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

SANS EMEA

SANS PRAGUE

MON 9 - SAT 14 MAY, 2016 #SANSPRAGUE

4 SANS COURSES

SEC401
Security Essentials
Bootcamp Style

SEC503
Intrusion Detection
In-Depth

SEC511
Continuous Monitoring
and Security Operations

SEC560
Network Penetration Testing
and Ethical Hacking

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

COURSES AT A GLANCE

	MON 9	TUE 10	WED 11	THU 12	FRI 13	SAT 14
SEC 401 Security Essentials Bootcamp Style *Tim Garcia*	p8	●	●	●	●	●
SEC 503 Intrusion Detection In-Depth *David Hoelzer*	p9	●	●	●	●	●
SEC 511 Continuous Monitoring and Security Operations *Bryan Simon*	p10	●	●	●	●	●
SEC 560 Network Penetration Testing and Ethical Hacking *Erik Van Buggenhout*	p11	●	●	●	●	●

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.

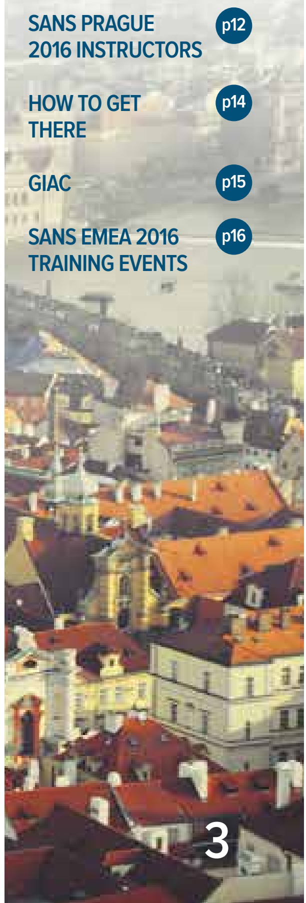
Why SANS is the best training and educational investment:

- 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 PRAGUE 2016

SANS PRAGUE 2016 RUNS FROM MONDAY 9TH MAY TO SATURDAY 14TH MAY AT THE ANGELO HOTEL PRAGUE AND HOSTS 4 COURSES DRAWN FROM ACROSS THE SANS CURRICULUM.

> SEC503 runs from 9am-5pm Monday till Saturday and SEC560 finishes at 7:15pm on Monday and SEC401 and SEC511 finish at 7pm Monday – Friday and then 5pm on Saturday.

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.

The demand for places at Prague events is always high so please register online as soon as possible to secure a seat at SANS Prague 2016. Read on for course descriptions or visit www.sans.org/prague-2016

Over the page you will find the SANS Career Roadmap which provides examples of how SANS courses fit into your career development plan.

CONTACT SANS

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

REGISTER ONLINE AT:

WWW.SANS.ORG/PRAGUE-2016

SANS
SANS PRAGUE
CONTINUOUS MONITORING AND SECURITY OPERATIONS
NETWORK PENETRATION TESTING AND ETHICAL HACKING

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/prague-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 13 April 2016 by emailing emea@sans.org

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR CAREER ROAD MAP

CORE COURSES

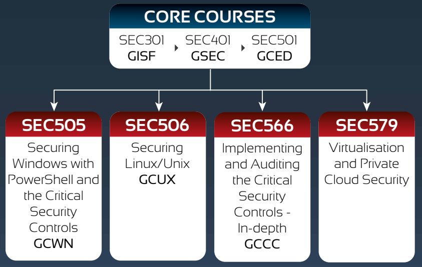
FUNCTION:

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

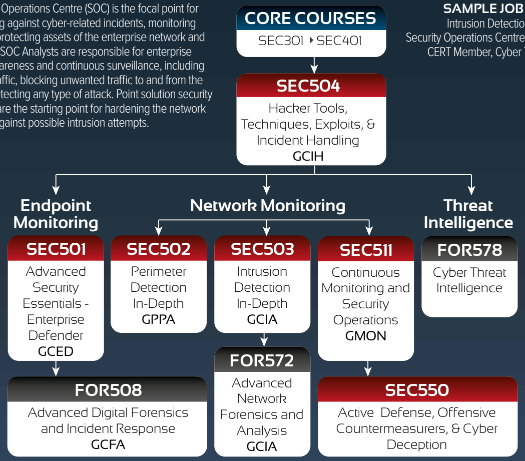
SEC579 Virtualisation and Private Cloud Security

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.

