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

SANS EMEA

SANS STOCKHOLM

MON 9TH – SAT 14 MAY, 2016 #SANSSTOCKHOLM

5 SANS COURSES

SEC504
Hacker Tools, Techniques, Exploits and Incident Handling

SEC575
Mobile Device Security and Ethical Hacking

SEC579
Virtualization and Private Cloud Security

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques

DEV522
Defending Web Applications Security Essentials

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

Save €450 with discount code "**EarlyBird16**" for any course by 23 March, 2016.

COURSES AT A GLANCE

		MO 9	TU 10	WE 11	TH 12	FR 13	SA 14
SEC 504	Hacker Tools, Techniques, Exploits and Incident Handling *BJ Gleason*	p8	●	●	●	●	●
SEC 575	Mobile Device Security and Ethical Hacking *Raul Siles*	p9	●	●	●	●	●
SEC 579	Virtualization and Private Cloud Security *Dave Shackleford*	p10	●	●	●	●	●
FOR 610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques *Jess Garcia*	p11	●	●	●	●	●
DEV 522	Defending Web Applications Security Essentials *Jason Lam*	p12	●	●	●	●	●

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 STOCKHOLM 2016

EVENT LOCATION
Radisson Blu Waterfront Hotel
Nils Ericsons Plan 4
Stockholm,
111 64 SE

Telephone
+46 (8) 5050 6000
Website
www.radissonblu.com

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

SANS STOCKHOLM 2016 RUNS FROM MONDAY 9TH MAY TO SATURDAY 14TH MAY AT THE RADISSON BLU WATERFRONT HOTEL AND HOSTS 5 COURSES DRAWN FROM ACROSS THE SANS CURRICULUM.

All courses run from 9am-5pm apart from SEC504 which finishes at 7:15pm Monday and then finishes at 5pm Tuesday till 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 Stockholm events is always high so please register online as soon as possible to secure a seat at SANS Stockholm 2016.

Read on for course descriptions or visit www.sans.org/stockholm-2016

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

REGISTER ONLINE AT:

WWW.SANS.ORG/STOCKHOLM-2016

REGISTER EARLY AND SAVE:

Register #SANSStockholm and pay before the 23rd Mar and save €450 by entering the code EarlyBird16

GROUP SAVINGS

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

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

TO REGISTER

To register, go to www.sans.org/stockholm-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

REGISTER NOW www.sans.org/stockholm-2016

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION: INFORMATION SECURITY

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

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

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

- **SEC301** Intro to Information Security **GISF**
- **SEC401** Security Essentials Bootcamp Style **GSEC**
- **SEC501** Advanced Security Essentials Enterprise Defender **GCED**

FUNCTION: NETWORK OPERATIONS CENTRE, SYSTEM ADMIN, SECURITY ARCHITECTURE

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

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

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

CORE COURSES
SEC301 GISF › SEC401 GSEC › SEC501 GCED

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

FUNCTION: SECURITY OPERATIONS CENTRE/ INTRUSION DETECTION

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

CORE COURSES
SEC301 › SEC401

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

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

Endpoint Monitoring
- **SEC501** Advanced Security Essentials - Enterprise Defender **GCED**
- **FOR508** Advanced Digital Forensics and Incident Response **GCFA**

Network Monitoring
- **SEC502** Perimeter Detection In-Depth **GPPA**
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **FOR572** Advanced Network Forensics and Analysis **GCIA**
- **SEC511** Continuous Monitoring and Security Operations **GMON**
- **SEC550** Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence
- **FOR578** Cyber Threat Intelligence

FUNCTION: RISK & COMPLIANCE/AUDITING/ GOVERNANCE

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

SAMPLE JOB TITLES:
Auditor, Compliance Officer

- **SEC566** Implementing & Auditing the Critical Security Controls - In-Depth **GCCC**
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

