensic Analysts
- System Administrators
- Federal Agents and Law Enforcement
- Red Team Members, Penetration Testers, and Exploit Developers

WWW.SANS.ORG/FOR518
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

MAC FORENSIC ANALYSIS

SANS DFIR PRAGUE
Oct 3 – 15

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are only familiar with Windows machines.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course enable Windows investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyse any Mac or iOS system.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focusses on topics such as the HFS+ file system, Mac specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

YOU WILL BE ABLE TO...

- Analyse and parse the Hierarchical File System (HFS+) file system by hand and recognise the specific domains of the logical file system and Mac-specific file types
- Understand and profile users through their data files and preference configurations
- Determine how a system has been used or compromised by using the system and user data files in correlation with system log files
- Understand and analyse many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime

WHO SHOULD ATTEND?

- Experienced Digital Forensic Analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law Enforcement Officers, Federal Agents, or Detectives who want to master advanced computer forensics and expand their investigative skill set
- Media Exploitation Analysts who need to know where to find the critical data they need from a Mac system
- Incident Response Team Members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information Security Professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR408, FOR508, FOR526, FOR610, FOR585 Alumni looking to round out their forensic skills

"BEST MAC FORENSICS COURSE AVAILABLE."
David Klopp
J.P MORGAN

"THE DEPTH OF TIME EXERCISE WAS OUTSTANDING. ONE CAN TELL THE AMOUNT OF WORK THAT WENT INTO IT."
Gary Titus
STROZ FRIEDBERG LLC

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/FOR526
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

FOR 526

MEMORY FORENSICS IN-DEPTH

FOR526 TRAINING EVENT DATES

SANS DFIR PRAGUE
Oct 3 – 15

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviours implemented by malicious code. It is this evidence that often proves to be the indicator that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyse captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

"BIGGEST KNOWLEDGE JUMP I CAN ACHIEVE IN 5 DAYS."
Sheldon Johnson
SELEX-ES

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defence techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

"THIS TRAINING OPENED MY EYES FOR THE NEED TO COLLECT MEMORY IMAGES, AS WELL AS PHYSICAL IMAGES FOR SINGLE COMPUTER ANALYSIS, SUCH AS THEFT OF IP OR OTHER EMPLOYEE INVESTIGATIONS."
Greg Caouette
KROLL

YOU WILL LEARN...

- Proper memory acquisition: Demonstrate targeted memory capture to ensure data integrity and combat anti-acquisition techniques.
- How to find evil in memory: Detect rogue, hidden, and injected processes, kernellevel rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms.
- Effective Step-by-Step memory analysis techniques: Use process timelining, high-low-level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behaviour.
- Best practice techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques, as well as how to devise custom parsing scripts for targeted memory analysis.

WHO SHOULD ATTEND?

- Incident Response Team Members who regularly respond to complex security incidents/intrusions and would like to know how memory forensics will expand their reach.
- Experienced Digital Forensic Analysts who want to consolidate and expand their understanding of memory forensics
- Red Team Members, Penetration Testers, and Exploit Developers who want to learn how their opponents can identify their actions. Discover how common mistakes can compromise operations on remote systems, and how to avoid them. This course covers remote system forensics and data collection techniques that can be easily integrated into post-exploit operating procedures and exploit testing batteries
- Law Enforcement Officers, Federal Agents, or Detectives who want to become a deep subject-matter expert on memory forensics
- SANS FOR508 and SEC504 Graduates looking to take their memory forensics skills to the next level

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify an attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process
- Learn how attackers leverage man-in-the middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyse wireless network traffic to find evidence of malicious activity
- Use visualisation tools and techniques to distil complex data sources into management-friendly reports
- Learn how to modify configuration on typical network devices to increase the intelligence value of their logs and alerts during an investigation

WHO SHOULD ATTEND?