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



CORE COURSES
SEC301 ▸ SEC401

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 Countermeasures, & Cyber Deception

Threat Intelligence

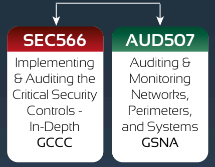
FOR578 Cyber Threat Intelligence

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

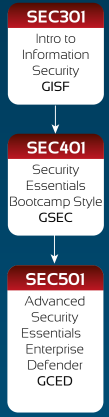
FUNCTION:

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

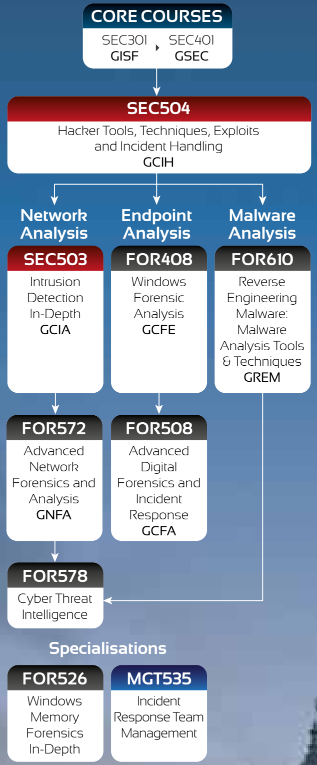
SEC501 Advanced Security Essentials Enterprise Defender GCED

FUNCTION:

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

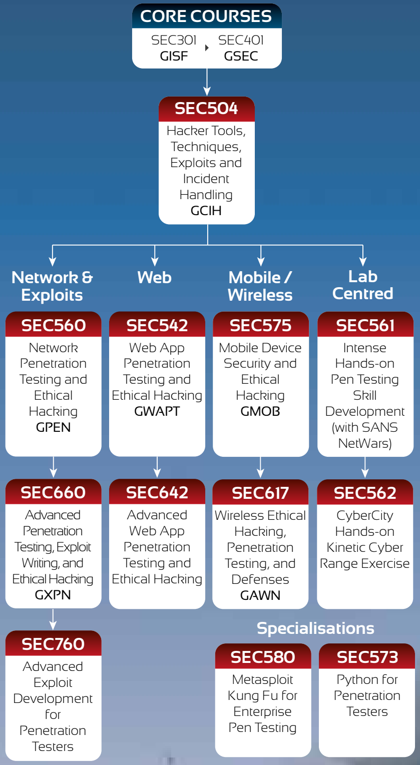
MGT535 Incident Response Team Management

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

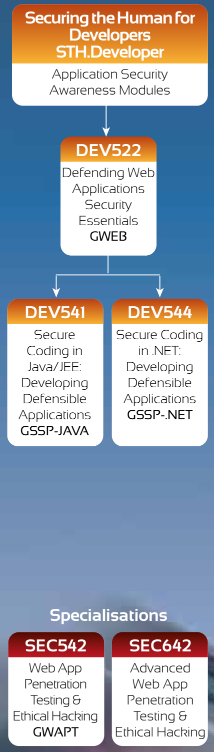
FUNCTION:

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

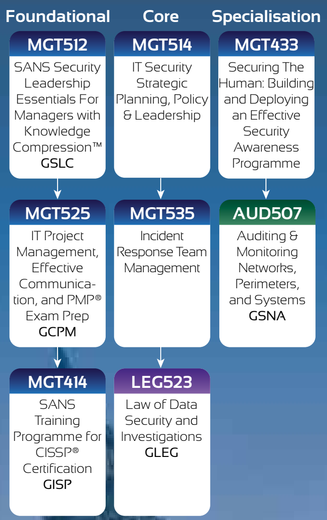
SEC642 Advanced Web App Penetration Testing & Ethical Hacking

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

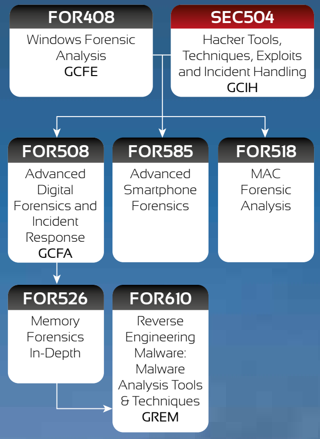
AUD507 Auditing & Monitoring Networks, Perimeters, and Systems GSNA

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

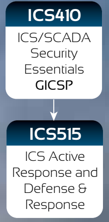
FOR526 Memory Forensics In-Depth

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.