FUNCTION: INCIDENT RESPONSE

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

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

CORE COURSES
SEC301 GISF › SEC401 GSEC

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

Network Analysis
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **FOR572** Advanced Network Forensics and Analysis **GNFA**
- **FOR578** Cyber Threat Intelligence

Endpoint Analysis
- **FOR408** Windows Forensic Analysis **GCFE**
- **FOR508** Advanced Digital Forensics and Incident Response **GCFA**

Malware Analysis
- **FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques **GREM**

Specialisations
- **FOR526** Windows Memory Forensics In-Depth
- **MGT535** Incident Response Team Management

FUNCTION: PENETRATION TESTING/ VULNERABILITY ASSESSMENT

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

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

CORE COURSES
SEC301 GISF › SEC401 GSEC

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

Network & Exploits
- **SEC560** Network Penetration Testing and Ethical Hacking **GPEN**
- **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**
- **SEC760** Advanced Exploit Development for Penetration Testers

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

Mobile / Wireless
- **SEC575** Mobile Device Security and Ethical Hacking **GMOB**
- **SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses **GAWN**

Lab Centred
- **SEC561** Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise

Specialisations
- **SEC580** Metasploit Kung Fu for Enterprise Pen Testing
- **SEC573** Python for Penetration Testers

FUNCTION: SECURE DEVELOPMENT

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

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

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

- **Securing the Human for Developers STH.Developer** Application Security Awareness Modules
- **DEV522** Defending Web Applications Security Essentials **GWEB**
- **DEV541** Secure Coding in Java/JEE: Developing Defensible Applications **GSSP-JAVA**
- **DEV544** Secure Coding in .NET: Developing Defensible Applications **GSSP-.NET**

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

FUNCTION: CYBER OR IT SECURITY MANAGEMENT

Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

SAMPLE JOB TITLES:
CISO, Cyber Security Manager / Officer, Security Director

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

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

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

FUNCTION: DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

With today's ever-changing technologies and environments, it is inevitable that every organisation will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. To help solve these challenges, organisations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

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

- **FOR408** Windows Forensic Analysis **GCFE**
- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling **GCIH**
- **FOR508** Advanced Digital Forensics and Incident Response **GCFA**
- **FOR585** Advanced Smartphone Forensics
- **FOR518** MAC Forensic Analysis
- **FOR526** Memory Forensics In-Depth
- **FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques **GREM**

FUNCTION: INDUSTRIAL CONTROL SYSTEMS / SCADA

ICS-focused courses are designed to equip both security professionals and control system engineers with the knowledge & skills they need to safeguard critical infrastructure.

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

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

SEC 504

WWW.SANS.ORG/SEC504

HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

BJ GLEASON
GCIH Certification 37 CPEs
Monday: 9am – 7:15pm, Tuesday – Saturday: 9am – 5pm

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

COURSE DETAILS

Organisations' systems are likely to get hacked. All that's needed is an internet connection or a disgruntled employee or two. From the five, ten, or even one hundred daily probes against internet infrastructure, to the malicious insider slowly creeping through vital information assets, attackers target systems with increasing viciousness and stealth.

SANS SEC504 helps defenders understand attackers' tactics and strategies in detail. It gives hands-on experience of finding vulnerabilities and discovering intrusions. This course equips students with a comprehensive incident handling plan. The in-depth information in this course helps turn the tables on computer attackers.

This course addresses the latest cutting-edge, insidious attack vectors, the "oldie but-goodie" attacks that are still so prevalent, and criminal methods between these extremes. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents. Students receive a detailed description of how attackers undermine systems. This empowers defenders to prepare for, detect, and respond to attacks. The course features hands-on workshops for discovering holes before the bad guys do.