- Incident response team members
- Law Enforcement Officers, Agents and Detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- IT lawyers and paralegals
- Anyone interested in computer network intrusions and investigations

WWW.SANS.ORG/FOR572
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GNFA

FOR 572

ADVANCED NETWORK FORENSICS AND ANALYSIS

FOR572 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18
SANS DFIR PRAGUE
Oct 3 – 15
SANS LONDON
Nov 14– 19

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

When it comes to handling an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

FOR572 is built, from the ground up, to cover the most critical skills needed to mount efficient and effective post-incident response investigations. Classes focus on the knowledge necessary to expand the forensic mind-set from residual data on the storage media (system or device), to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations. Students leave with a well-stocked toolbox and the knowledge to use it on their first day back on the job.

"FANTASTIC COURSE, VERY WELL TAUGHT WITH GREAT LABS THAT REINFORCE THE TAUGHT MATERIAL."
A. Honey
NCA

Lessons cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

The hands-on exercises in this class cover a wide range of tools, including: The venerable tcpdump and Wireshark for packet capture and analysis, commercial tools from Splunk, NetworkMiner and SolarWinds. Open-source tools include: nfdump, tcpxtract, ELSA, and more. Through all of these exercises, shell scripting abilities come in handy, making easy work of ripping through thousands of data records.

"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

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/FOR578
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits

FOR 578

CYBER THREAT INTELLIGENCE

FOR578 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18
SANS DFIR PRAGUE
Oct 3 – 15

PRIVATE TRAINING*

COURSE DETAILS

Conventional network defences such as intrusion detection systems and antivirus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organisations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defence mechanisms. Adversaries can remain undetected during the intrusion, and then go unnoticed on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries - collectively known as cyber threat intelligence - gives network defenders information superiority. This can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks. They also need methods to exploit this information so they can improve their defensive posture. Threat intelligence represents a force multiplier for organisations looking to update their response and detection programs. It also enables them to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organisation needs a cutting-edge incident response, armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578: Cyber Threat Intelligence teaches defenders to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

"FANTASTIC CLASS! I LOVE THE WAY THE TERMINOLOGY WAS COVERED. I WILL BE MAKING INDEX CARDS TO ENSURE I HAVE THEM MEMORISED."
Nate DeWitt
EBAY

"I AM NEW TO CTI AND THIS COURSE WAS REALLY WELL PUT TOGETHER TO CATER FOR PEOPLE WITH DIFFERENT LEVELS OF EXPERTISE"
Ben Hargreaves
PWC

YOU WILL BE ABLE TO...

- Construct and exploit threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Fully analyse successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organisations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions

WHO SHOULD ATTEND?

- Incident Response Team Members who regularly respond to complex security incidents/intrusions from APT adversaries and need to know how to detect, investigate, remediate, and recover fro compromised systems across an enterprise
- Security Operations Centre Personnel and Information Security Practitioners who support hunting operations that seek to identify attackers in their network environments
- Experienced Digital Forensic Analysts who want to consolidate and expand their understanding of filesystem forensics, investigations of technically advanced adversaries, incident response tactics, and advanced intrusion investigations
- Federal Agents and Law Enforcement Officials who want to master advanced intrusion investigations and incident response, as well as expand their investigative skills beyond traditional host-based digital forensics.
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/FOR585
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits

FOR 585

ADVANCED SMARTPHONE FORENSICS

YOU WILL BE ABLE TO...

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyse mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes

WHO SHOULD ATTEND?

- Experienced digital forensic examiners who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and what files they accessed

FOR585 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 9 – 18
SANS DFIR PRAGUE
Oct 3 – 15

PRIVATE TRAINING*

ONDEMAND

"THE BEST PART ABOUT ADVANCED SMARTPHONE FORENSICS IS IT PROVIDES REAL WORLD TECHNOLOGIES FOR FORENSICALLY INVESTIGATING DEVICES WITHOUT THE TYPICAL POINT AND CLICK APPROACHES."
Brad Wardman
PAYPAL

COURSE DETAILS

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break a case. FOR585: Advanced Smartphone Forensics teaches these skills.

Smartphone forensics involves more than just pressing the "find evidence" button and getting answers. Rather, it's essential to understand how to use tools correctly to guide an investigation, instead of just letting the tool report what it believes happened on the device.

