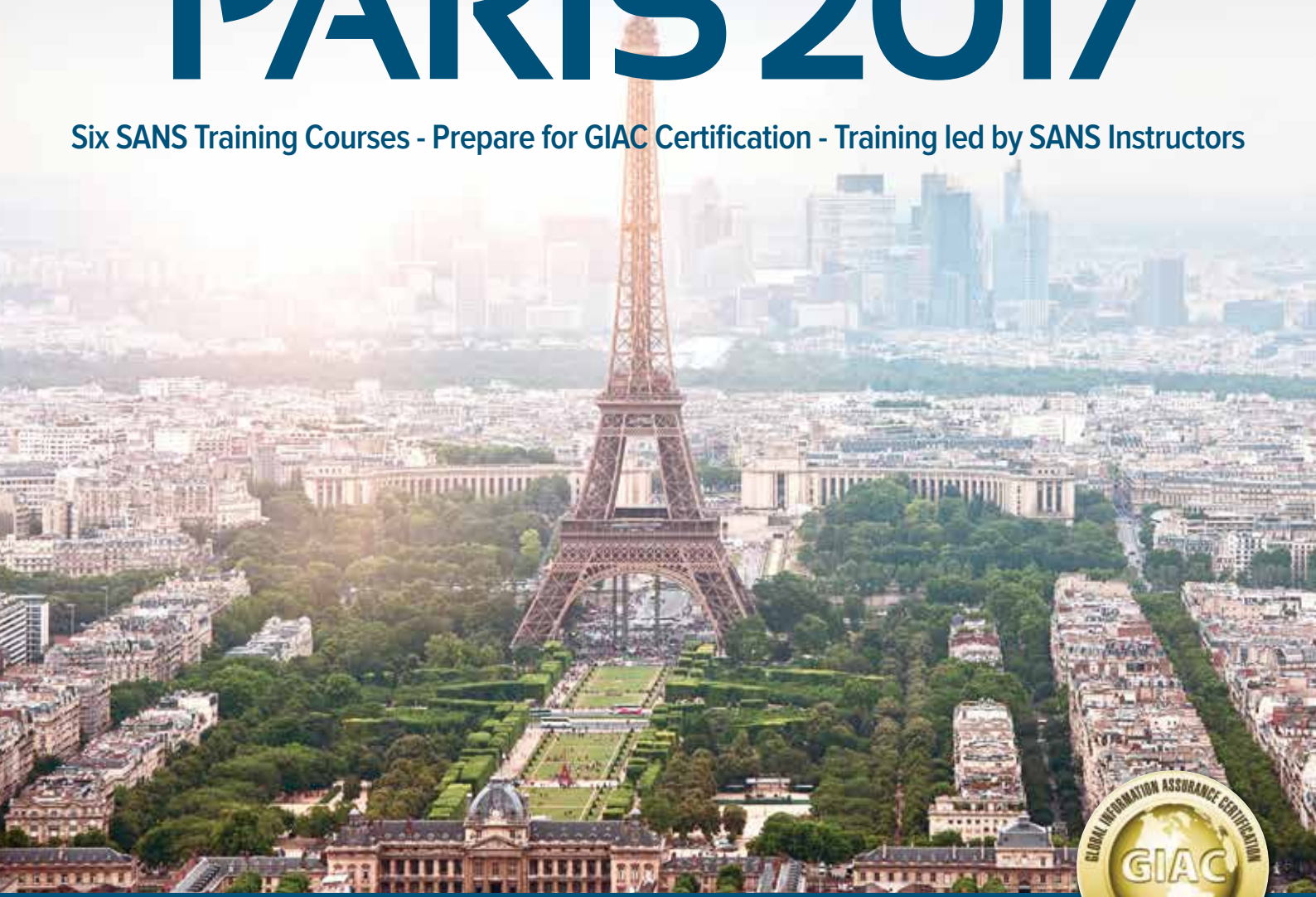
★ THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING ★

SANS EMEA

26 JUNE – 1 JULY, 2017 #SANSPARIS

SANS PARIS 2017

Six SANS Training Courses - Prepare for GIAC Certification - Training led by SANS Instructors



GLOBAL INFORMATION ASSURANCE CERTIFICATION GIAC www.giac.org

REGISTER ONLINE AND SEE FULL COURSE DESCRIPTIONS AT

WWW.SANS.ORG/PARIS-2017

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

HM Government

SANS is a Cyber Security Supplier to HM Government

Allianz für Cyber-Sicherheit Partner

HSD The Hague Security Delta

SANS IS THE WORLD'S LARGEST AND MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING. FOUNDED IN 1989, SANS OPERATES GLOBALLY AND HAS OVER 140,000 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 skills and knowledge.

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. 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 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 30 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, with both SANS and GIAC placing an emphasis on learning practical skills.