Additionally, SEC504 discusses the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well suited to individuals who lead, or are a part of, an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

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

WWW.SANS.ORG/SEC575

MOBILE DEVICE SECURITY AND ETHICAL HACKING

SEC 575

RAUL SILES
GMOB Certification 36 CPEs
Monday – Saturday: 9am – 5pm

COURSE DETAILS

Mobile phones and tablets have become an essential part of business life. Organisations of all types and sizes have embraced the agility and convenience that mobile offers. Along with convenience, however, the ubiquity of mobile in the work place has also brought new security risks.

As reliance on these devices has grown exponentially, organisations have quickly recognised that mobile phones and tablets need specific security implementations – solutions that go beyond simple screen protectors and clever passwords. Whatever the form factor and operating system, mobile devices have become hugely attractive and vulnerable targets for attackers. The use of such devices poses an array of new risks to organisations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- High probability of the device being hacked, lost or stolen

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

SEC575: Mobile Device Security and Ethical Hacking is designed to help organisations secure their mobile devices by equipping personnel with the knowledge to design, deploy, operate, and assess a well-managed and safe mobile environment. The course helps build the critical skills to support an organisation's secure deployment and use of mobile phones and tablets.

Students learn how to capture and evaluate mobile device network activity, disassemble and analyse mobile code, recognise weaknesses in common mobile applications, and conduct full-scale mobile penetration tests. Participants gain hands-on experience of designing a secure mobile phone network for local and remote users, and learn how to make critical decisions to support devices effectively and securely.

YOU WILL BE ABLE TO...

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android filesystem data to plunder compromised devices and extract sensitive mobile device use information
- Analyse Apple iOS and Android applications with reverse-engineering tools
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorised access to target devices
- Manipulate the behaviour of mobile applications to bypass security restrictions
- Auditors who need to build deeper technical skills

SEC 579

WWW.SANS.ORG/SEC579

VIRTUALISATION AND PRIVATE CLOUD SECURITY

DAVE SHACKLEFORD
36 CPEs
Monday – Saturday: 9am – 5pm

YOU WILL BE ABLE TO...

- Lock down and maintain a secure configuration for all components of a virtualisation environment
- Design a secure virtual network architecture
- Evaluate virtual firewalls, intrusion detection and prevention systems, and other security infrastructure
- Evaluate security for private cloud environments
- Perform vulnerability assessments and pen tests in virtual and private cloud environments, and acquire forensic evidence
- Perform audits and risk assessments within a virtual or private cloud environment

"EXCELLENT COURSE, VERY RELEVANT TO MY OWN DUTIES. SO I WILL BE ABLE TO APPLY SKILLS TO THIS. A LOT OF INFO TO TAKE IN BUT WILL USE THE GOOD BOOKS TO REFRESH!"
Mike Costello
QUALCOMM

COURSE DETAILS

Server virtualisation is one of today's most rapidly evolving and widely deployed technologies. Many organisations are already realising the cost savings from implementing virtualised servers. What's more, administrators love virtualised systems' ease of deployment and management.

With these benefits comes a dark side. Virtualisation technology is the focus of many new potential threats and exploits, and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams.

SEC579 starts with two days of architecture and security design for both virtual and private cloud infrastructures. The entire range of components is covered, ranging from hypervisor platforms to virtual networking, storage security, and locking down the individual virtual machine files.

The third and fourth days of SEC579 detail offense and defence - how virtualised environments can be assessed using scanning and penetration testing tools and techniques. The course also asks: how do things change when we move to a cloud model?

Once offense has been covered, SEC579 takes the opposite approach and goes into detail on performing intrusion detection and logging within the virtual environment, as well as covering anti-malware advances and changes within virtual infrastructure.

Day five helps students adapt existing security policies and practices to the new virtualised or cloud-based infrastructure. SEC579 shows how to design a foundational risk assessment program and then build on this with policies, governance, and compliance considerations within an environment.

Day six covers the top virtualisation configuration and hardening guides from Defense Information Security Agency (DISA), Center for Internet Security (CIS), Microsoft, and VMware. The course focusses on the most critical lessons and instructions from these guides. Students then perform a scripted, hands-on audit of VMware technology using controls guidance from the VMware hardening guide.

