★ THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING ★

SANS EMEA

# SANS SECURE EUROPE AMSTERDAM

MON 4 - SAT 16 APRIL, 2016 #SANSSECEUROPE

## 8 SANS COURSES

**SEC401**
Security Essentials Bootcamp Style

**SEC501**
Advanced Security Essentials Enterprise Defender

**SEC503**
Intrusion Detection In-Depth

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

**SEC566**
Implementing and Auditing the Critical Security Controls - In-Depth

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

**FOR408**
Windows Forensic Analysis

**FOR572**
Advanced Network Forensics and Analysis

Register online and see full course descriptions at **www.sans.org/event/secure-europe-2016**

**Save €450** with discount code "**EarlyBird16**" for a 4-6 day course by 17 Feb, 2016.

# COURSES AT A GLANCE

| | | MO 4 | TU 5 | WE 6 | TH 7 | FR 8 | SA 9 | SU 10 | MO 11 | TU 12 | WE 13 | TH 14 | FR 15 | SA 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SEC 401 | Security Essentials Bootcamp Style *Stephen Sims* | p8 | ● | ● | ● | ● | ● | | | | | | | |
| SEC 501 | Advanced Security Essentials Enterprise Defender *Paul A. Henry* | | | | | | | | p9 | ● | ● | ● | ● | ● |
| SEC 503 | Intrusion Detection In-Depth *Jess Garcia* | | | | | | | | p10 | ● | ● | ● | ● | ● |
| SEC 504 | Hacker Tools, Techniques, Exploits and Incident Handling *Dave Shackleford* | | | | | | | | p11 | ● | ● | ● | ● | ● |
| SEC 566 | Implementing and Auditing the Critical Security Controls - In-Depth *James Tarala* | p12 | ● | ● | ● | ● | | | | | | | | |
| SEC 660 | Advanced Penetration Testing, Exploit Writing, and Ethical Hacking *Stephen Sims* | | | | | | | | p13 | ● | ● | ● | ● | ● |
| FOR 408 | Windows Forensic Analysis *Rob Lee* | p14 | ● | ● | ● | ● | ● | | | | | | | |
| FOR 572 | Advanced Network Forensics and Analysis *Philip Hagen* | p15 | ● | ● | ● | ● | ● | | | | | | | |



# ABOUT SANS

**SANS IS THE MOST TRUSTED AND BY FAR THE LARGEST SOURCE FOR INFORMATION SECURITY TRAINING AND SECURITY CERTIFICATION IN THE WORLD.**

The SANS Institute was established in 1989 as a cooperative research and education organisation. Our training programs now reach more than 200,000 security professionals around the world.

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited.

SANS courses are full of important and immediately useful techniques that you can put to work as soon as you return to the office. They were developed through a consensus process involving hundreds of administrators, security managers and information security professionals. Courses address security fundamentals and awareness as well as the in-depth technical aspects of the most crucial areas of IT security.

SANS-certified instructors are recognised as the best in the world. To find the best teachers for each topic, SANS runs a continuous competition for instructors. Last year more than 100 people tried out for the SANS faculty, but only five new potential instructors were selected.

SANS provides training through several delivery methods, both live & virtual: classroom-style at a training event, online at your own pace, guided study with a local mentor, or onsite at your workplace. SANS courses are taught in English by our world class SANS instructors, or in French or Spanish if you attend one of our excellent partner training events in France or Spain.

In addition to top-notch training, SANS offers certification through the GIAC security certification program and numerous free security resources such as newsletters, whitepapers, and webcasts.