It is impossible for commercial tools to parse everything from smartphones and understand how the data was put on the device. This course provides students with the ability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensic course provides examiners and investigators with the skills needed to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs. These allow students to analyse different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hides and how it can be easily misinterpreted by forensic tools.

Each lab teaches a lesson that can be applied to other smartphones. Students gain experience with the different data formats on multiple platforms and learn how the data is stored and encoded on each type of smart device.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course arms students with mobile device forensic knowledge that can be applied immediately to cases.

FOR585: Advanced Smartphone Forensics helps students understand:

- Where key evidence is located on a smartphone
- How the data got onto the smartphone
- How to recover deleted mobile device data that most forensic tools miss
- How to decode evidence stored in third-party applications
- How to detect, decompile, and analyse mobile malware and spyware
- How to handle locked or encrypted devices, applications, and containers

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/FOR610
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GREM

FOR 610

REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

FOR610 TRAINING EVENT DATES

SANS STOCKHOLM
May 9 - 14
SANS DFIR PRAGUE
Oct 3 – 15

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Understanding the capabilities of malware is critical to an organisation's ability to derive threat intelligence, respond to information security incidents, and to fortify its defences. This course builds a strong foundation for reverse-engineering malicious software. It explores a variety of system and network monitoring utilities, disassemblers, debuggers, and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. Students learn how to set up an inexpensive and flexible laboratory. FOR610 then teaches how to examine malicious software's inner workings, and how to use the lab to dissect real-world malware samples. Students examine specimens' behavioural patterns and code. The course continues by discussing essential x86 assembly language concepts.

Students also examine malicious code to understand its key components and execution flow. In addition, the course explores how to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

With this covered, students learn to handle self-defending malware, bypassing the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, students explore practical approaches to analysing malicious browser scripts, deobfuscating JavaScript and VBScript to understand the nature of the attack.

FOR610 also teaches students to analyse malicious documents such as Microsoft Office and Adobe PDF files. These documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks.

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

YOU WILL BE ABLE TO...

- Build an isolated laboratory environment for analysing code and behaviour of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes on Microsoft Windows
- Uncover and analyse malicious JavaScript, VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- Control some aspect of the malicious program's behaviour through network traffic interception and code patching
- Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognise and understand common assembly-level patterns in malicious code, such as DLL injection
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files in the context of targeted attacks
- Derive Indicators of Compromise (IOCs) from malicious executables to contain and recover from the incident
- Utilise practical memory forensics techniques to examine capabilities of rootkits

WHO SHOULD ATTEND?

- Professionals with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration
- Professionals who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs
- Individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalise and expand their malware forensics expertise

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Understand the different types of controls (e.g. technical vs. non-technical) essential to performing a successful audit
- Conduct a proper network risk assessment to identify vulnerabilities and prioritise what will be audited
- Establish a well-secured baseline for computers and networks - a standard to conduct an audit against
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilise vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit web applications' configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilise scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

WHO SHOULD ATTEND?

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System & Network Administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit
- System & Network Administrators seeking to create strong change control management and detection systems for the enterprise

WWW.SANS.ORG/AUD507
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GSNA

AUD 507

AUDITING & MONITORING NETWORKS, PERIMETERS & SYSTEMS

AUD507 TRAINING EVENT DATES

SANS BRUSSELS AUTUMN
Sep 5 – 10

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

One of the most significant obstacles facing auditors is how to model the security of an enterprise. Which systems matter? How should the firewall and routers be configured? Which system settings should be checked? Is there a set of processes that can allow an auditor to focus on the business processes, rather than the security settings? How can this be turned into a continuous monitoring process? All of these questions - and more – are answered by AUD507.

This course provides a risk driven method for tackling the enormous task of designing an enterprise security validation programme. Initially, students cover a variety of high level audit issues and general audit best practice. Students then have the opportunity to dive deeply into determining the key controls necessary to provide assurance to an organisation.

Assisting management to understand the relationship between technical controls and the risks to a business is a common challenge for auditors. In this course, threats and vulnerabilities are explained based on validated information from real world situations.