WWW.SANS.ORG/FOR610

REVERSE ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

FOR 610

JESS GARCIA
GREM Certification 36 CPEs
Monday – Saturday: 9am – 5pm

COURSE DETAILS

Understanding the capabilities of malware is critical to an organisation's ability to derive threat intelligence, respond to information security incidents, and to fortify its defences. This course builds a strong foundation for reverse-engineering malicious software. It explores a variety of system and network monitoring utilities, disassemblers, debuggers, and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. Students learn how to set up an inexpensive and flexible laboratory. FOR610 then teaches how to examine malicious software's inner workings, and how to use the lab to dissect real-world malware samples. Students examine specimens' behavioural patterns and code. The course continues by discussing essential x86 assembly language concepts.

Students also examine malicious code to understand its key components and execution flow. In addition, the course explores how to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

With this covered, students learn 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, students explore practical approaches to analysing malicious browser scripts, deobfuscating JavaScript and VBScript to understand the nature of the attack.

FOR610 also teaches students to analyse malicious documents such as Microsoft Office and Adobe PDF files. These documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks.

"IT REALLY GIVES NICE REALISTIC GUIDANCE ON HOW TO APPROACH COMPLEX PROBLEMS IN MALWARE ANALYSIS."
Markus Jeckeln
LUFTHANSA

YOU WILL BE ABLE TO...

- Build an isolated laboratory environment for analysing code and behaviour of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes on Microsoft Windows
- Uncover and analyse malicious JavaScript, VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- Control some aspect of the malicious program's behaviour through network traffic interception and code patching
- Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognise and understand common assembly-level patterns in malicious code, such as DLL injection

DEV 522

WWW.SANS.ORG/DEV522

DEFENDING WEB APPLICATIONS SECURITY ESSENTIALS

JASON LAM
GWEB Certification 36 CPEs
Monday - Friday 9am - 5pm

YOU WILL BE ABLE TO...

- Understand the major risks and common vulnerabilities related to web applications through real-world examples
- Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- Fulfil the training requirement as stated in PCI DSS 6 5
- Deploy and consume web services (SOAP and REST) in a secure fashion
- Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- Strategically roll out a web application security program

COURSE DETAILS

Defenders must learn to secure web applications because the importance of the data entrusted to these products is growing. Traditional network defences, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and helps defenders better understand web application vulnerabilities, thus enabling them to properly protect their organisation's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside proven, real-world applications. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.

To maximise the benefit for a wider range of audiences, the discussions in this course are programming language agnostic. Rather, the course focusses on security strategies as opposed to coding-level implementation.

DEV522: Defending Web Applications Security Essentials is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to: Application security analysts, developers, application architects and pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

"I AM A NEW EMPLOYEE IN THIS FIELD. THIS COURSE GIVES ME REALLY GOOD KNOWLEDGE FOR MY WORK."
Wafa Al Raisi
CENTRAL BANK OF OMAN

EVENT LOCATION & TRAVEL INFORMATION

RADISSON BLU, WATERFRONT HOTEL

Nils Ericsons Plan 4, Stockholm, 111 64 SE
Tel: +46 (8) 5050 6000 **Website:** www.radissonblu.com

TRANSPORT

The hotel is adjacent to Central Station, which features subway, railway and airport shuttle stops. Travellers arriving at Arlanda International Airport can reach the Radisson Blu via a 20-minute train ride.

DIRECTIONS TO THE HOTEL:

From Bromma Airport:
The airport bus to Cityterminalen, next to the Congress Centre, takes about 40 minutes.

Taxi service from the airport takes 20 minutes.

From Stockholm Arlanda Airport:
The Arlanda Express train stops next to the Waterfront Congress Centre and affords direct access through Stockholm Central Station; the trip takes approximately 20 minutes.

The airport bus to Cityterminalen, next to the Congress Centre, takes about 40 minutes.

