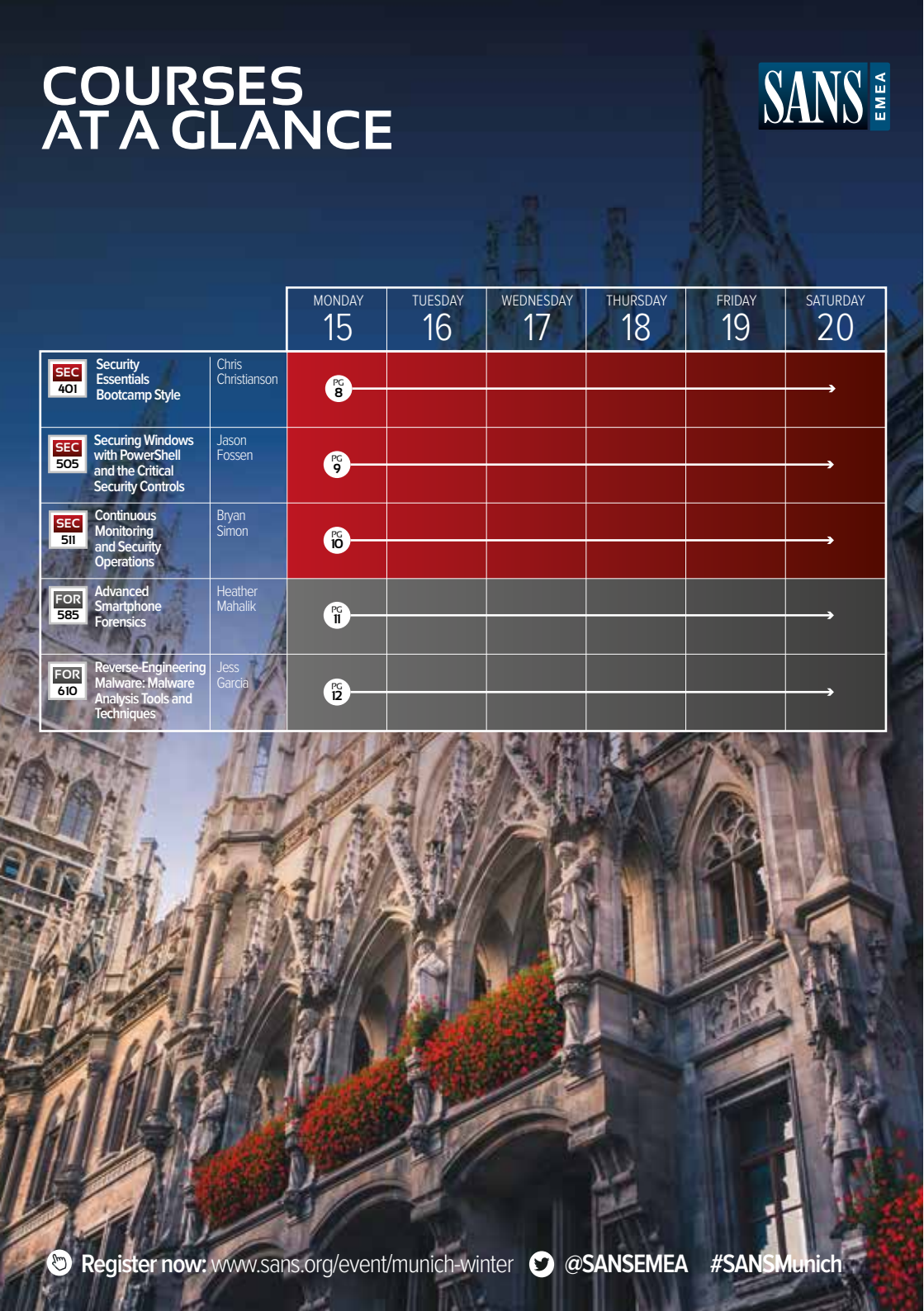

THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING
Immersive Training ★ World Class Instructors ★ GIAC Certification ★ SANS@Night evening talks and networking ★ Social Functions
SANS EMEA
MON 15 - SAT 20 FEBRUARY, 2016
SANS MUNICH
#SANSMunich
5 SANS COURSES
SEC401 Security Essentials Bootcamp Style
SEC505 Securing Windows with PowerShell and the Critical Security Controls
SEC511 Continuous Monitoring and Security Operations
FOR585 Advanced Smartphone Forensics
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Register online and see full course descriptions at www.sans.org/event/munich-winter-2016
Save 450 Euros with discount code "EarlyBird16" for a 4-6 day course by 30 Dec, 2015.
HM Government
SANS is a Cyber Security Supplier to Government
GIAC