The SANS Instructor takes time to explain how this can be used to raise managers' awareness. Students learn to communicate an understanding of why audit and these controls are important.

Students also learn to build an ongoing compliance monitoring system, and how to automatically validate defences through instrumentation and audit checklist automation.

"THE ENTIRE COURSE HAS BEEN AWESOME AND PREPARED ME TO PERFORM A COMPREHENSIVE AUDIT. IT ALSO PROVIDED ME EXCELLENT INFORMATION TO OPERATIONS TO IMPROVE NETWORK SECURITY POSTURE."
Srinath Kannan
ACCENTURE

Five of the six days provide students with continuous monitoring scripts and general checklists. These can be customised for specific audit situations.

Students also experience hands-on exercises with many of the tools discussed during the lecture sections. This ensures that, when students leave AUD507, they know how to verify the controls described in the class. This approach also ensures students know what to expect as audit evidence.

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/SEC566
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits | GIAC Cert: GCCC

SEC 566

IMPLEMENTING AND AUDITING THE CRITICAL SECURITY CONTROLS IN-DEPTH

SEC566 TRAINING EVENT DATES

SANS SECURE EUROPE
Apr 4 – 16
SANS LONDON SUMMER
Jul 9 – 18

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

Cyber security attacks increase and evolve so rapidly that it is more difficult than ever to prevent and defend against them. Does an organisation have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps students master specific, proven techniques and tools needed to implement and audit the Critical Security Controls - as documented by the Center for Internet Security (CIS).

As threats evolve, an organisation's security should too. To enable an organisation to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches how to implement the Critical Security Controls - a prioritised, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defences. They are designed to complement existing standards, frameworks, and compliance schemes by prioritising the most critical threat and highest payoff defences, while providing a common baseline for action against risks that we all face. The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The UK government's Centre for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

"I AM A NEW EMPLOYEE IN THIS FIELD. THIS COURSE GIVES ME REALLY GOOD KNOWLEDGE FOR MY WORK."
Wafa Al Raisi
CENTRAL BANK OF OMAN

YOU WILL BE ABLE TO...

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organisations' important information and systems
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of network and systems
- Identify and utilise tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how critical controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the critical security controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

WHO SHOULD ATTEND?

- Information Assurance Auditors
- System Implementers or Administrators
- Network Security Engineers
- IT Administrators
- Federal Agencies or clients
- Private sector

"PROVIDES GREATER STRUCTURE TO THE BASIC CONTROLS. GOOD METHODOLOGY PROVIDED IN IMPLEMENTING CONTROLS."
Jalal Moloo
DB SCHENKER

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Run Windows command line tools to analyse the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defence (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

WHO SHOULD ATTEND?

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

"EVERY IT SECURITY PROFESSIONAL AND OTHERS WITHIN SUPPORT AND PROJECTS AROUND ICS SHOULD TAKE THIS COURSE."

Simon Poole
SHELL

WWW.SANS.ORG/ICS410
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits | GIAC Cert: GISCP

ICS 410

ICS/SCADA SECURITY ESSENTIALS

ICS410 TRAINING EVENT DATES

SANS ICS AMSTERDAM
Apr 18 – 23
SANS ICS LONDON
Sep 19 – 25

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

SANS joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardised skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

When examining the greatest risks and needs in critical infrastructure sectors, the course authors look carefully at the core security principles necessary for the range of tasks involved in supporting control systems.

"VERY VALUABLE. I HAVE A MUCH GREATER UNDERSTANDING OF ICS SECURITY AND RISK."

D. Armour
OFFICE FOR NUCLEAR REGULATION

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defences do not always grasp systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When students leave the course, they have an appreciation, understanding, and common language that enables them to work together to secure industrial control system environments. The course helps develop cyber-secure-aware engineering practices and real-time control system IT /OT support carried out by professionals who understand the physical effects of actions in the cyber world.