Why SANS is the best training and educational investment:

- Intensive, hands-on immersion training with the highest-quality courseware in the industry.
- Incomparable instructors and authors who are industry experts and practitioners fighting the same cyber battles as you and discovering new ways to thwart attacks.
- Training that strengthens a student's ability to achieve a GIAC certification, which is unique in the field of information security certifications because it not only tests a candidate's knowledge, but also the candidate's ability to put that knowledge into practice in the real world. ●

**Contact SANS**
**www.sans.org/emea**
**Email:** emea@sans.org
**Tel:** +44 20 3384 3470

**Address:**
SANS EMEA,
PO Box 124, Swansea,
SA3 9BB, UK

## CONTENTS



# WELCOME TO SANS SECURE EUROPE 2016

**EVENT LOCATION**
**Radisson Blu Hotel**
Rusland 17
NL-1012 CK
Amsterdam, NL

**Telephone**
+31 20 623 1231
**Website**
www.radissonblu.com

**CONTACT SANS**
**Email:** emea@sans.org
**Tel:** +44 20 3384 3470

**SANS SECURE EUROPE 2016 RUNS FROM MONDAY 4TH APRIL TO APRIL 16TH AT THE RADISSON BLU HOTEL AND HOSTS 8 COURSES DRAWN FROM ACROSS THE SANS CURRICULUM. FOUR COURSES RUN IN WEEK ONE AND ANOTHER FOUR IN WEEK 2.**

Registration fees include all courseware and training materials plus morning and afternoon break refreshments and lunch served in the hotel restaurant. Accommodation is not included.

Training runs from 9am-5pm except for course SEC401 that finishes at 7pm Monday - Friday and 5pm on Saturday and SEC504 finishes at 7:15pm on Monday. SEC660 runs from 9am - 5pm and then restarts 5:15pm - 7pm Monday-Friday and finishes at 5pm Saturday.

Students are able to attend free SANS@Night talks and evening social functions. The demand for places at Secure Europe is always high so please register online as soon as possible to secure a seat at SANS Secure Europe 2016.

Read on for course descriptions or visit www.sans.org/event/secure-europe-2016. Over the page you will find the SANS Career Roadmap which provides examples of how SANS courses fit into your career development plan. ●



# REGISTER ONLINE AT:

## WWW.SANS.ORG/SECURE-EUROPE-2016


## REGISTER EARLY AND SAVE:

Register #SANSSecureEurope and pay before the 17th Feb and save €450 by entering the code EarlyBird16

## GROUP SAVINGS

(APPLIES TO TUITION ONLY)
5-9 people = 5%
10 or more people = 10%

Early bird rates and/or other discounts cannot be combined with the group discount. To obtain a group discount please email emea@sans.org.

## TO REGISTER

To register, go to www.sans.org/secure-europe-2016 Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course: If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with internet access must complete the online registration form. We do not take registrations by phone.

## CONFIRMATION

Look for e-mail confirmation. It will arrive soon after you register. We recommend you register and pay early to ensure you get your first choice of courses.

An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at +1 301-654-7267 9:00am - 8:00pm Eastern Time or email emea@sans.org.

## CANCELLATION

You may subsitute another person in your place at any time by sending an e-mail request to emea@sans.org. Cancellation requests by 9 Mar 2016 by emailing emea@sans.org

**REGISTER NOW** www.sans.org/secure-europe-2016

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: 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

**SAMPLE JOB TITLES:**
Intrusion Detection Analyst, Security Operations Centre Analyst / Engineer, CERT Member, Cyber Threat Analyst

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

**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: 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**
- **FOR578** Cyber Threat Intelligence

**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**

**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: 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**
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ **GSLC**
- **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep **GCPM**
- **MGT414** SANS Training Programme for CISSP® Certification **GISP**

**Core**
- **MGT514** IT Security Strategic Planning, Policy & Leadership
- **MGT535** Incident Response Team Management
- **LEG523** Law of Data Security and Investigations **GLEG**

**Specialisation**
- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Programme
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

## 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.

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

- **ICS410** ICS/SCADA Security Essentials **GICSP**
- **ICS515** ICS Active Response and Defense & Response

SEC 401

WWW.SANS.ORG/SEC401

# SECURITY ESSENTIALS BOOTCAMP STYLE

**STEPHEN SIMS**
GSEC Certification 46 CPEs
Monday - Friday: 9am - 7pm, Saturday: 9am-5pm

## YOU WILL BE ABLE TO...

- Develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand
- Analyse and assess the risk to your environment in order to drive the creation of a security roadmap that focuses on the right areas of security
- Learn practical tips and tricks to focus in on high-priority security problems within your organisation and on doing the right things that will lead to security solutions that work
- Learn why some organisations are winning and some are losing when it comes to security and, most importantly, how to be on the winning side
- Learn the core areas of security and how to create a security program that is anchored on PREVENT-DETECT-RESPOND

## COURSE DETAILS

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organisation's critical information assets and business systems.