COURSES AT A GLANCE

SANS EMEA

		MONDAY 15	TUESDAY 16	WEDNESDAY 17	THURSDAY 18	FRIDAY 19	SATURDAY 20
SEC 401 Security Essentials Bootcamp Style	Chris Christianson	PG 8 →					
SEC 505 Securing Windows with PowerShell and the Critical Security Controls	Jason Fossen	PG 9 →					
SEC 511 Continuous Monitoring and Security Operations	Bryan Simon	PG 10 →					
FOR 585 Advanced Smartphone Forensics	Heather Mahalik	PG 11 →					
FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	Jess Garcia	PG 12 →					



Register now: www.sans.org/event/munich-winter **@SANSEMEA** **#SANSMunich**

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.

Register now www.sans.org/event/munich-winter-2016

@SANSEMEA #SANSMunich

CONTENTS

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

SANS EMEA

WELCOME TO SANS MUNICH 2016

SANS Munich runs from Monday 15th to Saturday 20th February at the Munich Marriott Hotel 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 except for course SEC401 which finishes at 7pm Monday-Friday and 5pm on Saturday.

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

Read on for course descriptions or visit www.sans.org/event/munich-winter. 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:
Munich Marriott Hotel
Berliner Strasse 93
Munich, 80805 DE

Telephone: +49-89-360020
E-mail: info.brussels@radissonblu.com
Website: www.marriott.co.uk

Register now www.sans.org/event/munich-winter

@SANSEMEA #SANSMunich

SANS MUNICH 2016
REGISTRATION INFORMATION

REGISTER ONLINE AT: WWW.SANS.ORG/EVENT/MUNICH-WINTER

REGISTER EARLY AND SAVE

Register for #SANSMunich and pay before the 30th of December and save €450 by entering the code EarlyBird16

All course prices are listed at sans.org/event/munich-winter

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/munich-winter** 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 Jan 20th, 2016, by emailing emea@sans.org

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION:

INFORMATION SECURITY

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

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

SAMPLE JOB TITLES:
Cyber Security Analyst , Cyber Security Engineer, Cyber Security Architect

SEC301
Intro to Information Security
GISF

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials Enterprise Defender
GCED

FUNCTION:

NETWORK OPERATIONS CENTRE, SYSTEM ADMIN, SECURITY ARCHITECTURE

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

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

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

CORE COURSES
SEC301 GISF › SEC401 GSEC › SEC501 GCED

SEC505
Securing Windows with PowerShell and the Critical Security Controls
GCWN

SEC506
Securing Linux/Unix
GCUX

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

SEC579
Virtualisation and Private Cloud Security

FUNCTION:

INCIDENT RESPONSE

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

SAMPLE JOB TITLES:
Security analyst/engineer, SOC analyst, Cyber threat analyst, CERT member, Malware analyst

CORE COURSES
SEC301 GISF › SEC401 GSEC

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
GCIH

Network Analysis

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GNFA

Endpoint Analysis

FOR408
Windows Forensic Analysis
GCFE

FOR508
Advanced Digital Forensics and Incident Response
GCFA

Malware Analysis

FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

FOR578
Cyber Threat Intelligence

Specialisations

FOR526
Windows Memory Forensics In-Depth

MGT535
Incident Response Team Management

FUNCTION:

PENETRATION TESTING/ VULNERABILITY ASSESSMENT

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

SAMPLE JOB TITLES:
Penetration tester, Vulnerability assessor, Ethical hacker, Red/Blue team member, Cyberspace engineer

CORE COURSES
SEC301 GISF › SEC401 GSEC

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling
GCIH

Network & Exploits

SEC560
Network Penetration Testing and Ethical Hacking
GPEN

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

SEC760
Advanced Exploit Development for Penetration Testers

Web

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing and Ethical Hacking

Mobile / Wireless

SEC575
Mobile Device Security and Ethical Hacking
GMOB

SEC617
Wireless Ethical Hacking, Penetration Testing, and Defenses
GAWN

Lab Centred

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

SEC562
CyberCity Hands-on Kinetic Cyber Range Exercise

Specialisations

SEC580
Metasploit Kung Fu for Enterprise Pen Testing

SEC573
Python for Penetration Testers

Nov 15

FUNCTION:

SECURITY OPERATIONS CENTRE/ INTRUSION DETECTION

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

CORE COURSES
SEC301 ▸ SEC401

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

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

Endpoint Monitoring

SEC501
Advanced Security Essentials - Enterprise Defender
GCED

FOR508
Advanced Digital Forensics and Incident Response
GCFA

Network Monitoring

SEC502
Perimeter Detection In-Depth
GPPA

SEC503
Intrusion Detection In-Depth
GCIA

FOR572
Advanced Network Forensics and Analysis
GCIA

SEC511
Continuous Monitoring and Security Operations
GMON

SEC550
Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence

FOR578
Cyber Threat Intelligence

FUNCTION:

RISK & COMPLIANCE/ AUDITING/ GOVERNANCE

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

SAMPLE JOB TITLES:
Auditor, Compliance Officer

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

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

FUNCTION:

SECURE DEVELOPMENT

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

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

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

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

DEV522
Defending Web Applications Security Essentials
GWEB

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

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

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

Specialisations

SEC542
Web App Penetration Testing & Ethical Hacking
GWAPT

SEC642
Advanced Web App Penetration Testing & Ethical Hacking

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

Instructor: Chris Christianson
Six-Day Programme: Mon 15th – Sat 20th February 9:00am - 7:00pm
46 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.

"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

SEC 505

SECURING WINDOWS WITH POWERSHELL AND THE CRITICAL SECURITY CONTROLS

Instructor: Jason Fossen

Six-Day Programme: Mon 15th – Sat 20th February 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GCWN
Laptop Required

Course details

What is *Windows Hello* in Windows 10? How can we defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? We tackle these tough problems in SEC505: Securing Windows with PowerShell and the Critical Security Controls. Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defences against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is very useful, but there is no simple patch against the abuse of these tools. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future.

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy and PowerShell scripting.

Learning PowerShell is probably the single best new skill for Windows administrators, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills; so knowing PowerShell is a great way to make your resume stand out. This course devotes the entire first day to PowerShell, and then we do more PowerShell exercises throughout the rest of the week. Don't worry; you don't need any prior scripting experience to attend.

You will learn...

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

SEC 511

CONTINUOUS MONITORING AND SECURITY OPERATIONS

Instructor: Bryan Simon

Six-Day Programme: Mon 15th – Sat 20th February 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GMON
Laptop Required

You will learn...

- To analyse a security architecture for deficiencies
- To apply the principles learned in the course to design a defensible security architecture
- The importance of a detection-dominant security architecture and security operations centres
- To identify the key components of Network Security Monitoring/ Continuous Diagnostics and Mitigation/ Continuous Monitoring
- How to determine appropriate security monitoring needs for organisations of all sizes
- To implement a robust Network Security Monitoring/Continuous Security Monitoring
- How to determine requisite monitoring capabilities for a SOC environment
- How to determine capabilities required to support continuous monitoring of key Critical Security Controls
- To utilise tools to support implementation of Continuous Monitoring per NIST guidelines SP 800-137

Course details

We continue to underestimate the tenacity of our adversaries! Organisations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organisations are still getting compromised. 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 victimised by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organisations, because they know that the lack of visibility and internal security controls will then 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 your 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 will greatly increase your understanding and enhance your skills in implementing Continuous Monitoring utilising NIST framework.

The final day features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed.

"An energetic engaging teacher with the experience and knowledge to tackle subjects facing SOCs today and make this information relevant-useful."

MICK LEACH, NATIONWIDE

FOR 585

ADVANCED SMARTPHONE FORENSICS

Instructor: Heather Mahalik

Six-Day Programme: Mon 15th – Sat 20th February 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GCFE
Laptop Required

Course details

FOR585: Advanced Smartphone Forensics teaches real-life, hands-on skills that help digital forensic examiners, law enforcement officers, and information security professionals handle investigations involving even the most complex smartphones currently available.

The course focuses on smartphones as sources of evidence, providing students with the skills needed to handle mobile devices in a forensically sound manner, manipulate locked devices, understand the different technologies, discover malware, and analyse the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyse data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. Students will walk away with knowledge they can immediately put to use on their next smartphone investigation.

The hands-on exercises in this course cover the best commercial and open-source tools available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorised activities, determine if a smartphone has been compromised with malware or spyware, and provide your organisation with the capability to use evidence from smartphones.

This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and constantly changing, most forensics professionals are unfamiliar with the data formats. It is time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

You will learn...

- How to determine the who, what, when, where, why, and how of a case. Who used a smartphone? What did the user do on a smartphone? Where was the smartphone located at key times? What online activities did the user conduct using a smartphone, and when?
- How to recover deleted data: Use manual decoding techniques to recover deleted data stored on smartphones and mobile devices.
- How to detect data stored in Third-Party Applications: Who did the user communicate with using a smartphone and why are these activities sometimes hidden?
- How to detect malware: Detect smartphones compromised by malware using forensics methods.
- How to bypass locks: Bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes.