"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 ENTERPRISES

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/ICS515
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits

ICS 515

ICS ACTIVE DEFENCE AND INCIDENT RESPONSE

ICS515 TRAINING EVENT DATES

SANS ICS AMSTERDAM
Apr 18 – 23
SANS ICS LONDON
Sep 19 – 25

PRIVATE TRAINING*

COURSE DETAILS

ICS515 empowers students with the ability to understand their networked industrial control system environment. Students learn to monitor their ICS infrastructure for threats, to perform incident response against identified threats, and to enhance network security through learning from interactions with the adversaries.

This process of monitoring, responding to, and learning from threats internal to the network is known as active defence. An active defence is needed to counter advanced adversaries targeting ICS – threats such as such as Stuxnet, Havex, and BlackEnergy2.

Students leave this course with the ability to deconstruct targeted ICS attacks and fight these adversaries. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS infrastructure. Students gain a practical and technical understanding of leveraging active defence concepts. These include using threat intelligence, performing network security monitoring, and utilising malware analysis and incident response to ensure the safety - and reliability - of operations.

You Will Learn:

- How to perform ICS incident response focusing on security operations and prioritising the safety and reliability of operations.
- How ICS threat intelligence is generated and how to use what is available in the community to support ICS environments.
- How to identify ICS assets and their network topologies, and how to monitor ICS hotspots for abnormalities and threats.
- How to analyse ICS malware and extract the most important information needed to quickly scope the environment and understand the nature of the threat.
- How to operate through an attack and gain the information necessary to instruct teams and decision-makers on when operations must shut down, or if it is safe to respond to the threat and continue operations.
- How to use multiple security disciplines in conjunction with each other to leverage an active defence and safeguard the ICS, all reinforced with hands-on labs and technical concepts.

"THIS COURSE IS THE MISSING PIECE TO GET COMPANIES TO TAKE THREATS SERIOUSLY, PURSUE THE TRUTH, AND SHARE THEIR FINDINGS."
Rob Cantu
DOE

YOU WILL BE ABLE TO...

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defence concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analysers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

WHO SHOULD ATTEND?

- ICS Incident Response Team Leads and Members
- ICS and Operations Technology Security Personnel
- IT Security Professionals
- Security Operations Center (SOC) Team Leads and Analysts
- ICS Red Team and Penetration Testers
- Active Defenders

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Identify the maturity level of existing awareness programmes and decide where to take it next
- Explain the difference between awareness, education and training
- Explain the three different variables of risk and how they apply to human risk and security awareness training
- Explain why people are vulnerable and how cyber attackers exploit these vulnerabilities
- Create a Project Charter and gain management support for a security awareness programme
- Identify the different targets of an awareness programme
- Characterise the culture of an organisation and determine the most effective communication methods for that culture
- Identify, measure and prioritise human risks
- Design and implement key metrics to measure the impact of an awareness programme
- Create an effective phishing assessment programme

WHO SHOULD ATTEND?

- Security Awareness Officers
- Chief Security Officers & Security Management Officials
- Security Auditors, Governance & Compliance Officers
- Human Resources and communications staff
- Representatives from organisations regulated by industries such as HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security awareness programme

"VALUABLE SKILLS LEARNT TO TAKE BACK AND APPLY IN MY SECURITY AWARENESS PROGRAMME."

Cornelius Thiart
CONTRARIUS INVESTMENT ADVISORY

WWW.SANS.ORG/MGT433
Hands On | Two Days | Laptop Required
12 CPE/CMU Credits

MGT 433

SECURING THE HUMAN:

HOW TO BUILD, MAINTAIN AND MEASURE A HIGH-IMPACT AWARENESS PROGRAMME

MGT433 TRAINING EVENT DATES

SANS LONDON SUMMER
Jul 7 – 8

PRIVATE TRAINING*

COURSE DETAILS

Organisations invest a tremendous amount of money and resources in securing technology, but little - if anything - into securing their employees and staff.

As a result, people, not technology, have become the weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness programme – a programme that changes behaviour as opposed to merely achieving compliance.