"Prevention is Ideal but Detection is a Must."

With the advanced persistent threat, 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 on going challenge, with new threats emerging all of the time, including the next generation of threats. Organisations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defence. Before your organisation spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, 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 you focus on the right areas of defence. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organisations.

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*





WWW.SANS.ORG/SEC501

# ADVANCED SECURITY ESSENTIALS ENTERPRISE DEFENDER

SEC 501

**PAUL A. HENRY**
GCED Certification 36 CPEs
Monday - Saturday: 9am - 5pm

## COURSE DETAILS

SEC501: Advanced Security Essentials - Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

Detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in robust network architecture, or on a portable device.

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

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

## 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

**"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*

SEC 503

WWW.SANS.ORG/SEC503

# INTRUSION DETECTION IN-DEPTH

**JESS GARCIA**
GCIA Certification 36 CPEs
Monday - Saturday 9am - 5pm

## 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

## 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.

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.

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


WWW.SANS.ORG/SEC504

# HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

SEC 504

**DAVE SHACKLEFORD**
GCIH Certification 37 CPEs
Monday 9am - 7:15pm, Tuesday - Saturday 9am - 5pm

## 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.

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

## 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

SEC 566

WWW.SANS.ORG/SEC566

# IMPLEMENTING AND AUDITING THE CRITICAL SECURITY CONTROLS - IN-DEPTH

**JAMES TARALA**
GCCC Certification 30 CPEs
Monday - Friday 9am - 5pm

## 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

## 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.

**"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*





WWW.SANS.ORG/SEC660

SEC 660

# ADVANCED PENETRATION TESTING, EXPLOIT WRITING, AND ETHICAL HACKING

**STEPHEN SIMS**
GXPN Certification 46 CPES
Monday - Friday 9am-5pm, Saturday 5:15pm - 7pm.

## COURSE DETAILS

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking is designed as a logical progression point for those who have completed SANS SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through 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 hands-on lab to consolidate advanced concepts and facilitate the immediate application of techniques in the workplace. Each day of the course includes a two-hour evening boot camp to drive home additional mastery of the techniques discussed. A sample of topics covered includes weaponising Python for penetration testers, attacks against network access control (NAC) and virtual local area network (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 address space layout randomisation (ASLR) and data execution prevention (DEP), return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. To keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. This course provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and furnishes an environment to perform these attacks in numerous hands-on scenarios. The course goes far beyond simple scanning for low-hanging fruit and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

**"FROM HIGH-LEVEL CONCEPTS TO HANDS ON TRAINING THIS COURSE PROVIDES ENOUGH DETAILS AND DEPTH TO ALLOW ME TO SHOW MY EMPLOYER THEIR RETURN ON INVESTMENT."**
*Ewe Konkolska*
*PRUDENTIAL*

## 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

FOR 408

WWW.SANS.ORG/FOR408

# WINDOWS FORENSIC ANALYSIS

**ROB LEE**
GCFE Certification 36 CPEs
Monday - Saturday 9am - 5pm

## YOU WILL BE ABLE TO...

- 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
- 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
- Focus capabilities on analysis instead of how to use a specific tool
- 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
- Perform proper Windows forensic analysis by applying core techniques focusing on Windows 7/8/8.1

## 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.


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

WWW.SANS.ORG/FOR572

# ADVANCED NETWORK FORENSICS AND ANALYSIS

FOR 572

**PHILLIP HAGEN**
GNFA Certification 36 CPEs
Monday - Saturday 9am - 5pm

## 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.

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.