ICS410 ICS/SCADA Security Essentials GICSP

ICS515 ICS Active Response and Defense & Response

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

SEC 401

WWW.SANS.ORG/SEC401

SECURITY ESSENTIALS BOOTCAMP STYLE

TIM GARCIA
46 CPE/CMU Credits | GIAC Cert: GSEC
Monday - Saturday: 9am - 5pm

COURSE DETAILS

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

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

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

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

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

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

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

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

YOU WILL BE ABLE TO...

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

GIAC SECURITY ESSENTIALS CERTIFICATION
GSEC

WWW.SANS.ORG/SEC503

INTRUSION DETECTION IN-DEPTH

DAVID HOELZER
36 CPE/CMU Credits | GIAC Cert: GCIA
Monday - Saturday: 9am - 5pm

SEC 503

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

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

GIAC CERTIFIED INTRUSION ANALYST
GCIA

WWW.SANS.ORG/SEC511

CONTINUOUS MONITORING AND SECURITY OPERATIONS

BRYAN SIMON
36 CPE/CMU Credits | GIAC Cert: GMON
Monday - Saturday: 9am - 5pm

YOU WILL BE ABLE TO...

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

COURSE DETAILS

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

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

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

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

The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether.

The National Institute of Standards and Technology developed guidelines described in NIST SP 800-137 for Continuous Monitoring, and day five greatly increase students' understanding and enhances their skills in implementing Continuous Monitoring systems utilising NIST framework.

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

WWW.SANS.ORG/SEC560

NETWORK PENETRATION TESTING AND ETHICAL HACKING

ERIK VAN BUGGENHOUT
37 CPE/CMU Credits | GIAC Cert: GPEN
Monday - Saturday: 9am - 5pm

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.

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

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

SANS PRAGUE 2016 INSTRUCTORS

Bryan Simon

CERTIFIED INSTRUCTOR

@BryanOnSecurity

Bryan Simon is an internationally recognised expert in cybersecurity and has been working in the information technology and security field since 1991.

Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. He has instructed individuals from organisations such as the FBI, NATO, and the UN in matters of cybersecurity, on two continents.

Bryan has specialised expertise in defensive and offensive capabilities. He has received recognition for his work in I.T. Security, and was most recently profiled by McAfee (part of Intel Security) as an I.T. Hero. Bryan holds 11 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, and GCUX.

Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program. Bryan is a SANS Certified Instructor for SEC401: Security Essentials Bootcamp Style, SEC501: Advanced Security Essentials - Enterprise Defender, SEC505: Securing Windows with Powershell and the Critical Security Controls, and SEC511: Continuous Monitoring and Security Operations. ●

David Hoelzer

FELLOW

@it_audit

David Hoelzer is a SANS Fellow instructor and author of more than twenty sections of SANS courseware.

He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years.

David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organisations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities.

Currently, David serves as the principal examiner and director of research for Enclave Forensics; a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defence, an open source security software solution provider. ●

Erik Van Buggenhout

Erik is an instructor for the SANS SEC542 "Web Application Penetration Testing & Ethical Hacking" and SANS SEC560 "Network Penetration Testing & Ethical Hacking" courses.

Next to his teaching activities for SANS, Erik is the head of technical security services at nViso. NViso is a Brussels-based IT security firm founded in early 2013. At nViso, Erik mainly focuses on security assessments (both on a network and application level).

Next to security assessments, he also advises clients on how they can improve their IT security posture. Before co-founding nViso, Erik was a manager at Ernst & Young, where he led a team of technical security experts in the Diegem (Brussels) office. Together with his team, he delivered technical security advisory services to major clients in the EMEA financial services industry. ●

Tim Garcia

@tbg911

Timothy Garcia is an experienced security professional who loves the challenge and continuously changing landscape of defence.

Tim started his career as an engineer in IT and after working on a few security incidents related to Code Red and Nimda; he realised he had found his calling.

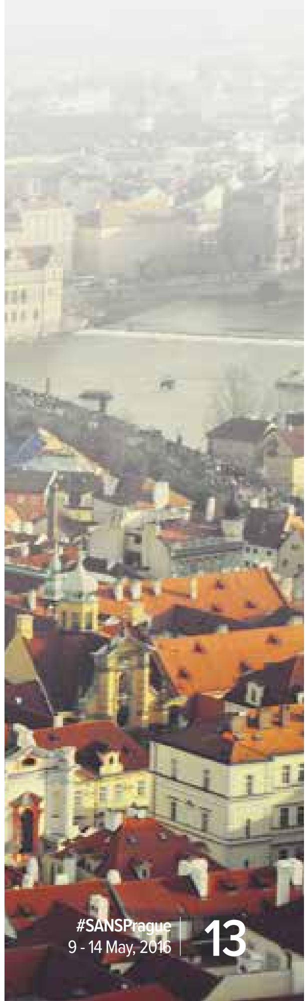
Tim currently works as an Information Security Consultant for Wells Fargo and has expertise in systems engineering, project management and information security principles and procedures/ compliance. Before Wells Fargo, Tim worked for Intel and served in the military.