HOW TO REGISTER FOR SANS TRAINING

SANS runs public training events globally, including multiple events across Europe and the Middle East, 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, German, and Spanish. For details of all our training delivery options visit www.sans.org/emea.

VENUE

HOTEL

Paris Marriott Rive Gauche Hotel and Conference Centre
17 Boulevard Saint Jacques
Paris,
75014 FR

WELCOME TO SANS PARIS 2017

SANS PARIS 2017 RUNS FROM MONDAY 26TH JUNE TO SATURDAY JULY 1ST AT THE PARIS MARRIOTT RIVE GAUCHE HOTEL AND HOSTS 6 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.

Four courses at SANS Paris will be taught in English and two will be taught in French. Please note, all course books are in English.

Read on for course descriptions or visit **www.sans.org/paris-2017**

COURSES AT A GLANCE

		MON 26	TUE 27	WED 28	THU 29	FRI 30	SAT 01
FOR 408	WINDOWS FORENSIC ANALYSIS (In English)	●	●	●	●	●	●
FOR 508	ADVANCED DIGITAL FORENSICS, INCIDENT RESPONSE, AND THREAT HUNTING (In English)	●	●	●	●	●	●
ICS 515	ICS ACTIVE DEFENSE AND INCIDENT RESPONSE (In English)	●	●	●	●	●	●
SEC 401	SECURITY ESSENTIALS BOOTCAMP STYLE (In English)	●	●	●	●	●	●
SEC 504	HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING (In French)	●	●	●	●	●	●
SEC 560	NETWORK PENETRATION TESTING AND ETHICAL HACKING (In English)	●	●	●	●	●	●

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 artefacts 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

REGISTER NOW:
www.sans.org/paris-2017

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

FOR 408

WINDOWS FORENSIC ANALYSIS

LANGUAGE
ENGLISH

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

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

LANGUAGE
ENGLISH

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

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 attack 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

REGISTER NOW:
www.sans.org/paris-2017

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

REGISTER NOW:
www.sans.org/paris-2017

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

ICS 515

ICS ACTIVE DEFENCE AND INCIDENT RESPONSE

LANGUAGE
ENGLISH

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 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

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

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

LANGUAGE
ENGLISH

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 which 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)

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 in which to test and evaluate the 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

REGISTER NOW:
www.sans.org/paris-2017

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.

REGISTER NOW:
www.sans.org/paris-2017

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

LANGUAGE
FRENCH

COURSE DETAILS

Organisations' systems are likely to get hacked. All that's needed is an internet connection and 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

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

SEC 560

NETWORK PENETRATION TESTING AND ETHICAL HACKING

LANGUAGE
ENGLISH

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.

"THANKS 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)

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

REGISTER NOW:
www.sans.org/paris-2017

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION: INFORMATION SECURITY

Les professionnels de la sécurité informatique sont chargés de faire la recherche et l'analyse des menaces de sécurité qui peuvent mettre en danger les actifs, les produits ou les spécificités techniques d'une organisation.

Grâce à une formation pointue, ces professionnels de la sécurité vont explorer, de façon bien plus approfondie que la plupart de leurs collègues, les protocoles et les spécificités techniques liés aux menaces afin de déterminer des stratégies de défense contre les attaques.

EXEMPLES:
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

Un Network Operations Center (NOC) est un centre opérationnel où des professionnels de l'informatique encadrent, surveillent et mettent à jour les réseaux d'une entreprise. Ils effectuent des diagnostics de réseau en cas de problème, des mises à jour et la distribution de logiciels, la gestion des systèmes et des routeurs ; ils veillent au bon fonctionnement et à la coordination de réseaux liés. Les analystes NOC travaillent en liaison étroite avec le Security Operations Center (SOC) qui est chargé de la protection de l'entreprise et assure une surveillance en continu contre les menaces.

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

CORE COURSES
SEC301 GISF › SEC401 GSEC › SEC501 GCED

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

FUNCTION: SECURITY OPERATIONS CENTRE/ INTRUSION DETECTION

Le SOC est un centre opérationnel chargé de la détection d'intrusions, de la protection contre les incidents liés à une cyberattaque, de la veille sécuritaire, et de la protection des actifs du réseau de l'organisation et de ses terminaux. Les analystes SOC sont chargés de la sensibiliser l'entreprise aux situations, et de la surveillance continue, notamment la surveillance du trafic, le blocage de trafic Internet indésirable entrant et sortant, et la détection de tout type d'attaque. Les technologies de solution de sécurité sont le point de départ pour rendre les réseaux plus résistants aux tentatives d'intrusion potentielles.

CORE COURSES
SEC301 › SEC401

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

EXEMPLES:
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
- **SEC503** Intrusion Detection In-Depth GCIA
- **FOR572** Advanced Network Forensics and Analysis GNFA
- **SEC511** Continuous Monitoring and Security Operations GMON
- **SEC550** Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence
- **FOR578** Cyber Threat Intelligence

FUNCTION: RISK & COMPLIANCE/AUDITING/ GOVERNANCE

Ces experts évaluent et font des rapports de risque pour l'organisation en mesurant la conformité aux politiques, procédures et normes. Ils font des recommandations d'amélioration pour rendre l'organisation plus efficace et plus rentable à l'aide de contrôles permanents de la gestion du risque.