## 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


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

# SANS SECURE EUROPE 2016 INSTRUCTORS

**WE HAVE AN OUTSTANDING LINE UP OF EUROPEAN AND US-BASED INSTRUCTORS AT SANS SECURE EUROPE 2016. READ ON FOR PROFILES OF THIS ELITE GROUP.**

## 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, and is a VMware vExpert with extensive experience designing and configuring secure virtualised infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Centre for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualisation Security:

Protecting Virtualized Environments, as well as the co-author of Hands-On Information Security from Course Technology. Recently Dave co-authored the first published course on virtualisation security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. ●

## James Tarala

SENIOR INSTRUCTOR

*@isaudit*

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies.

He has also spent a large amount of time consulting with organisations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. ●

## Jess Garcia

PRINCIPAL INSTRUCTOR

*@j3ssgarcia*

Jess Garcia is the founder and technical lead of One eSecurity, a global Information Security company specialised in Incident Response and Digital Forensics.

With near 20 years in the field, and an active researcher in the area of innovation for Digital Forensics, Incident Response and Malware Analysis, Jess is today an internationally recognised Digital Forensics and Cybersecurity expert, having led the response and forensic investigation of some of the world's biggest incidents in recent times.

In his career Jess has worked in a myriad of highly sensitive projects with top global customers in sectors such as financial & insurance, corporate, media, health, communications, law firms or government, in other Cybersecurity areas as well such as Security Architecture Design and Review, Penetration Tests, Vulnerability Assessments, etc.

A Principal SANS Instructor with almost 15 years of SANS instructing experience, Jess is also a regular invited speaker at Security and DFIR conferences. ●

## Paul A. Henry

SENIOR INSTRUCTOR

*@phenrycissp*

Paul Henry is a Senior Instructor with the SANS Institute and one of the world's foremost global information security and computer forensic experts with more than 30 years of experience covering all 10 domains of network security. Paul began his career in critical infrastructure / process control supporting power generation and currently manages security initiatives and incident response for Global 2000 enterprises and government organisations worldwide.

Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security and as a retained security expert for multiple financial and healthcare firms.

Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defence's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. ●

## Philip Hagen
CERTIFIED INSTRUCTOR
*@PhilHagen*

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities.

Currently, Phil works at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats

Phil served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil shifted to a government contractor, providing technical services for various IT and information security projects. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is also a certified instructor for the SANS Institute, and is the course lead and co-author of FOR572, Advanced Network Forensics and Analysis. ●

## Rob Lee
FELLOW
*@RobTLee*

Rob Lee is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response.

Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies in the law enforcement, U.S. Department of Defence, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a computer forensic and security software development team. ●

## Stephen Sims
SENIOR INSTRUCTOR
*@Steph3nSim*

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.

Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking.

He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. ●



# EVENT LOCATION & TRAVEL INFORMATION

### SANS SECURE EUROPE TAKES PLACE AT THE RADISSON BLU HOTEL, AMSTERDAM.

Students can take advantage of Amsterdam's public transport with metro and tram stops near the hotel. The city's famous canal boats and bicycles provide a picturesque to explore the city. With the hotel's convenient downtown location, it's easy to access the city's museums, shopping venues and theatres.

### PUBLIC TRANSPORT IN AMSTERDAM

Tram stop Spui - 400 m
Metro stop Nieuwmarkt - 500 m
Central Railway Station - 1.2 km
Amsterdam Schiphol Airport - 20 km

### PARKING

Attendees can make a reservation for the hotel's private parking garage. The charge is EUR 55 per day. Parking is also available at the Stopera Amsterdam Music Theater, in the garage at Bijenkorf or in the guarded car park at the Rokin.

### DRIVING DIRECTIONS TO HOTEL FROM AIRPORT

**By car on ring Amsterdam A10 from exit S112 Diemen:**
Take exit S112 and follow the signs toward Centrum. Take the roundabout at the Amstel train station toward Centrum. This is Wibautstraat, which leads to Weesperstraat. At the end of Weesperstraat, take the roundabout toward Centrum (4th street on the right). Pass the Stopera Amsterdam Music Theater and pass the bridge; then take the 1st street on the right, Amstel. Cross the 1st bridge on the right, Kloveniersburgwal. Cross the 2nd bridge on the left, and continue straight on Rusland to the hotel.