Taxi service from the airport takes about 40 minutes.

From Skavsta Airport:
Airport bus to Cityterminalen, next to the Congress Centre, takes about 80 minutes.

Taxi service from the airport takes approximately 50 minutes.

Arlanda Express train and bus transportation:
Take the train to Stockholm Central Station, which provides direct access to the Congress Centre next to the hotel. National and international buses and airport buses arrive at Cityterminalen, next to the Congress Centre.

Driving directions:
Follow signs for Stockholm C, Centrum and Centralstationen (Central Station). The Congress Centre is located next to Central Station. Limited on-site parking service is available. Parking is also available in the vicinity of the Congress Centre.

Walking directions:
Guests can reach Nils Ericsons Plan via Klarabergsviadukten 59, next to the upper entrance to Central Station.

SANS STOCKHOLM 2016 INSTRUCTORS

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

READ ON FOR PROFILES OF THIS ELITE GROUP.

BJ Gleason

BJ Gleason has been teaching graduate and undergraduate information systems and computer security classes for over 30 years.

He holds undergraduate degrees in Computer Science, Criminal Justice, Asian Studies, and graduate degrees in Computer Science, Education, Information Security and Assurance as well as an Ed.S in Computer in Education. In addition, Mr. Gleason holds about 40 computer industry certifications from SANS (GCWN, G2700, GCFA, GREM, GPEN, GSLC, GWAPT, GCFE, GLEG, and GCIH), as well as (ISC)2, ISACA, Microsoft and is a Certified Computer Examiner from the International Society of Forensic Computer Examiners.

He has taught at New Jersey Institute of Technology, Upsala College, The American University in Washington DC, and University of Maryland University College.

He is currently working as a system and security administrator under contract with the US Military, and has been since 1999. He was the lead author of the user manual of Drew Fahey's Helix3 Forensic CD. ●

Dave Shackleford

SENIOR INSTRUCTOR

@daveshackleford

Dave Shackleford is the owner and principal consultant of Voodoo Security and a SANS analyst, senior instructor, and course author. He has consulted with hundreds of organisations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualised infrastructures.

He has previously worked as CSO for Configuresoft, CTO for the Centre for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is the author of the Sybex book Virtualisation Security: Protecting Virtualized Environments, as well as the co-author of Hands-On Information Security from Course Technology.

Recently Dave co-authored the first published course on virtualisation security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance. ●

Jason Lam

CERTIFIED INSTRUCTOR

@jasonlam_sec

Jason is a senior security analyst at a major financial institution in Canada. His recent SANS Institute courseware development includes Defending Web Application Security Essentials and Web Application Pen Testing Hands-On Immersion. He is currently a SANS certified instructor.

Jason started his career as a programmer before moving on to ISP network administration, where he handled network security incidents, which sparked his interest in information security.

Jason specialises in Web application security, penetration testing, and intrusion detection. He holds a BA in computer science from York University in Toronto, Ontario, as well as the CISSP, GCIA, GCFW, GCUX, GCWN, and GCIH certifications. ●

Jess Garcia

PRINCIPAL INSTRUCTOR

@j3ssgarcia

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

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

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

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

Raul Siles

CERTIFIED INSTRUCTOR

@raulsiles

Raul Siles is founder and senior security analyst at DinoSec.