MGT433 is an intense two-day course. It teaches the key concepts and skills needed to build, maintain and measure a security awareness programme. All course content is based on lessons learned from hundreds of security awareness programmes from around the world.

"GOOD COURSE WHETHER YOU ARE DEVELOPING TRAINING AND AWARENESS OR IMPROVING YOUR CURRENT SYSTEM."

Tina Baker
AWE PLC

Students learn from their SANS Instructor and also through extensive interaction with their peers. As such, attendees should bring example material from their security awareness programme.

Finally, through a series of labs and exercises, students develop a custom security awareness plan that can be implement as soon as they return to their organisation.

"THE COURSE PROVIDES AN EXCELLENT FRAMEWORK WITHIN WHICH ANY TYPE OF ORGANISATION CAN DEVELOP A SECURITY AWARENESS PROGRAMME THAT FITS IN WITH NEEDS."

Mark James
UNIVERSITY OF BRISTOL

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/MGT512
Hands On | Five Days | Laptop Required
33 CPE/CMU Credits | GIAC Cert: GSLC

MGT 512

SECURITY LEADERSHIP ESSENTIALS FOR MANAGERS

WITH KNOWLEDGE COMPRESSION™

MGT512 TRAINING EVENT DATES

SANS LONDON AUTUMN
Sep 19 – 24

PRIVATE TRAINING*

ONDEMAND

COURSE DETAILS

MGT512 empowers advancing managers who need to get up to speed quickly on information security issues and terminology. Students don't just learn about security, they learn how to manage security.

Managers gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance. This means MGT512 is particularly useful to US Government managers and supporting contractors.

Essential security topics covered in this management track include: Network fundamentals and applications, power, cooling and safety, architectural approaches to defence in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum.

The material uses Knowledge Compression™ - special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand from every teaching hour of the course.

The course has been evaluated and approved by CompTIA's CAQC programme for Security + 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. Managers will be able to deploy what you learn into practice the day you get back into the office.

YOU WILL BE ABLE TO...

- Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in SANS Security Essentials, though not to the same depth. The goal is to enable managers and auditors to speak the same language as system, security, and network administrators.
- Establish a minimum standard for IT management knowledge, skills and abilities. I keep running into managers that do not know TCP/IP, and that is okay; but then they do not know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know.
- Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is okay to make mistakes, just make new ones.

WHO SHOULD ATTEND?

- All newly-appointed Information Security Officers
- Technically-skilled Administrators that have recently been given leadership responsibilities
- Seasoned Managers who need to understand technical processes, points and policies.

"THIS COURSE IS HIGHLY USEFUL FOR GIVING ME A SOUND BASELINE OF TECHNICAL AND GENERAL SKILLS TO HELP ME MANAGE AN EFFECTIVE TEAM"
Richard Ward
REA GROUP

"WAS ABLE TO MERGE MANAGEMENT SKILLS AND TECHNICAL MATERIALS IN ONE A SIMPLE FORMAT."
Abdulaziz Al-Sultan
SAUDI ELECTRIC COMPANY

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

YOU WILL BE ABLE TO...

- Understand the major risks and common vulnerabilities related to web applications through real-world examples
- Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- Fulfil the training requirement as stated in PCI DSS 6 5
- Deploy and consume web services (SOAP and REST) in a secure fashion
- Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- Strategically roll out a web application security program in a large environment
- Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
- Develop strategies to assess the security posture of multiple web applications

WHO SHOULD ATTEND?

- Application Developers
- Application Security Analysts or Managers
- Application Architects
- Penetration Testers who are interested in learning about defensive strategies
- Security Professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organisations who need to be trained to comply with PCI requirements

WWW.SANS.ORG/DEV522
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GWEB

DEV 522

DEFENDING WEB APPLICATIONS SECURITY ESSENTIALS

DEV522 TRAINING EVENT DATES

SANS STOCKHOLM
May 9 – 14
SANS LONDON
Nov 14 – 19

PRIVATE TRAINING*

ONDEMAND

"GIVES A GOOD LEVEL OF TRAINING FOR DEFENDING WEB APPS"
Kar Hopkinson -Turrell QA

"DEV522 REALLY COVERS THE SECURITY ASPECTS EVERY WEB DEVELOPER MUST KNOW"
Daniel Abrahamsson KLARNA AB

COURSE DETAILS

Defenders must learn to secure web applications because the importance of the data entrusted to these products is growing. Traditional network defences, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and helps defenders better understand web application vulnerabilities, thus enabling them to properly protect their organisation's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside proven, real-world applications. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.