EXEMPLES:
Auditor, Compliance Officer

- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Programme
- **SEC566** Implementing & Auditing the Critical Security Controls - In-Depth GCCC
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems GSNA
- **LEG523** Law of Data Security and Investigations GLEG

FUNCTION: INCIDENT RESPONSE AND THREAT HUNTING

Lorsque la sécurité d'un système ou d'un réseau est compromise, la personne chargée de répondre aux incidents est en première ligne de défense pendant la brèche. Celui qui répond n'est pas seulement ingénieux sur le plan technique, il doit aussi gérer le stress généré par l'incident, s'occuper des personnes, des processus et des technologies afin de répondre de façon rapide et efficace et de minimiser les dommages causés par l'incident.

EXEMPLES:
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

Parce que la meilleure défense consiste à connaître ses adversaires et ses propres faiblesses, ces experts apportent une énorme valeur ajoutée à l'organisation. Ils appliquent diverses techniques d'attaque leur permettant de trouver les points de vulnérabilité, évaluent le risque encouru par l'organisation, et recommandent des solutions de protection avant que ces failles ne soient exploitées par de véritables hackers.

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

CORE COURSES
SEC301 GISF › SEC401 GSEC

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

Network & Exploits
- **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** Immersive Hands-on Hacking Techniques
- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise

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

FUNCTION: SECURE DEVELOPMENT

Le développeur, expert en matière de sécurisation des logiciels, encourage naturellement tous ses collègues développeurs à concevoir des logiciels sécurisés et à implémenter des techniques de programmation sécurisées ne comportant pas de faille du point de vue de la conception et de la mise en application technique. L'expert a l'ultime responsabilité d'assurer que le logiciel de son client ne comporte aucune vulnérabilité pouvant être exploitée par un assaillant.

EXEMPLES:
Developer, Software Architect, QA Tester, Development Manager

Core
- **Securing the Human for Developers STH. Developer** Application Security Awareness Modules
- **DEV522** Defending Web Applications Security Essentials GWEB
- **DEV531** Defending Mobile Applications Security Essentials
- **DEV534** Secure DevOps: A Practical Introduction

Secure Coding
- **DEV541** Secure Coding in Java/JEE GSSP-JAVA
- **DEV544** Secure Coding in .NET GSSP-.NET
- **DEV543** Secure Coding in C/C++

Specialisations
- **SEC542** Web App Penetration Testing & Ethical Hacking GWAPT
- **SEC642** Advanced Web App Penetration Testing & Ethical Hacking

FUNCTION: CYBER OR IT SECURITY MANAGEMENT

La gestion du personnel, des processus et des technologies est essentielle pour maintenir de façon proactive une sensibilisation à la sécurité dans l'organisation et pour assurer une surveillance continue efficace. Ces dirigeants doivent avoir des connaissances actualisées et des compétences en matière de leadership ; ils se doivent d'être exemplaires, en appliquant des pratiques exemplaires, et capables de prendre des décisions au bon moment, des décisions efficaces qui profiteront à la totalité de l'infrastructure de l'information de l'entreprise.

EXEMPLES:
CISO, Cyber Security Manager / Officer, Security Director

Foundational
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ GSLC
- **MGT525** IT Project Management, Effective Communica-tion, 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
- **MGT415** A practical Introduction to Cybersecurity Risk Management

Specialisation
- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Programme
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems GSNA
- **SEC566** Implementing and Auditing the Critical Security Controls - In-depth GCCC

FUNCTION: DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

De nos jours, en raison de l'évolution perpétuelle des technologies et des environnements, il est inévitable que toute organisation doive faire face à la cybercriminalité, notamment en matière de fraude, de menaces internes, d'espionnage industriel et d'hameçonnage (phishing). Pour relever ces défis, les organisations recrutent des professionnels de l'investigation inforensique et elles s'appuient aussi sur des agents de lutte contre la cybercriminalité pour reconstituer dans le détail l'attaque qui a été commise.

EXEMPLES:
Computer Crime Investigator, Law Enforcement, Digital Investigations Analyst, Media Exploitation Analyst, Information Technology Litigation Support & Consultant, Insider Threat Analyst

- **FOR408** Windows Forensic Analysis GCFE
- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling GCIH
- **FOR508** Advanced Digital Forensics and Incident Response GCFA
- **FOR585** Advanced Smartphone Forensics GASF
- **FOR518** MAC Forensic Analysis
- **FOR526** Memory Forensics In-Depth

FUNCTION: INDUSTRIAL CONTROL SYSTEMS

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 GRID

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