FOR 610

REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

Instructor: Jess Garcia

Six-Day Programme: Mon 15th – Sat 20th February 9:00am - 5:00pm
36 CPE/CMU Credits | GIAC Cert: GREM
Laptop Required

You will learn...

- How to build an isolated, controlled laboratory environment for analysing the code and behaviour of malicious programs.
- To employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment.
- How to uncover and analyse malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks.
- To control relevant aspects of the malicious program's behaviour through network traffic interception and code patching to perform effective malware analysis.
- How to use a disassembler and a debugger to examine the inner workings of malicious Windows executables.

Course details

This course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organisation's ability to derive threat intelligence, respond to information security incidents, and fortify defences. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioural patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. In addition, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

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

You will learn how to analyse malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if the software exhibits rootkit characteristics.

"High valuable content that has immediately boosted my skills. The day 6 CTF was awesome."

RAFE PILLING, DELL SECUREWORKS

SANS MUNICH 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 Munich 2016. Read on for profiles of this elite group.

CHRIS CHRISTIANSON

Chris Christianson is an Information Security Analyst and Network Engineer who lives and works in Northern California. He currently works in the financial industry and is the Assistant Vice President of Network Services for one of the nation's largest credit unions. With more than fifteen years of experience, Chris has spoken at conferences, contributed articles for magazines, and obtained many technical certifications including: CCSE, CCDP, CCNP, GSEC, CISSP, IAM, GCIH, CEH, IEM, GCIA, GREM, GPEN, and GWAPT. He has also earned a Bachelor of Science in Management Information Systems.

JASON FOSSEN

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS Institute's week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. Jason blogs about Windows Security Issues on the SANS Cyber Defense Blog.

BRYAN SIMON

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. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. 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.

HEATHER MAHALIK

Heather Mahalik is leading the forensic effort for Ocean's Edge as a project manager. Heather's extensive experience in digital forensics began in 2003. She is currently a senior instructor for the SANS Institute and is the course lead for FOR585: Advanced Smartphone Forensics.

Most of Heathers experience includes: Smartphone forensics: including acquisition, analysis, vulnerability discovery, malware analysis, application reverse engineering, manual decoding, forensic instruction on mobile, smartphone, computer and Mac forensics in support of the U.S government, LE, and commercial level. Heather is also a co-author of practical mobile forensics which is currently a best seller from Pack't Publishing as well as a technical editor for Learning Android Forensics from Pack't Publishing.

JESS GARCIA

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 MUNICH 2016

Event Location: Munich Marriott Hotel, Berliner Strasse 93 Munich, 80805 DE
Telephone: +49-89-360020 **Website:** www.marriott.co.uk

From Munich airport

- Alternate transportation: Lufthansa Airport Shuttle Bus, 5am-9.30pm every 20 min; fee: 10.5 EUR (one way); scheduled
- Bus service, fee: 10.5 EUR (one way)
- Subway service, fee: 10.8 EUR (one way)
- Estimated taxi fare: 50 EUR (one way)

