

5 SANS COURSES

SEC401

Security Essentials
Bootcamp Style

SEC504

Hacker Tools,
Techniques, Exploits
and Incident Handling

SEC542

Web App Penetration
Testing and Ethical
Hacking

FOR408

Windows Forensic
Analysis

FOR572

Advanced Network
Forensics and Analysis

SANS

EMEA

MON 18 - SAT 23 JANUARY, 2016

SANS BRUSSELS

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

#SANSBRUSSELS

Immersive Training ★ World Class Instructors ★ GIAC Certification ★ SANS@Night evening talks and networking ★ Social Functions

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

Early bird **save €450 Euros** "EarlyBird16" for a 4-6 day course by 2 Dec, 2015

 HM Government
SANS is a Cyber Security Supplier to Government



COURSES AT A GLANCE

		MONDAY 18	TUESDAY 19	WEDNESDAY 20	THURSDAY 21	FRIDAY 22	SATURDAY 23
SEC 401	Security Essentials Bootcamp Style Dr. Eric Cole	PG 8					
SEC 504	Hacker Tools, Techniques, Exploits and Incident Handling Steve Armstrong	PG 9					
SEC 542	Web App Penetration Testing and Ethical Hacking Raul Siles	PG 10					
FOR 408	Windows Forensic Analysis Jess Garcia	PG 11					
FOR 572	Advanced Network Forensics and Analysis George Bakos	PG 12					

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 programmes 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 1000 people tried out for the SANS faculty, but only a handful of potential instructors were selected.

SANS provides training through several delivery methods, both live and virtual: classroom-style at a training event, online at your own pace, guided study with a local mentor, or private training 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 certification programme and numerous free security resources such as newsletters, whitepapers, and webcasts.

CONTENTS

COURSES AT A GLANCE	2
ABOUT SANS	3
TRAINING & YOUR CAREER ROADMAP	4
WELCOME TO SANS BRUSSELS 2016	6
REGISTRATION INFORMATION	7
COURSE CONTENT SUMMARIES	8
SANS BRUSSELS 2016 INSTRUCTORS	13
LOCATION & TRAVEL	15
SANS EMEA 2015/16 TRAINING EVENTS	16

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

 **Register now** www.sans.org/event/belgium-2016

 **@SANSEMEA #SANSBrussels**





FUNCTION: INFORMATION SECURITY

Information security professionals are responsible for research and analysis of security threats that may affect 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

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.

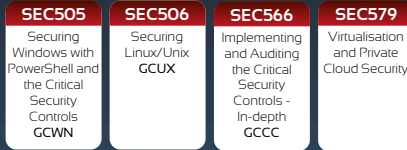
The NOC analysts work hand-in-hand with the Security Operations Centre, which safeguards the enterprise and continuously monitors threats against it.

SAMPLE JOB TITLES:

Security Analyst/ Engineer, SOC Analyst, Cyber Threat Analyst, CERT Member, Malware Analyst

CORE COURSES

SEC301, SEC401, SEC501
GISF, GSEC, GCED



FUNCTION: INCIDENT RESPONSE

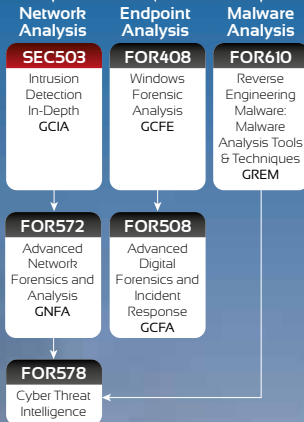
When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responder not only has to be technically astute, he/she must be able to handle stress under fire while navigating people, processes, and technology to help respond and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

SAMPLE JOB TITLES:

Security analyst/engineer, SOC analyst, Cyber threat analyst, CERT member, Malware analyst