To maximise the benefit for a wider range of audiences, the discussions in this course are programming language agnostic. Rather, the course focusses on security strategies as opposed to coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to: Application security analysts, developers, application architects and pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course also covers additional issues that authors find important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course makes heavy use of hands-on exercises and concludes with a large defensive exercise that reinforces the lessons learned throughout the week.

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

WWW.SANS.ORG/DEV541
Hands On | Four Days | Laptop Required
24 CPE/CMU Credits | GIAC Cert: GSSP-JAVA

DEV 541

SECURE CODING IN JAVA/JEE: DEVELOPING DEFENSIBLE APPLICATIONS

DEV541 TRAINING EVENT DATES

SANS OSLO
Oct 3 – 8

PRIVATE TRAINING*

ONDEMAND

"THIS COURSE TEACHES YOU PRACTICAL AND REAL LIFE APPLICABLE METHODS WITH MANY EXAMPLES IN THE LABS."
Purcaru Alexandru
SRI

COURSE DETAILS

DEV541 teaches students how to build secure Java applications. The course shares the skills and knowledge necessary to build sites that protect against intrusion. Students learn to counter a wide range of application attacks and remediate critical security vulnerabilities – vulnerabilities that can lead to data loss. Going further, DEV541 help students understand their attacker's mind-set.

The course teaches the art of modern web defence for Java applications by focussing on foundational defensive techniques, cutting-edge protection, and Java EE security features. These are also techniques and concepts that students can apply to their projects. This includes learning how to:

- Identify security defects in code
- Fix security bugs using secure coding techniques
- Utilise secure HTTP headers to prevent attacks
- Secure sensitive representational state transfer (REST) services
- Incorporate security into your development process
- Use freely available security tools to test applications

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a theory course - it is about real-world, hands-on programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources needed to improve the security of Java applications.

The course covers concepts of secure programming, rather than teaching students to use a given set of tools. This involves looking at a specific piece of code, identifying a security flaw and implementing a fix for flaws found on the OWASP Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors. The course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. Students conduct a code review, perform security testing to exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques learned in class.

"GREAT REAL WORLD EXAMPLES OF ATTACKS! GREAT COURSE MATERIAL AND QUALITY. GREAT STUDENT INTERACTION. THE BEST SECURE DEVELOPMENT COURSE I HAVE COME ACROSS. GREAT INSTRUCTOR WITH TOP TEACHING SKILLS. GREAT TIME MANAGEMENT."
Andreas Hegna
STOREBRAND LIVSFORSIKRING AS

YOU WILL BE ABLE TO...

- Use a web application proxy to view and manipulate HTTP requests and responses
- Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10

Mitigate common web application vulnerabilities using secure coding practices and Java libraries, including:

- Input validation
- Blacklist and whitelist validation
- Regular expressions
- Output encoding
- Content Security Policy
- Client-side security headers

Build applications using:

- Java Enterprise Edition authentication
- Basic and form-based authentication
- Client certificates
- Sockets Layer/Transport Layer Security (SSL/TLS)
- Java Secure Sockets Extension
- Secure password storage techniques
- Java Cryptography Architecture
- Security Manager