Driving instructions

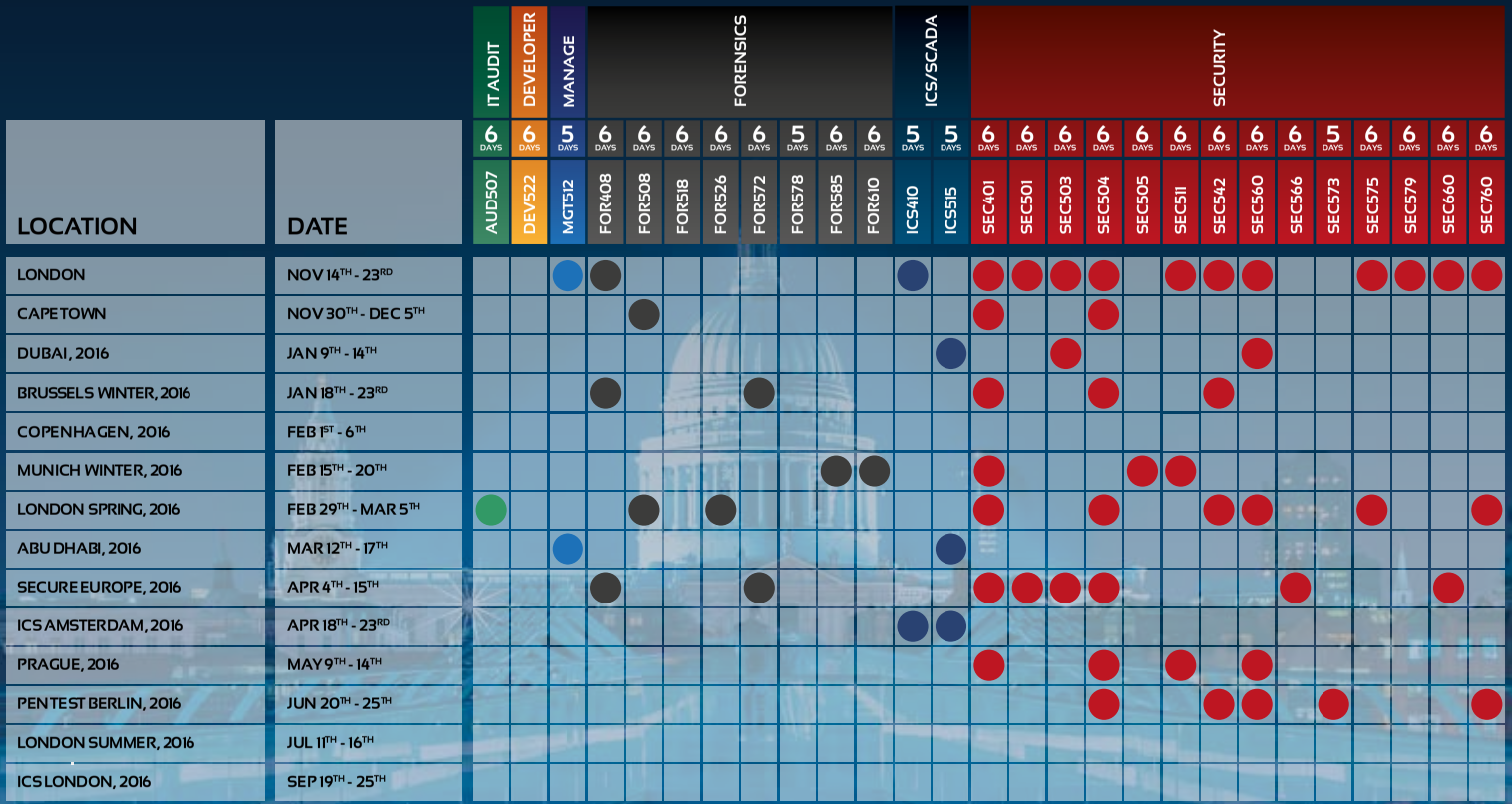
From Munich Airport: Take HWY A9 direction 'Muenchen' follow the signs 'Muenchen' until the end of the highway. After 200 m, take a right into 'Theodor Dombart Strasse.' Turn right again into 'Berliner Strasse.'

Nearest public transport

- Bus Station: Nordfriedhof 0.5km,
- Subway Station: U6, Nordfriedhof 0.5km
- Train Station: Munich Train Station 6km

FUTURE SANS EMEA TRAINING EVENTS 2015/16

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



		IT AUDIT	DEVELOPER	MANAGE	FORENSICS							ICS/SCADA		SECURITY													
		6 DAYS	6 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	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS
LOCATION	DATE	AUD507	DEV522	MGT512	FOR408	FOR508	FOR518	FOR526	FOR572	FOR578	FOR585	FOR610	ICS410	ICS515	SEC401	SEC501	SEC503	SEC504	SEC505	SEC511	SEC542	SEC560	SEC566	SEC573	SEC575	SEC579	SEC660	SEC760
LONDON	NOV 14TH - 23RD			●	●								●		●	●	●	●		●	●	●			●	●	●	●
CAPE TOWN	NOV 30TH - DEC 5TH					●									●			●										
DUBAI, 2016	JAN 9TH - 14TH													●			●					●						
BRUSSELS WINTER, 2016	JAN 18TH - 23RD				●				●						●			●			●							
COPENHAGEN, 2016	FEB 1ST - 6TH																											
MUNICH WINTER, 2016	FEB 15TH - 20TH										●	●			●				●	●								
LONDON SPRING, 2016	FEB 29TH - MAR 5TH	●				●		●							●			●			●	●			●			●
ABU DHABI, 2016	MAR 12TH - 17TH			●										●														
SECURE EUROPE, 2016	APR 4TH - 15TH				●				●						●	●	●	●					●				●	
ICS AMSTERDAM, 2016	APR 18TH - 23RD												●	●														
PRAGUE, 2016	MAY 9TH - 14TH														●			●		●		●						
PENTEST BERLIN, 2016	JUN 20TH - 25TH																	●			●	●		●				●
LONDON SUMMER, 2016	JUL 11TH - 16TH																											
ICS LONDON, 2016	SEP 19TH - 25TH																											

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

Dates, Locations and Courses offered subject to change