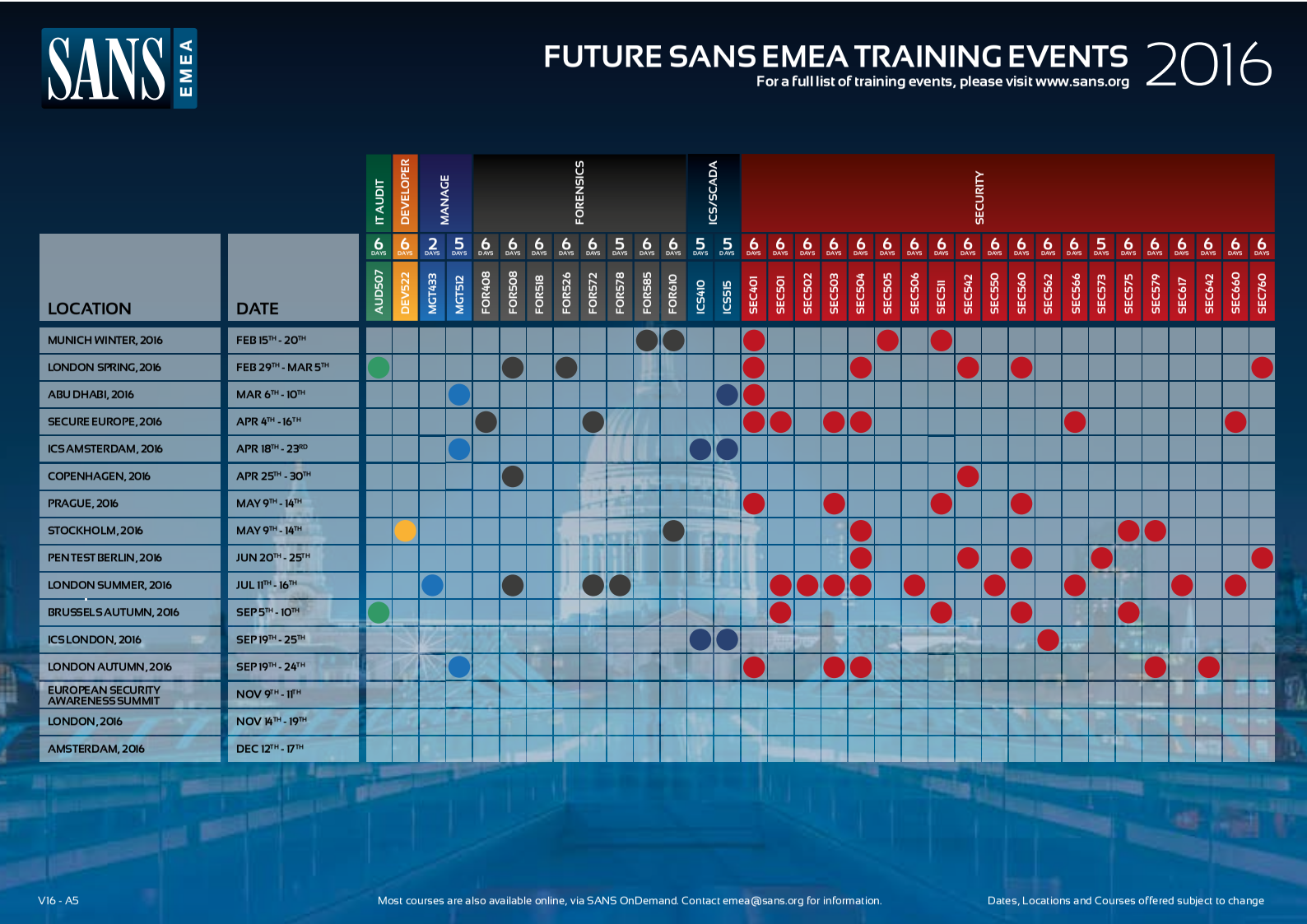
**By car on ring Amsterdam A10 from exit S116 Noord:**
Take exit S116 Noord, Centrum. Drive approximately 2.5 kilometers toward Centrum. Drive through the IJ Tunnel, continuing toward Centrum. At the 2nd traffic light, take the roundabout toward Centrum, the 2nd street on the right. Pass the Stopera Amsterdam Music Theater and pass the bridge, then take the 1st street on the right, Amstel. Cross the 1st bridge on the right, Kloveniersburgwal. Cross the 2nd bridge on the left, and continue straight on Rusland to the hotel.