CORE COURSES

SEC301, SEC401
GISF, GSEC



Specialisations



FUNCTION: PENETRATION TESTING/ VULNERABILITY ASSESSMENT

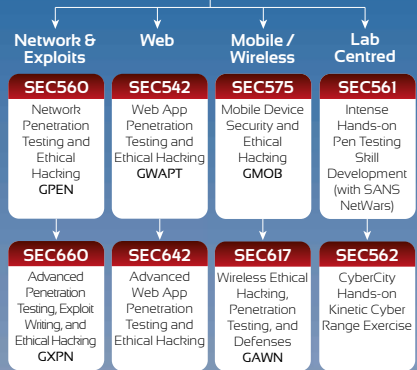
Because offense must inform defense, these experts provide enormous value to an organisation by applying attack techniques to find security vulnerabilities, analyse their business risk implications, and recommend mitigations before they are exploited by real-world attackers.

SAMPLE JOB TITLES:

Penetration tester, Vulnerability assessor, Ethical hacker, Red/Blue team member, Cyberspace engineer

CORE COURSES

SEC301, SEC401
GISF, GSEC



Specialisations



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 CCED

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 Countermeasures, & Cyber Deception

Threat Intelligence

FOR578

Cyber Threat Intelligence

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

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

FUNCTION: CYBER OR IT SECURITY MANAGEMENT

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
GCMP

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 agencies 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

SAMPLE JOB TITLES:

IT & OT Support, IT & OT Cyber Security, ICS Engineer

ICS515

ICS Active Response and Defense & Response

Specialisations

SEC542

Web App Penetration Testing & Ethical Hacking
GWAPT

SEC642

Advanced Web App Penetration Testing & Ethical Hacking





WELCOME TO SANS BRUSSELS 2016

SANS Brussels runs from Monday 18th to Saturday 23rd January at the Radisson Blu Royal Hotel in Brussels and hosts 5 courses drawn from across the SANS curriculum.

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 each day except for course SEC401 which finishes at 7pm Monday-Friday and 5pm on Saturday and course SEC504 which finishes at 7.15pm Monday.

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

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

EVENT LOCATION:

Hotel:

Radisson Blu Royal Hotel
Rue du Fosse-aux-Loups 47, Brussels,
B-1000 BE

Telephone: +32 2 2192828

E-mail: info.brussels@radissonblu.com

Website: www.radissonblu.com

 **Register now** www.sans.org/event/belgium-2016

 **@SANSEMEA #SANSBrussels**

SANS BRUSSELS 2016

REGISTRATION INFORMATION

REGISTER ONLINE AT: WWW.SANS.ORG/EVENT/BELGIUM-2016



REGISTER EARLY AND SAVE

Register for #SANSBRUSSELS and pay before the 2nd of December and save €450 by entering the code EarlyBird16

All course prices are listed at sans.org/event/belgium-2016

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/event/belgium-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 substitute another person in your place at any time by sending an e-mail request to emea@sans.org.

Cancellation requests by Dec 23rd, 2015, by emailing emea@sans.org



SECURITY ESSENTIALS BOOTCAMP STYLE

Instructor: Dr. Eric Cole

Six-Day Programme: Mon 18th – Sat 23rd January 9:00am - 7:00pm
36 CPE/CMU Credits | GIAC Cert: GSEC
Laptop Required

You will learn...

- To develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand
- To 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
- 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
- Why some organisations are winning and some are losing when it comes to security and, most importantly, how to be on the winning side
- 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.



Register now www.sans.org/event/belgium-2016



@SANSEMEA #SANSBrussels

"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."



HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

Instructor: Steve Armstrong

Six-Day Programme: Mon 18th – Sat 23rd January 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GCIH
Laptop Required

Course details

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organisation has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. 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.

You will learn...