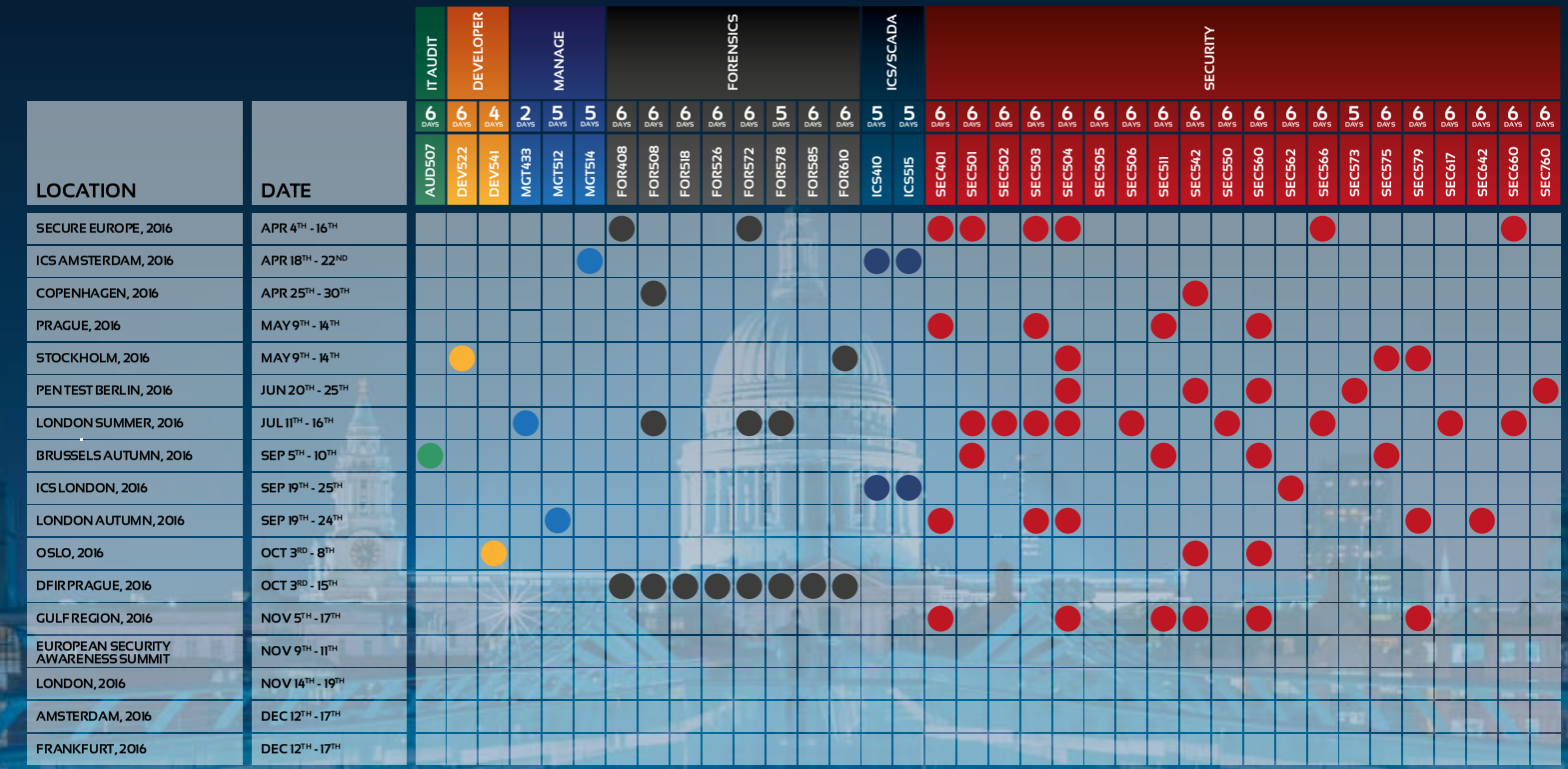
He has been involved in security architecture design and reviews, penetration tests, incident handling, intrusion and forensic analysis, security assessments and vulnerability disclosure, web applications, mobile and wireless environments, and security research in new technologies.

Throughout his career, starting with a strong technical background in networks, systems and applications in mission critical environments, he has worked as an information security expert, engineer, researcher and penetration tester at Hewlett Packard, as an independent consultant, and on his own companies, Taddong and DinoSec.

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

SANS EMEA TRAINING EVENTS 2016

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



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

Dates, Locations and Courses offered subject to change