### EVENT LOCATION

**Radisson Blu Hotel**
Rusland 17
NL-1012 CK
Amsterdam, NL
**Telephone**
+31 20 623 1231
**Website**
www.radissonblu.com

# FUTURE SANS EMEA TRAINING EVENTS 2016

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



| LOCATION | DATE | IT AUDIT | DEVELOPER | MANAGE | | FORENSICS | | | | | | | | ICS/SCADA | | SECURITY | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 6 DAYS | 6 DAYS | 2 DAYS | 5 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 5 DAYS | 6 DAYS | 6 DAYS | 5 DAYS | 5 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 5 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS | 6 DAYS |
| | | AUD507 | DEV522 | MGT433 | MGT512 | FOR408 | FOR508 | FOR518 | FOR526 | FOR572 | FOR578 | FOR585 | FOR610 | ICS410 | ICS515 | SEC401 | SEC501 | SEC502 | SEC503 | SEC504 | SEC505 | SEC506 | SEC511 | SEC542 | SEC550 | SEC560 | SEC562 | SEC566 | SEC573 | SEC575 | SEC579 | SEC617 | SEC642 | SEC660 | SEC760 |
| MUNICH WINTER, 2016 | FEB 15TH - 20TH | | | | | | | | | | | ● | ● | | | ● | | | | | ● | | ● | | | | | | | | | | | |
| LONDON SPRING, 2016 | FEB 29TH - MAR 5TH | ● | | | | | ● | | ● | | | | | | | ● | | | | ● | | | | ● | | ● | | | | | | | | ● |
| ABU DHABI, 2016 | MAR 6TH - 10TH | | | | ● | | | | | | | | | | ● | ● | | | | | | | | | | | | | | | | | |
| SECURE EUROPE, 2016 | APR 4TH - 16TH | | | | | ● | | | | ● | | | | | | ● | ● | | ● | ● | | | | | | | | ● | | | | | ● | |
| ICS AMSTERDAM, 2016 | APR 18TH - 23RD | | | | ● | | | | | | | | | ● | ● | | | | | | | | | | | | | | | | | | |
| COPENHAGEN, 2016 | APR 25TH - 30TH | | | | | | ● | | | | | | | | | | | | | | | | | ● | | | | | | | | | | |
| PRAGUE, 2016 | MAY 9TH - 14TH | | | | | | | | | | | | | | | ● | | | ● | | | | ● | | | ● | | | | | | | | |
| STOCKHOLM, 2016 | MAY 9TH - 14TH | | ● | | | | | | | | | | ● | | | | | | | ● | | | | | | | | | | ● | ● | | | |
| PEN TEST BERLIN, 2016 | JUN 20TH - 25TH | | | | | | | | | | | | | | | | | | | ● | | | | ● | | ● | | | ● | | | | | ● |
| LONDON SUMMER, 2016 | JUL 11TH - 16TH | | | ● | | | ● | | | ● | ● | | | | | | ● | ● | ● | ● | | ● | | | ● | | | ● | | | | ● | ● | |
| BRUSSELS AUTUMN, 2016 | SEP 5TH - 10TH | ● | | | | | | | | | | | | | | | ● | | | | | | ● | | | ● | | | | ● | | | | |
| ICS LONDON, 2016 | SEP 19TH - 25TH | | | | | | | | | | | | | ● | ● | | | | | | | | | | | | ● | | | | | | | |
| LONDON AUTUMN, 2016 | SEP 19TH - 24TH | | | | ● | | | | | | | | | | | ● | | | ● | ● | | | | | | | | | | ● | | ● | | |
| EUROPEAN SECURITY AWARENESS SUMMIT | NOV 9TH - 11TH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LONDON, 2016 | NOV 14TH - 19TH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AMSTERDAM, 2016 | DEC 12TH - 17TH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



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

Dates, Locations and Courses offered subject to change