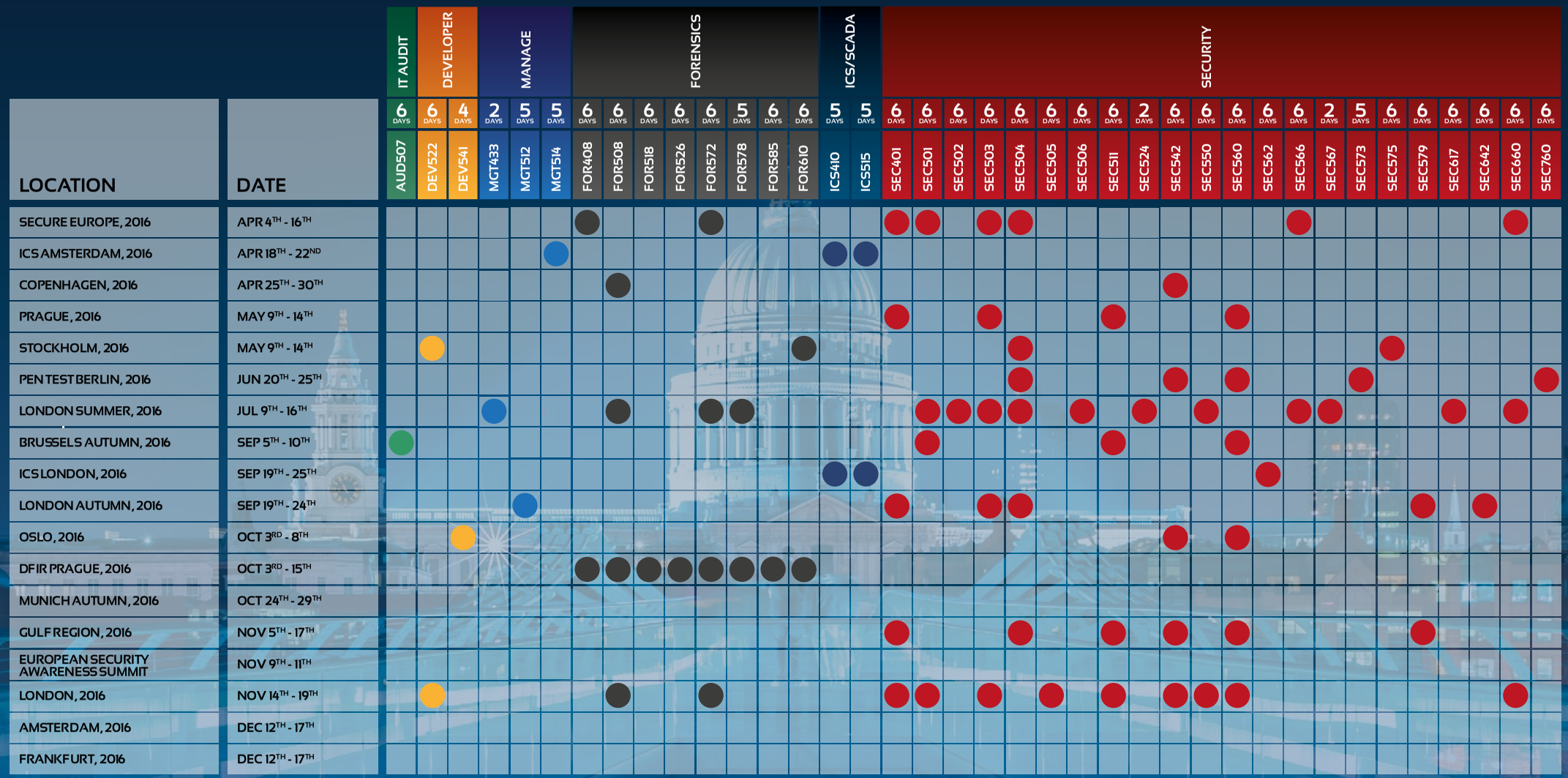
WHO SHOULD ATTEND?

- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) Programmers
- Software Engineers
- Software Architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application Security Auditors
- Technical Project Managers
- Senior Software QA Specialists
- Penetration Testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

Although we rarely amend the schedule, all dates/courses are subject to change.
See www.sans.org/emea for up to date schedule *(minimum attendee numbers apply)

FUTURE SANS EMEA TRAINING EVENTS 2016

For a full list of training events, please visit www.sans.org



Q2 A4

Most courses are also available online, via SANS OnDemand. Contact emea@sans.org for information.

Dates, locations and courses offered subject to change