Tim is as passionate about teaching security as he is performing it and receives the greatest joy when he sees the look in a student's eye when something they never quite understood finally makes sense.

Tim holds the CISSP, GSEC, GCIH and NSA-IAM certifications. He has extensive knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, CobiT, COSO, and ISO 1779. ●

WE HAVE AN OUTSTANDING LINE UP OF EUROPEAN AND US-BASED INSTRUCTORS AT SANS PRAGUE 2016.

READ ON FOR PROFILES OF THIS ELITE GROUP.



HOW TO GET THERE

SANS PRAGUE TAKES PLACE AT THE ANGELO HOTEL, PRAGUE

BY TRAIN:

From the main train station:
The easiest way to get to the angelo Hotel from the main train station is by tram. The tram stop is located directly in front of the station. Take tram no. 9 in the direction of “Sídliště Řepy” and get off at the “Anděl” tram stop.
Travel time: 17 min

From Holešovice train station:
From Holešovice station, take metro line C to “Florenc” station. Change to yellow line B towards “Zličín” and go five stops to “Anděl”.
Travel time: 17 min

BY PLANE:

From Václav Havel Airport Prague:
Take bus No. 191 (a stop is located directly in front of Terminal 1 and Terminal 2) from the airport to the “Anděl” stop.
Travel time: 48 min.

BY CAR:

From Václav Havel Airport Prague:
From the airport, follow the signs to Pilsen / R1 and take exit 26 for “Pražský okruh”. Continue on through Karlovarská, Bělohorská and Patočkova streets. Merge onto Pražský okruh (slight left) and continue directly onto Strahov Tunnel. Exit onto Plzeňská and after approx. 400 m turn right onto Radlická. The hotel will be on the left.

From Nuremberg / Pilsen:
Take highway D5 and exit after km 151. Turn left onto Bucharova and continue for 1,3 km onto Radlická street. Turn left after 4,4 km to stay on Radlická street. The hotel will be on the right.

From Vienna / Brno:
Follow Highway D1 to Prag and exit onto 5. května. Merge onto jižní spojka and follow this highway for 5,7 km to Barrandov Bridge. After another 3,9 km, take the exit toward Smíchov / Radlice and continue onto Radlická street. The hotel will be on the right.

Please use the following GPS coordinates: N50°4’13.746” E14°24’5.753” or our address: Radlická 1g, 150 00 Prague 5.

PARKING:

The angelo Hotel Prague has an underground car park. 19 parking places are available for and extra fee of CZK 700 (EUR 26) each day.

SANS EMEA

SANS EMEA TRAINING EVENTS 2016

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

		IT AUDIT	DEVELOPER		MANAGE			FORENSICS								ICS/SCADA		SECURITY																			
		6 DAYS	6 DAYS	4 DAYS	2 DAYS	5 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	6 DAYS	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS
LOCATION	DATE	AUD507	DEV522	DEV541	MGT433	MGT512	MGT514	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
SECURE EUROPE, 2016	APR 4TH - 16TH							●				●						●	●		●	●								●						●	
ICS AMSTERDAM, 2016	APR 18TH - 22ND						●									●	●																				
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					●												●			●	●											●		●		
OSLO, 2016	OCT 3RD - 8TH			●																						●		●									
DFIR PRAGUE, 2016	OCT 3RD - 15TH							●	●	●	●	●	●	●	●																						
GULF REGION, 2016	NOV 5TH - 17TH																	●				●			●	●		●					●				
EUROPEAN SECURITY AWARENESS SUMMIT	NOV 9TH - 11TH																																				
LONDON, 2016	NOV 14TH - 19TH		●						●			●						●	●		●		●		●	●	●	●								●	
AMSTERDAM, 2016	DEC 12TH - 17TH																																				
FRANKFURT, 2016	DEC 12TH - 17TH																																				

V17 - A5

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

Dates, Locations and Courses offered subject to change