- How best to prepare for an eventual breach
- The step-by-step approach used by many computer attackers
- Proactive and reactive defences for each stage of a computer attack
- How to identify active attacks and compromises
- The latest computer attack vectors and how you can stop them
- How to properly contain attacks
- How to ensure that attackers do not return
- How to recover from computer attacks and restore systems for business
- How to understand and use hacking tools and techniques
- Strategies and tools for detecting each type of attack
- Attacks and defences for Windows, Unix, switches, routers, and other systems
- Application-level vulnerabilities, attacks, and defences
- How to develop an incident handling process and prepare a team for battle
- Legal issues in incident handling

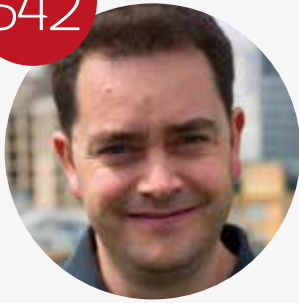


Register now www.sans.org/event/belgium-2016



@SANSEMEA #SANSBrussels

"Allows me to improve and understand the technical side in more detail, learning about attacks before, when and after they happen"



WEB APP PENETRATION TESTING AND ETHICAL HACKING

Instructor: Raul Siles

Six-Day Programme: Mon 18th – Sat 23rd January 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GWAPT
Laptop Required

You will learn...

- To apply a repeatable methodology to deliver high-value penetration tests.
- How to discover and exploit key web application flaws.
- How to explain the potential impact of web application vulnerabilities.
- The importance of web application security to an overall security posture.
- How to wield key web application attack tools more efficiently.

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, so 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.

Modern cyber defence requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper. SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the impact of inadequate security that plagues most organisations.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organisations. Even technically gifted security geeks often struggle with helping organisations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organisation to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organisations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.



Register now www.sans.org/event/belgium-2016



@SANSEMEA #SANSBrussels

“Fun while you learn! Just don’t tell your manager. Every class gives you invaluable information from realworld testing you cannot find in a book.”

WINDOWS FORENSIC ANALYSIS



Instructor: Jess Garcia

Six-Day Programme: Mon 18th – Sat 23rd January 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GCFE
Laptop Required

Course details

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artefacts is a core component of information security. Learn to recover, analyse, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organise findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you 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. Nothing is left out - attendees learn to analyse everything from legacy Windows XP systems to just discovered Windows 8.1 artefacts.

FOR408 is continually updated: This course utilises a brand-new intellectual property theft and corporate espionage case that took over 6 months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artefacts and technologies an investigator can encounter while analysing Windows systems. The incredibly detailed workbook details the tools and techniques step-by-step that each investigator should follow to solve a forensic case.

You will learn...

- 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
- To identify artifact 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
- To focus your capabilities on analysis instead of how to use a specific tool
- To 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



Register now www.sans.org/event/belgium-2016



@SANSEMEA #SANSBrussels

*"Hands down the BEST forensics class EVER!!
Blew my mind at least once a day for 6 days!"*

JASON JONES, USAF

ADVANCED NETWORK FORENSICS AND ANALYSIS

Instructor: George Bakos

Six-Day Programme: Mon 18th – Sat 23rd January 9:00am - 5:00pm

36 CPE/CMU Credits | GIAC Cert: GNFA

Laptop Required



FOR
572

You will learn...


- 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 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
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation

Course details

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mind-set from residual data on the storage media from a 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. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking - we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will 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.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS Forensic alumni from 408 and 508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same calibre of real-world problems without any convenient hard drive or memory images.

 Register now www.sans.org/event/belgium-2016

 @SANSEMEA #SANSBrussels

"The SANS Institute is currently the leader in the commercial IR and Computer Forensic training market. They have a large number of quality courses."

SANS BRUSSELS 2016 INSTRUCTORS

SANS instructors are considered the best in the world. Not only do they meet SANS' stringent requirements for excellence, they are also all real-world practitioners. The instructors ensure that what you learn in class will be up to date and relevant to your job.

We have an outstanding line up of European and US-based instructors at SANS Brussels 2016. Read on for profiles of this elite group.

STEVE ARMSTRONG



Certified Instructor

Steve began working in the security arena in 1994 whilst serving in the UK Royal Air Force. He specialised in the technical aspects of IT security from 1997 onward, and before retiring from active duty, he led the RAF's penetration and TEMPEST testing teams. He founded Logically Secure in 2006 to provide specialist security advice to government departments, defence contractors, the online video gaming industry, and both music and film labels worldwide. When not teaching for SANS, Steve provides penetration testing and incident response services for some of the biggest household names in gaming and music media.

GEORGE BAKOS



Certified Instructor

George Bakos has been interested in computer security since the early 1980s when he discovered the joys of BBSs and corporate databases. These days he is Technical Fellow & Manager of Cyber Threat Assessment & Awareness at Northrop Grumman, a global leader in Cybersecurity, Aerospace & Defence. While at the Institute for Security Technology Studies, George was the developer of Tiny HoneyPot and the IDABench intrusion analysis system and led the Dartmouth Distributed HoneyNet System, fielding deception systems and studying the actions of attackers worldwide. He developed and taught the U.S. Army National Guard's CERT technical curriculum and ran the NGB's Information Operations Training and Development Center research lab for two years, fielding and supporting Computer Emergency Response Teams throughout the United States. A recognised authority in computer security, he has contributed to numerous books and open source software projects; has been interviewed on radio, television, and online publications; briefed the highest levels of government; and has been a member of the SANS Institute teaching faculty since 2001.

DR. ERIC COLE



Fellow

Dr. Cole is an industry-recognised security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defence. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible 2nd Edition, and Insider Threat. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole was the lone inductee into the InfoSec European Hall of Fame in 2014. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty Fellow and course author who works with students, teaches, and develops and maintains courseware.

RAUL SILES



Certified Instructor

Raul Siles is founder and senior security analyst at DinoSec. For over a decade, he has applied his expertise performing advanced technical security services and innovating offensive and defensive solutions for large enterprises and organisations in various industries worldwide. He has been involved in security architecture design and reviews, penetration tests, incident handling, intrusion and forensic analysis, security assessments and vulnerability disclosure, web applications, mobile and wireless environments, and security research in new technologies. Throughout his career, starting with a strong technical background in networks, systems and applications in mission critical environments, he has worked as an information security expert, engineer, researcher and penetration tester at Hewlett Packard, as an independent consultant, and on his own companies, Taddong and DinoSec.

Raul is a certified instructor for the SANS Institute, regularly teaching penetration testing courses. He is an active speaker at international security conferences and events, such as RootedCON, Black Hat, OWASP, BruCON, etc.

JESS GARCIA



Principal Instructor

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 worldwide.

EVENT LOCATION & TRAVEL INFORMATION SANS BRUSSELS 2016

Event Location: Radisson Blu Royal Hotel, Rue du Fosse-aux-Loups 47, Brussels, B-1000 BE

Telephone: +32 2 2192828

E-mail: info.brussels@radissonblu.com

Website: www.radissonblu.com



15

Nearby transport

Central Station rail and metro
400m
(Airport terminal)

Midi Station rail and metro
2 km
(Thalys and Eurostar terminals)

Directions

From Brussels Airport:

The train is the quickest transportation from airport to hotel. Airport Express trains depart every 15 minutes and take only 20 minutes to reach Brussels Central Station (Gare Centrale), which is just a few hundred meters from the hotel property.

From South Station

(Gare du Midi - Zuidstation):

From South Station, trams depart every 10 minutes and take only 10 minutes to reach De Brouckère Station or Central Station. Take Tram 3 (direction Esplanade) or Tram 4 (direction Gare du Nord) and disembark at Central Station or De Brouckère. The property is a short walk from either station.

Bus and metro options

Guests can travel efficiently throughout Brussels via the metro system. The De Brouckère and Central Station stops are only a few hundred meters away. Another convenient option is the Arenberg public bus, which stops next to the hotel's main entrance.

